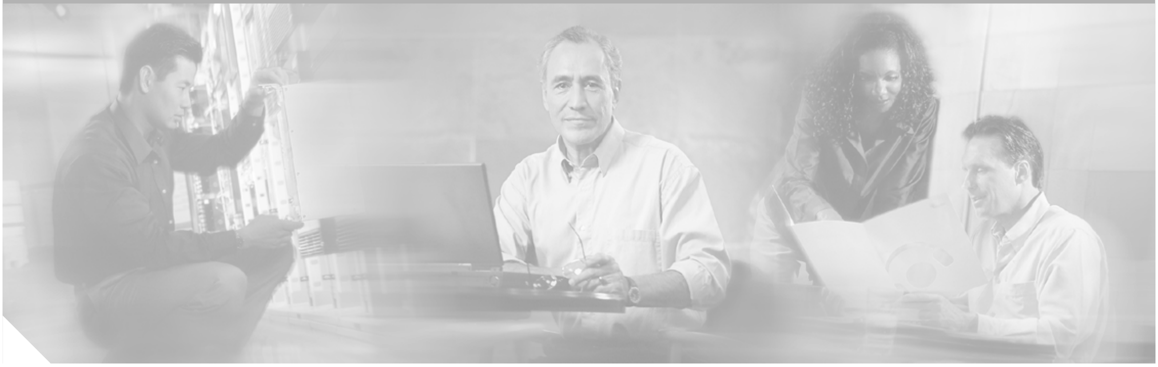


Cisco Content Services Switch Command Reference

Software Version 7.40
August 2004

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

Text Part Number: OL-5654-01

Cisco Content Services Switch Command Reference

CONTENTS

Preface

This guide provides the following information:

- The command-line interface (CLI) for the Cisco 11500 series Content Services Switches (CSS) and how to use the CLI.
- The CLI commands, including syntax, options, and related commands. All commands apply to all CSS models except where noted.

This preface contains the following major sections:

- Audience
- How to Use This Guide
- Related Documentation
- Symbols and Conventions
- Obtaining Documentation
- Documentation Feedback
- Obtaining Technical Assistance
- Obtaining Additional Publications and Information

Audience

This guide is intended for the following trained and qualified service personnel who are responsible for operating a CSS:

- System administrator
- Web master
- System operator

How to Use This Guide

This guide is organized as follows:

Chapter	Description
Chapter 1, Using the Command-Line Interface	This chapter provides an overview of the CLI, and instructions on how to use the CLI and its commands.
Chapter 2, CLI Commands	This chapter provides an alphabetical listing of all general and configuration mode CLI commands. The information for each command includes a brief description, syntax with any options and variables, and related commands when applicable. This chapter also provides information about the configuration modes for the commands and how to access each mode.

Related Documentation

In addition to this document, the CSS documentation set includes the following:

Document Title	Description
Release Note for the Cisco 11500 Series Content Services Switch	This release note provides information on operating considerations, caveats, and command line interface (CLI) commands for the Cisco 11500 series CSS.
Cisco 11500 Series Content Services Switch Hardware Installation Guide	This guide provides information for installing, cabling, and powering the Cisco 11500 series CSS. In addition, this guide provides information about CSS specifications, cable pinouts, and hardware troubleshooting.
Cisco Content Services Switch Getting Started Guide	This guide describes how to perform initial administration and configuration tasks on the CSS, including: • Booting the CSS for the first time and a routine basis, and logging in to the CSS • Configuring the username and password, Ethernet management port, static IP routes, and the date and time • Configuring DNS server for hostname resolution • Configuring sticky cookies with a sticky overview and advanced load-balancing method using cookies • Finding information in the CSS documentation with a task list • Troubleshooting the boot process

Document Title	Description
Cisco Content Services Switch Administration Guide	This guide describes how to perform administrative tasks on the CSS, including upgrading your CSS software and configuring the following: • Logging, including displaying log messages and interpreting sys.log messages • User profile and CSS parameters • SNMP • RMON • XML documents to configure the CSS • CSS scripting language • Offline Diagnostic Monitor (Offline DM) menu
Cisco Content Services Switch Routing and Bridging Configuration Guide	This guide describes how to perform routing and bridging configuration tasks on the CSS, including: • Management ports, interfaces, and circuits • Spanning-tree bridging • Address Resolution Protocol (ARP) • Routing Information Protocol (RIP) • Internet Protocol (IP) • Open Shortest Path First (OSPF) protocol • Cisco Discovery Protocol (CDP) • Dynamic Host Configuration Protocol (DHCP) relay agent

Document Title	Description
Cisco Content Services Switch Content Load-Balancing Configuration Guide	This guide describes how to perform CSS content load-balancing configuration tasks, including: • Flow and port mapping • Services • Service, global, and script keepalives • Source groups • Loads for services • Dynamic Feedback Protocol (DFP) • Owners • Content rules • Sticky parameters • HTTP header load balancing • Content caching • Content replication
Cisco Content Services Switch Global Server Load-Balancing Configuration Guide	This guide describes how to perform CSS global load-balancing configuration tasks, including: • Domain Name System (DNS) • DNS Sticky • Content Routing Agent • Client-Side Accelerator • Network proximity
Cisco Content Services Switch Redundancy Configuration Guide	This guide describes how to perform CSS redundancy configuration tasks, including: • VIP and virtual interface redundancy • Adaptive session redundancy • Box-to-box redundancy

Document Title	Description
Cisco Content Services Switch Security Configuration Guide	This guide describes how to perform CSS security configuration tasks, including: • Controlling access to the CSS • Secure Shell Daemon protocol • Radius • TACACS+ • Firewall load balancing
Cisco Content Services Switch SSL Configuration Guide	This guide describes how to perform CSS SSL configuration tasks, including: • SSL certificate and keys • SSL termination • Back-end SSL • SSL initiation
Cisco Content Services Switch Device Management User's Guide	This guide describes how to use the Device Management user interface, an HTML-based Web-based application that you use to configure and manage your CSS.

Symbols and Conventions

This guide uses the following symbols and conventions to identify different types of information.

Caution A caution describes a specific action that could cause loss of data or adversely impact the use of the equipment.

Warning **A warning describes a specific action that could cause either physical harm to you or damage to the equipment.**

Note A note provides important related information, reminders, and recommendations.

Bold text indicates a command in a paragraph.

`Courier text` indicates text that appears in a command line, including the CLI prompt.

`Courier bold text` indicates commands and text you enter in a command line.

Italics text indicates the first occurrence of a new term, book title, emphasized text, and variables that you supply.

1. A numbered list indicates that the order of these list items is important.
   a. An alphabetical list indicates that the order of these secondary list items is important.

- A bulleted list indicates that the order of these list topics is unimportant.
  – An indented list indicates that the order of these list subtopics is unimportant.

For information about the command syntax conventions for the CLI, refer to Chapter 1, Using the Command-Line Interface.

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

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

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

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

Documentation Feedback

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco Technical Support Website

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

http://www.cisco.com/techsupport

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

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

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 automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

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

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

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

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

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

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

  http://www.ciscopress.com

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

  http://www.cisco.com/packet

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

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

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

  http://www.cisco.com/ipj

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

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

Using the Command-Line Interface

The command-line interface (CLI) is a line-oriented user interface that has a set of commands for configuring, managing, and monitoring the CSS. To help you use these commands, this chapter provides you with information on:

- CLI Modes
- Logging into and Exiting the CLI
- Using CLI Commands
- Getting CLI Help
- User-Defined Variables
- CSS Scripts

For information on specific CLI commands, refer to Chapter 2, CLI Commands.

CLI Modes

The CLI provides the following modes:

- User
- SuperUser
- Configuration and its subordinate modes

The following sections describe each of these modes:

- User Mode
- SuperUser Mode

User Mode

When the CSS administrator assigns a username with User permission, this permission level allows you to log in to User mode on the CSS. This mode is identified by a prompt that ends with a greater-than symbol (>). Within this mode, you can use a limited set of commands to monitor and display CSS parameters but not change them.

For information on the commands you can use in User mode, refer to Chapter 2, CLI Commands, "General Commands".

SuperUser Mode

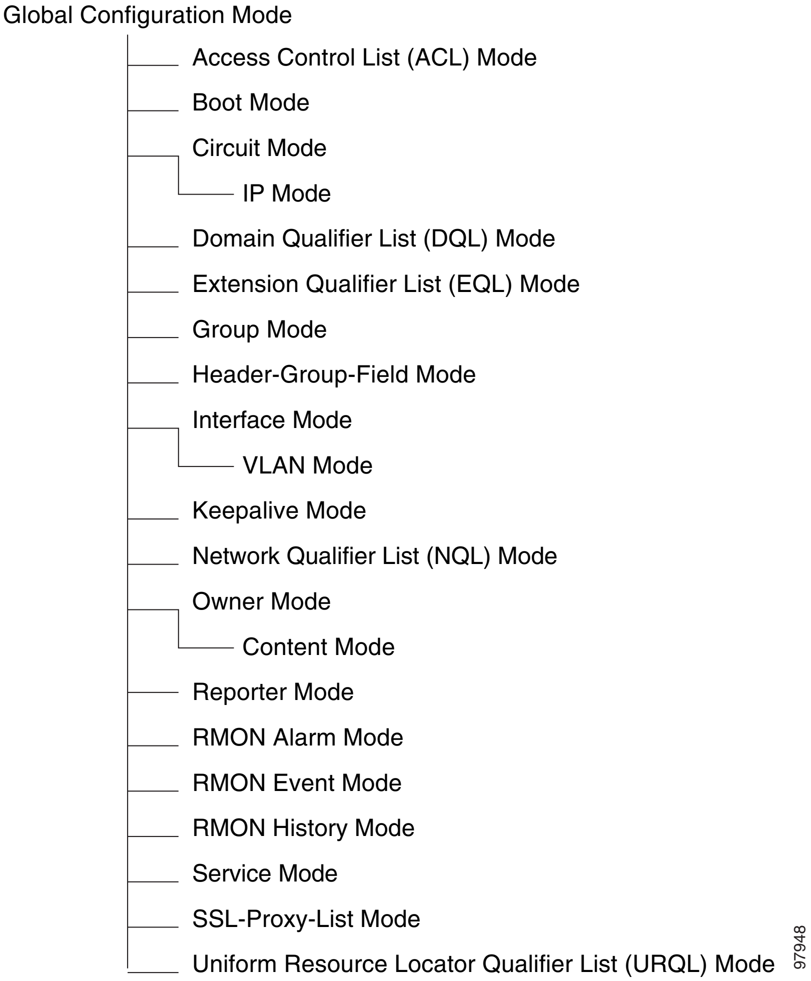
When the CSS administrator assigns a username with SuperUser permission, this permission level allows you to log in to SuperUser mode on the CSS. This mode is identified by a prompt that ends with a pound sign (#).

Within this mode, you can use the commands to maintain the CSS and to access global configuration mode to configure the CSS. You can also use User-mode commands in SuperUser mode.

For information on the commands you can use in SuperUser mode, refer to Chapter 2, CLI Commands, "General Commands".

Configuration Modes

When you log in to the CSS as a SuperUser, you can use the **configure** command to access global configuration mode. This mode is identified by a (config) prompt. Within this mode, you can use its set of commands to configure the CSS and access its subordinate configuration modes.



When you access any of the subordinate configuration modes, the CSS appends the mode name to the (config) prompt. For example, when you access owner mode from global configuration mode, the prompt changes to (config-owner [*owner_name*]).

Each mode has its own set of commands. Many of the modes have commands allowing you to access other related modes. When you switch modes, you exit the current mode and enter the new mode. For example, from interface configuration mode, you can move directly to ACL, circuit, DQL, EQL, group, owner, RMON alarm, RMON event, RMON history, service, or URQL configuration mode.

To exit any configuration mode and return to SuperUser mode, press **Ctrl-Z**.

For information on the commands you can use in global configuration mode and its subordinate modes, including the **configure** command, refer to Chapter 2, CLI Commands.

Logging into and Exiting the CLI

When the CSS completes the system boot, the CLI starts automatically and is available for use. To log in to the CSS and access the CLI, use a terminal device connected to the Console port on the CSS.

Instead of using the Console port, you can also use Telnet. For more information on terminal settings for Telnet use, refer to the *Cisco 11500 Series Content Services Switch Hardware Installation Guide* for the 11500 series CSS.

You can use the CLI from any terminal device that is compatible with ANSI, VT52, or VT100 characteristics. ANSI and VT100 devices let you use cursor-control and cursor-movement keys: left-arrow, up-arrow, down-arrow, right-arrow, Delete, and Backspace. The CLI senses the use of cursor-control keys and automatically uses the optimal device characteristics.

Note The first time you log in to the CLI, use the default username of **admin** and the default password of **system**.

To exit from the CLI, use the **exit** command from SuperUser mode. If you are currently in one of the configuration modes and want to exit the CLI, press **Ctrl-Z** to return to SuperUser mode, and then use the **exit** command.

Using CLI Commands

This section provides information on:

- Command conventions for syntax used in this book and variable argument conventions
- Entering multiple commands
- CLI keyboard shortcuts when you are using the CLI
- Using grep
- Understanding CLI syntax checking and error messages

Syntax Conventions

To help you identify the parts of a CLI command, Chapter 2, CLI Commands, uses conventions to show the syntax of commands. Table 1-1 lists these syntax conventions and their descriptions.

Table 1-1 Syntax Conventions

Syntax Convention	Description
boldface	Identifies commands and options you must enter exactly as shown.
italics	Identifies variables you must supply. For more information on variable arguments, see the next section.
... (ellipsis)	Identifies the continuation of the command.
| (vertical bar)	Identifies mutually exclusive choices. Note that you can also use the | character as a pipe with **grep**. For more information on **grep**, see the "Using grep" section.
[ ] (square brackets)	Encloses required keywords or variables.
{ } (braces)	Encloses optional options or variables.

Note Do not enter the ellipsis, brackets, vertical bar, or braces in command lines. This guide uses these symbols only to show the types of entries.

CLI commands and options are in lowercase and are case-sensitive. For example, when you enter the **configure** command, enter it all in lowercase, not CONFIGURE or Configure. Text entries you create are also case-sensitive. For example, if you set a username to Sys1, enter it exactly, not sys1 or SYS1.

Note When Cisco Systems makes syntax changes to existing commands, the CSS automatically updates the startup-config file with the most recent changes when you upgrade the software on the CSS. For example, the CSS changes the **web-mgmt state enabled** command to the **no restrict xml** command.

Variable Argument Conventions

Some commands require variable arguments for information you must supply. CLI command variable arguments generally consist of integers, quoted and unquoted text strings, IP addresses and subnet masks, host names, Media Access Control (MAC) addresses, interfaces, stack layers, and timeslots.

Table 1-2 lists the types of arguments you may encounter and the conventions to enter this information.

Table 1-2 Variable Arguments

Variable Argument	Convention
host names	Enter host names in mnemonic host-name format. For example: `myhost.mydomain.com`
integers	Enter only whole numbers with no decimal points. For example: `200`

Table 1-2 Variable Arguments (continued)

Variable Argument	Convention

Internet Protocol (IP) Addresses and Subnet Masks	Enter IP addresses and subnet masks in dotted-decimal notation. This notation is four groups of up to three decimal numbers, separated by periods. Each group has a maximum number of 255. For example:
	`192.168.11.1`
	`255.255.255.0`
	For some arguments, you can also use Classless Interdomain Routing (CIDR) notation for subnet masks. For example:
	• /24 is equivalent to 255.255.255.0
	• /16 is equivalent to 255.255.0.0

Interface	Interface entries specify physical interfaces present in the CSS. Enter interfaces in groups of one to three characters. The format depends on your CSS. • For the 11501 CSS, enter: *interface type-port* For example: **`e2`** • For the 11503 or 11506 CSS, enter: *slot/port* For example: **`1/1`** **`13/5`**
MAC addresses	Enter MAC addresses as six groups of two hexadecimal numbers each, separated by hyphens. The alphabetic characters are not case-sensitive. For example: `07-77-25-C9-af-13`

Table 1-2 Variable Arguments (continued)

Variable Argument	Convention
stack layers	Stack layer entries specify layers within interface stacks. Enter one of the following: • circuit - An CSS circuit • mlppp - A point-to-point multilink bundle • physical - The physical interface
text strings: quoted	Enter quoted text strings as text and spaces enclosed in quotation marks. For example: **"Server lab A-3"**

text strings: unquoted	Enter unquoted text strings as contiguous alphanumeric characters without spaces or quotation marks. For example:
	`Sys_1`
	`MyLink`

timeslots	Timeslots specify channels within a channelized serial interface. With timeslots, you can arbitrarily specify slots for individual use within a serial interface. Enter numbers separated by commas or hyphens with no spaces. For example: `1,2,4-8,9,20`

Entering Multiple Commands

You can enter multiple commands on a single command line by separating them with the semicolon (;) character. For example:

```
copy running-config startup-config;archive startup-config
```

CLI Command Keyboard Shortcuts

Table 1-3 lists the CLI keyboard shortcuts to help you enter and edit command lines.

Table 1-3 CLI Command Keyboard Shortcuts

Action		Keyboard Shortcut
Cancel the current operation, additional display of MORE output, or delete the current line.		Ctrl-C
Capitalize the character at the cursor.		Esc-C
Change:	The word at the cursor to lowercase.	Esc-L
	The word at the cursor to uppercase.	Esc-U
Delete:	A character at the cursor.	Ctrl-D
	A character to the left of the cursor.	Ctrl-H, Delete, or Backspace
	All characters from the cursor to the beginning of the line.	Ctrl-U or Ctrl-X
	All characters from the cursor to the end of the line.	Ctrl-K
	All characters from the cursor to the end of the word.	Esc-D
	The word to left of the cursor.	Ctrl-W or Esc-Backspace
Display the buffer's:	Next line.	Ctrl-N or Down Arrow
	Previous line.	Ctrl-P or Up-Arrow

Table 1-3 CLI Command Keyboard Shortcuts (continued)

Action		Keyboard Shortcut
Display MORE output:	Current line number.	l or L
	Exit from MORE output.	q, Q, or Ctrl-C
	Go to a line number in the buffer. The default is the last line. To go to a specific line, enter the line number before pressing the g or G key. For example, enter 3G to go to the third line in the buffer.	g or G
	Help screen.	h or H
	Next additional screen. The default is one screen. To display more than one screen, enter a number before pressing the Spacebar key.	Spacebar
	Next line. The default is one line. To display more than one line, enter the number before pressing the Return key.	Return
	Previous line. To display more than one line, enter the number before pressing Up Arrow key.	Up Arrow
	Previous screen. The default is one screen. To display more than one screen, enter a number before pressing the b, B, or Ctrl-B key.	b, B, or Ctrl-B
	Redraw screen.	r, R, or Ctrl-L
	Search forward for *regular_expression.*	/*regular_expression*
	Search backward for *regular_expression.*	?*regular_expression*
Enter an Enter or Return key character.		Ctrl-M
Enter a global configuration mode *command* from any mode.		@*command*
Expand the command or abbreviation.		Ctrl-I or Tab

Table 1-3 CLI Command Keyboard Shortcuts (continued)

Action		Keyboard Shortcut
Move the cursor:	One character to the left (back).	Ctrl-B or Left Arrow
	One character to the right (forward).	Ctrl-F or Right Arrow
	One word to the left (back), to the beginning of current or previous word.	Esc-B
	One word to the right (forward), to the end of the current or next word.	Esc-F
	To the beginning of the line.	Ctrl-A
	To the end of the line.	Ctrl-E
Redisplay the current line.		Ctrl-L or Ctrl-R
Return to the SuperUser mode from any configuration mode.		Ctrl-Z
Toggle:	Line logging suppression.	Esc-S
	MORE support.	Esc-M
Transpose a character at the cursor with a character to left of the cursor.		Ctrl-T

Using grep

You can apply **grep** to any CLI commands with the (|) pipe character. For example:

show running-config|grep IP

show log log.file|grep -i ip

The usage of grep is:

grep [**-**[**i**|**v**|**s**]] *keyword*

The options are:

- **i** - Case-insensitive search
- **v** - Displays all lines not containing keyword
- **s** - Displays all lines following match

Understanding CLI Syntax Checking and Error Messages

If you enter an invalid or incomplete command, the CLI responds with a pointer (^) and an error message. The following example shows the CLI response when you enter an invalid command:

```
# bobo
  ^
%% Invalid input detected at '^' marker.
```

The following example shows the CLI response when you enter an incomplete command:

```
(config)# service
                 ^
%% Insufficient arguments to form command.
```

Getting CLI Help

The CLI provides several types of context-sensitive help:

- Question mark
- Tab key
- Help commands

Question Mark (?)

The question mark (?) character allows you to get the following type of help about a command at the command line:

Question Mark Usage	Command Help Type
? at command prompt	All commands for that mode
command **?**	All options for a command
command option **?**	All arguments for a command and its option
*command-abbrev***?**	All commands that begin with specific letters

If the CLI is unable to provide question mark support, a bell sounds when you enter the key.

Tab Key

When you press the Tab key or Ctrl-I at the end of a unique command or option abbreviation, the CLI completes the command or options for you. For example:

```
#al<Tab>
#alias
```

Pressing the Tab key or Ctrl-I keys also completes an option up to the point where it is unique. If multiple commands have the same abbreviation that you entered, the CLI lists all of these commands.

Note If the CLI is unable to provide complete Tab key support, a bell sounds when you enter the key.

Help Command

You can display a series of help topics by entering the **help** command at the CLI prompt, or display help information about specific topics including the following:

- Entering commands - Use the **help commands** command.
- Configuration files - Use the **help configuration** command.
- Keyboard shortcuts - Use the **help keys** command.
- Navigating modes - Use the **help modes** command.
- Variables - Use the **help variables** command.

User-Defined Variables

The CLI supports user-defined variables for use from the command line and from scripts. There are two types of variables: character and numeric. If you assign the variable with all integers and no spaces, it is a numeric variable. If you assign the variable with any text characters and spaces, it is a character variable.

To create or manipulate variables, refer to the **set**, **input**, **modify**, and **var-shift** commands in Chapter 2, CLI Commands.

CSS Scripts

CSS scripts include scripts that you write using CLI commands, scripts provided with your CSS, and special scripts containing user profile information. For detailed information about writing scripts, refer to the *Content Services Switch Basic Configuration Guide.*

Writing and Running CLI Scripts

Use the CLI **script record** command to record command entries in a script file. You can also use an ASCII text editor to write CLI scripts (for example, Microsoft Notepad, MS-DOS Edit, UNIX PICO, or EMACS). Do not use a word processing program such as Microsoft Word or WordPad.

The CLI provides the following script commands:

- **echo**
- **endbranch**
- **exit**
- **function**
- **if**
- **input**
- **modify**
- **pause**
- **set**
- **while**

For more information about these commands and their options, refer to Chapter 2, CLI Commands.

When you finished creating the file, press **Ctrl-C** to exit the **script record** command mode. If you used a text editor, save the script by entering any filename and extension with a maximum of 32 characters. Then, use the **copy** command to move the script file to the CSS.

To run a CLI script, use the **script play** command.

CSS-Provided Scripts

The CSS contains scripts that CSS provides to assist you with tasks, for example, CLI setup and upgrade. To see a list of CSS-provided scripts, use the **show script** command. To run a CLI script, use the **script play** command.

The CSS also provides aliases to run the scripts. To see a list of all aliases, refer to the **show aliases** command.

Profile Scripts

When a user logs into the CSS, the CSS runs a profile script. These scripts contain commands that are exclusive to the current CLI session. The CSS performs the folllowing tasks:

- A default-profile script for everyone
- A user-profile script for the matching username

After you log in to the CSS, you can modify your profile by changing the CLI prompt, terminal parameters, or expert mode setting, or by adding alias commands. The CSS keeps these changes in a temporary running profile until you exit the CLI.

To permanently save any running profile changes to your user profile, do either of the following:

- Copy the running profile to your user-profile script with the **copy profile user-profile** command.
- Wait until you exit the CLI, and enter a **y** in response to the prompt and query to save your profile changes; if you enter an **n**, your profile changes are discarded.

For more information on changing your profile, refer to the *Content Services Switch Administration Guide*.

CLI Commands

This chapter provides detailed information for the following types of CSS CLI commands:

- General commands are commands you can enter after you log in to the CSS as a User or SuperUser.
- Configuration mode commands are commands you can enter after you log in to the CSS as a SuperUser, and then access global configuration mode and its subset of modes.

The description for each command includes:

- The syntax for the command
- Any related commands, when appropriate

Note CSS software is available in a Standard or optional Enhanced feature set. The Enhanced feature set includes the commands of the Standard feature set, and the commands for Network Address Translation (NAT) Peering, Domain Name System (DNS), Demand-Based Content Replication (Dynamic Hot Content Overflow), Content Staging and Replication, and Network Proximity DNS.

Proximity Database and the Secure Management option (including Secure Shell Host and SSL strong encryption for the Device Management software) are optional features. For details about activating a CSS software option, refer to the *Cisco Content Services Switch Administration Guide*.

General Commands

General commands are commands available to you immediately after you log in to a CSS. The commands you can run depends on your permission level. If you have:

- User permissions, the CSS limits you to the following general commands and any associated **no** forms in User mode:

    - **cls**
    - **echo**
    - **enable**
    - **endbranch**
    - **exit**
    - **function**
    - **help**
    - **if**
    - **input**
    - **modify**
    - **pause**
    - **ping**
    - **prompt**
    - **set**
    - **show**
    - **terminal**
    - **traceroute**
    - **var-shift**
    - **version**
    - **while**
    - **zero dos statistics**
    - **zero ip-fragment-stats**
    - **zero ip statistics**
    - **zero reporter state-transitions**
    - **zero service**

    These commands, except **enable**, **prompt**, and **terminal**, are also available in all configuration modes.

- SuperUser permissions, all general commands and SuperUser commands are available to you. You can also access global configuration mode and its commands. For more information on global configuration mode commands, see the "Global Configuration Mode Commands" section.

The descriptions of the general commands in this section indicate whether you can use the command in User or SuperUser mode or both, and if the command is available in all modes.

admin-shutdown

To shut down all interfaces simultaneously, use the **admin-shutdown** command. This command provides a quick way to shut down all physical devices in the CSS. Use the **no** form of the command to restart all interfaces.

admin-shutdown

no admin-shutdown

Command Modes

SuperUser

Usage Guidelines

To shut down an individual interface, use the **(config-if) admin-shutdown** command.

Caution Shutting down the physical interfaces on the CSS terminates all activity on them.

Related Commands

show interface
(config-if) admin-shutdown
(config-if) shut

alias

To create an alias for one or more commands, use the **alias** command. Assign the alias to a specific mode. If you want to assign the alias to all modes, use the **all** keyword. Use the **no** form of this command to delete the alias from a mode.

alias *mode alias_name* **"***CLI_command*{**;***CLI_command***;***CLI_command***...**}"

no alias *mode alias_name*

Syntax Description

mode	Mode that you want to assign to the alias.To view all available CSS modes, enter: `# alias ?`
alias_name	Name for the new alias command. Enter an unquoted text string with no spaces and a maximum length of 32 characters.
CLI_command	One or more CLI commands to be aliased. Enter the command, its options, and variables exactly. Enclose the command text string in quotes (“”). When entering multiple CLI commands, insert a semicolon (;) character to separate each command.

Command Modes

All modes

Usage Guidelines

You can include an alias as a session-based configuration parameter for a profile script.

Related Commands

show aliases

archive

To archive files, use the **archive** command. Archiving is useful when you update software and want to save a script, log, or startup-config file from a previous release of software. An archive directory on the CSS disk stores the archive files.

archive [[**startup-config**|**log** *log_filename*|**script** *script_filename*] {*archive_filename*}|**running-config** *archive_filename*]

Syntax Description

startup-config	Archives the startup configuration file.
log	Archives a log file.
script	Archives a script file.

log_filename	Filename of the log to archive. To see a list of log files, enter the **archive log ?**command.
script_filename	Filename of the script to archive. To see a list of script files, enter the **archive script ?** command.
running-config	Archives the running configuration.
archive_filename	Name you want to assign to the archive file. Enter an unquoted text string with a maximum length of 32 characters.

Command Modes

All modes

Usage Guidelines

The archive directory resides on the CSS hard drive. If you booted your CSS from a network-mounted system and your hard drive is not working, archive- and restore-related functions are suspended.

Related Commands

copy
restore
script
show

clear *disk_slot*

To delete the startup configuration file or specific log, script, or archive file stored on a disk in the CSS, use the **clear** *disk_slot* command.

clear *disk_slot* [**archive** *archive_filename*
|**log** *log_filename*|**startup-config**|**script** *script_filename*]

Syntax Description

disk_slot	Disk location containing the file you want to delete. The valid entries are: • **0** for the disk in slot 0 • **1** for the disk in slot 1
archive	Clears a file in the archive directory.
archive_filename	Name of the archive file to clear.
log	Clears a log file.
log_filename	Filename for the log.
script	Clears a script file.
script_filename	Filename for a valid script file.
startup-config	Clears the startup configuration.

Command Modes

SuperUser

Usage Guidelines

The **clear** *disk_slot* command is applicable for an 11500 series CSS with two disks.

The startup-config file provides the CSS with the initial configuration. If you delete this file, the CSS will boot the default configuration.

clear

To clear system information, use the **clear** command.

clear [**archive** *archive_filename*|**arp cache** {*ip_or_host*}|**arp file**
|**log** *log_filename*|**running-config**|**script** *script_filename*
|**ssl** [**file** *filename* "*password*"|**statistics** {**slot** *number*}]
|**startup-config**|**startup-errors**|**statistics** *interface_name*]

Syntax Description

archive *archive_filename*	Clears the specified file in the archive directory. The *archive_filename* is the name of the archive file to clear. To list the archive files, enter: `# clear archive ?`
arp cache	Deletes all of the dynamic entries from the ARP cache.
ip_or_host	Address for the single ARP entry you want to remove from the ARP cache. Enter the address in either dotted-decimal IP notation (for example, 192.168.11.1) or mnemonic host-name format (for example, myhost.mydomain.com).
arp file	Clears the file containing the host addresses that the ARP module on the CSS resolved for the ARP table at initialization or boot time.
log *log_filename*	Clears a log file. The *log_filename* variable is the filename for the log. To see a list of log files, enter: `# clear log ?`
running-config	Clears the running configuration.
script *script_filename*	Clears a script file. The *script_filename* variable is the filename for a valid script file. To see a list of script files, enter: `# clear script ?`
ssl	Clears SSL files on the CSS or statistics on the SSL module.
file *filename* "*password*"	Clears SSL certificates and private keys from the CSS that are no longer valid. Note that the **clear ssl file** command does not function if the file currently has an association with it. The association must be removed first. • The *filename* variable is the name of the certificate, key pair, or Diffie-Hellman parameter file that you want to remove from the CSS. • The *password* variable is the password used to DES (Data Encryption Standard) encode the file when it was originally imported or generated by the CSS. This password must be an exact match or the file cannot be cleared.

statistics {**slot** *number*}	Clears the SSL statistics counters for all SSL modules in the CSS chassis. The **show ssl** command displays the statistics. To clear SSL statistics counters for a specific module, use the **slot** *number* option to specify the slot of the module. The valid slot entries are 2 to 3 (CSS 11503) or 2 to 6 (CSS 11506).
startup-config	Clears the startup configuration. The startup-config file provides the CSS initial configuration. Without this file, the CSS will boot the default configuration. The **startup-config** keyword does not clear the IP address for the management port.
startup-errors	Clears the startup configuration errors file. Before each boot, the CSS automatically removes the startup-errors file.
statistics *interface_name*	Resets the Ethernet errors, MIB-II, and RMON statistics on a CSS Ethernet interface to zero. The *interface_name* argument is the name of the physical interface. Enter a case-sensitive unquoted text string. To see a list of interfaces, enter: `# clear statistics ?`

Command Modes

SuperUser

Related Commands

archive
show arp
show ether-errors
show mibii
show rmon
show ssl
update arp
(config) arpscript
(config) logging

cliLogMessage subsystem

To define a log message for a subsystem at a logging level, use the **cliLogMessage subsystem** command.

cliLogMessage subsystem *name* **“***message***”** **level** *level*

Syntax Description

name Name of a CSS subsystem. Enter one of the following subsystem names:

- **acl** - Access control lists
- **all** - All subsystems
- **app** - Application Peering Protocol (APP)
- **boomerang** - DNS Content Routing Agent
- **buffer** - Buffer Manager
- **cpd** - Cisco Discovery Protocol (CDP)
- **chassis** - Chassis Manager
- **circuit** - Circuit Manager
- **csdpeer** - Content Server Database (CSD) Peer
- **dhcp** - Dynamic Host Configuration Protocol (DHCP)
- **dql** - Domain qualifier list (DQL)
- **fac** - Flow Admission Control (FAC)
- **flowagent** - Flow Agent
- **flowmgr** - Flow Manager
- **fp-driver** - Fathpath Driver
- **hfg** - Header field group (HFG)
- **ipv4** - Internet Protocol version 4
- **keepalive** - Keepalive
- **natmgr** - NAT Manager

name (cont.)	• **netman** - Network Management • **nql** - Network qualifier list (NQL) • **ospf** - OSPF • **pcm** - Proximity CAPP Messaging (PCM) • **portmapper** - PortMapper • **proximity** - Proximity • **publish** - Publish • **radius** - Remote Authentication Dial-In User Server (RADIUS) • **replicate** - Replication • **redundancy** - CSS Redundancy • **rip** - RIP • **security** - Security Manager • **slr** - Session Level Redundancy • **sntp** - Simple Network Time Protocol (SNTP) • **ssl-accel** - Secure Socket Layer (SSL) Acceleration • **syssoft** - System software • **urql** - Uniform resource qualifier list • **vlanmgr** - VLAN Manager • **vpm** - Virtual Pipe Manager • **vrrp** - Virtual Router Redundancy Protocol • **wcc** - Web Conversation Control To see a list of subsystems, enter: `# cliLogMessage subsystem ?`

level	Log level for the message. Enter one of these levels: • **fatal-0** - Fatal errors only • **alert-1** - Alert errors, including errors at the fatal-0 level • **critical-2** - Critical errors, including errors at the alert-1 level • **error-3** - Error errors, including errors at the critical-2 level • **warning-4** - Warning errors (default), including errors at the error-3 level • **notice-5** - Notice messages, including errors at the warning-4 level • **info-6** - Informational messages, including errors at the notice-5 level • **debug-7** - All errors and messages

Command Modes

All modes

Related Commands

show log
(config) logging disk
(config) logging host
(config) logging line

clock

To set the date, time, or time zone, use the **clock** command. Use the **no** form of the **clock timezone** command to reset the time zone information to 00:00:0.

clock [**date**|**time**|**timezone** *name* **hour** *hours* {**before-UTC**|**after-UTC**} {**minute** *minutes* {**before-UTC**|**after-UTC**}}]

no clock timezone

Syntax Description

date	Sets the date. When you enter this command, a prompt appears and shows the current date in the format you must use to enter the new date. Enter the month, day, and year as integers with dash characters separating them. For example, enter June 15th 2000 as 06-15-2000. If you use the **(config) date european-date** command, the format for entering the date is day, month, and year. For example, enter June 15th 2000 as 15-06-2000.
time	Sets the time in military-time format. When you enter this command, a prompt appears and shows the current time in the format you must use to enter the new time. Enter the hour, minutes, and seconds as integers with colon characters separating them. For example, enter 12:23:14. If you configure a time zone, the **show clock** command displays the time adjusted with the time zone offset.
timezone *name*	Sets the time zone to offset the Universal Time Coordinated (UTC) time from an SNTP server. Enter a name with a maximum of 32 characters and no spaces. The **timezone** keyword applies only when you configure an SNTP server. Otherwise, the CSS ignores this option.
hour *hours*	Sets the hours offset for the time zone. Enter a number from 0 to 12. If the **before-UTC** or **after-UTC** option is omitted, the offset is set to a positive number.

before-UTC	(Optional) Sets the offset as a negative number. For example, if the hour offset is 12, the **before-UTC** keyword sets it to -12.
after-UTC	(Optional) Sets the offset as a positive number. This is the default offset.
minute *minutes*	(Optional) Sets the minutes offset for the time zone. Enter a number from 0 to 59. If the **before-UTC** or **after-UTC** option is omitted, the offset is set to a positive number.

Command Modes

SuperUser

Usage Guidelines

You cannot use the backspace key for the **clock date** or **time** command.

Related Commands

show clock
(config) date european-date
(config) sntp

cls

To clear the terminal screen, use the **cls** command.

cls

Command Modes

All modes

configure

To enter global configuration mode, use the **configure** command. Configuration commands apply to the system as a whole.

config

Command Modes

SuperUser

Usage Guidelines

When you use the **configure** command to enter global configuration mode, the CLI prompt changes to (config).

From this mode, you can also enter these configuration modes:

- ACL
- Boot
- Circuit and IP
- DQL
- EQL
- Group
- Header-field group
- Interface and VLAN
- Keepalive
- NQL
- Owner and Content
- RMON alarm, RMON event, and RMON history
- Service
- SSL-proxy-list
- URQL

For information about the commands available in these modes, see the "Global Configuration Mode Commands" section.

To exit the current configuration mode, enter **exit**.

To exit any configuration mode and return to SuperUser mode, press **Ctrl-Z**.

copy *source_disk_slot*

To copy all of the contents or specified startup configuration, core dumps, logs, scripts, archive, and boot image files from the source disk to the destination disk in the CSS, use the **copy** *source_disk_slot* command. The CSS software creates the software directory and hierarchy on the destination disk.

copy *source_disk_slot* {**archive** *filename* {*destination_filename*}|**archives**
|**boot-image** *filename*|**core** *filename* {*destination_filename*}|**cores**
|**log** *filename* {*destination_filename*}|**logs**
|**script** *filename* {*destination_filename*}|**scripts**|**startup-config**}

Syntax Description

source_disk_slot	Designates the disk as the source location containing the files. The other disk is designated as the destination disk. The valid entries are: • 0 for the disk in slot 0 • 1 for the disk in slot 1
archive *filename*	(Optional) Copies the specified archive filename to the destination disk.
destination_filename	(Optional) Name you want to assign to the file on the destination disk.
archives	(Optional) Copies all archive files to the destination disk.
boot-image *filename*	(Optional) Copies the specified ADI (ArrowPoint Distribution Image) of the boot-image to the destination disk.
core *filename*	(Optional) Copies the specified core dump file to the destination disk.
cores	(Optional) Copies all core dump files to the destination disk.
log *filename*	(Optional) Copies the specified log file to the destination disk.
logs	(Optional) Copies all log files to the destination disk.
script *filename*	(Optional) Copies the specified script to the destination disk.

scripts	(Optional) Copies all scripts from the specified disk to the destination disk.
startup-config	(Optional) Copies the startup configuration to the destination disk.

Command Modes

SuperUser

Usage Guidelines

You can use the **copy** *disk_slot* command only on an 11500 series SCM (System Control Module) with two disks. Make sure that an equivalent release of CSS software is present on the destination disk before you copy files to it. If necessary, copy the boot-image to the destination disk before copying a startup-config, log, or script file.

Related Commands

script
show installed-software
(config) logging

copy

To copy files to and from File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) servers, use the **copy** command. The keywords for this command are:

- **copy core** - Copies a core dump file
- **copy ftp** - Copies from an FTP server
- **copy log** - Copies a log file
- **copy profile** - Copies the running profile
- **copy running-config** - Copies the running configuration
- **copy script** - Copies a script file
- **copy ssl** - Imports or exports certificates and private keys from or to the CSS
- **copy ssl** - Copies the startup configuration
- **copy tftp** - Copies from a TFTP server

For information about these commands and any associated options, see the **copy** commands in this section.

Command Modes

SuperUser

## copy core

To copy a core dump file from the CSS to an FTP or TFTP server, use the **copy core** command.

copy core *core_filename* [**ftp** *ftp_record*|**tftp** *ip_or_host*] *filename*

Syntax Description

core_filename	Name of the core dump file on the CSS. Enter an unquoted text string with the appropriate capitalization, no spaces, and a maximum length of 32 characters. To see a list of core dump files, enter: `# copy core ?`
ftp *ftp_record*	Copies a core dump file to an FTP server. The name of the FTP record file contains the FTP server IP address, username, and password. Enter an unquoted text string with no spaces. To create an FTP record, see the **(config) ftp-record** command.
tftp *ip_or_host*	Copies a core dump file to a TFTP server. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or in mnemonic host-name format (for example, myhost.mydomain.com).
filename	Name you want to assign to the file on the server. Include the full path to the file. Enter an unquoted text string with no spaces and a maximum length of 32 characters.

Command Modes

SuperUser

Usage Guidelines

Before you copy a core dump file from the CSS to an FTP server, you must create an FTP record file containing the FTP server IP address, username, and password. See the **(config) ftp-record** command for more information.

Related Commands

(config) ftp-record

copy ftp

To copy an ArrowPoint Distribution Image (ADI), script file, or startup configuration file from an FTP server to the CSS, use the **copy ftp** command.

copy ftp *ftp_record filename* [**boot-image**|**script** *script_filename* |**startup-config**]

Syntax Description

ftp_record	Name of the FTP record file that contains the FTP server IP address, username, and password. Enter an unquoted text string with no spaces. To create an FTP record, see the **(config) ftp-record** command.
filename	Name of the file on the FTP server that you want to copy to the CSS. Include the full path to the file. Enter an unquoted text string with no spaces and a maximum length of 32 characters. If you are using the **boot-image** keyword to copy an ADI file from an FTP server to the CSS, include the full path to the file including the file extension. Enter an unquoted text string with no spaces and a maximum length of 32 characters. You can also copy a GZIP-compressed version of the ADI file. The CSS uncompresses the file. If there is not enough disk space available, the CSS provides a message.
boot-image	Copies an ADI file from an FTP server. The ADI file contains the CSS software including boot files and logging and archiving directories. To unpack the CSS software in the ADI file, use the **(config-boot) unpack** command. When you use the **boot-image** keyword, the file you copy to the CSS must be an ADI file. Otherwise, the CSS rejects it.

script *script_file*	Copies an FTP file to the script directory. To assign a name to the script file on the CSS, enter an unquoted text string with no spaces and a maximum length of 32 characters.
startup-config	Copies the startup configuration and overwrites the existing configuration file.

Command Modes

SuperUser

Usage Guidelines

Before using this command, you must use the **(config) ftp-record** command to create an FTP record file containing the FTP server IP address, username, and password.

Related Commands

script
(config) ftp-record
(config-boot) unpack

## copy log

To copy a log file from the CSS to an FTP or TFTP server, use the **copy log** command.

copy log *log_filename* [**ftp** *ftp_record*|**tftp** *ip_or_host*] *filename*

Syntax Description

log_filename	Name of the log file on the CSS. Enter an unquoted text string with no spaces and a maximum length of 32 characters. To see a list of log files, enter: `# copy log ?`
ftp *ftp_record*	Copies a log file to an FTP server. The name of the FTP record file contains the FTP server IP address, username, and password. Enter an unquoted text string with no spaces. To create an FTP record, see the **(config) ftp-record** command.
tftp *ip_or_host*	Copies a log file to a TFTP server. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or in mnemonic host-name format (for example, myhost.mydomain.com).
filename	Name you want to assign to the file on the server. Include the full path to the file. Enter an unquoted text string with no spaces and a maximum length of 32 characters.

Command Modes

SuperUser

Related Commands

(config) ftp-record
(config) logging

copy profile

To copy the running profile from the CSS to an FTP server, TFTP server, your user profile, or the default profile, use the **copy profile** command.

copy profile [**default-profile**|[**ftp** *ftp_record*|**tftp** *ip_or_host*] *filename*|**user-profile**]

Syntax Description

default-profile	Copies the running profile to the default profile.
ftp *ftp_record*	Copies the running profile to an FTP server. The name of the FTP record file contains the FTP server IP address, username, and password. Enter an unquoted text string with no spaces. To create an FTP record, see the **(config) ftp-record** command.
tftp *ip_or_host*	Copies the running profile to a TFTP server. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or in mnemonic host-name format (for example, myhost.mydomain.com).
filename	Name you want to assign to the file on the server. Include the full path to the file. Enter an unquoted text string with no spaces and a maximum length of 32 characters.
user-profile	Proactively copies the changes on the running profile to the user profile. This command creates a file *username*-profile if one does not exist, where *username* is the current username. If the CSS is not in expert mode and you exit the CSS without copying any changes in the running profile to your user profile, the CSS prompts you that the profile has changed and queries whether you want to save your changes.

Command Modes

SuperUser

Related Commands

(config) ftp-record

copy running-config

To copy the running configuration to an FTP or TFTP server or to the startup configuration file on the CSS disk, use the **copy running-config** command.

copy running-config [[**ftp** *ftp_record*|**tftp** *ip_or_host*] *filename*|**startup-config**]

Syntax Description

ftp *ftp_record*	Copies the running configuration to an FTP server. The name of the FTP record file contains the FTP server IP address, username, and password. Enter an unquoted text string with no spaces. To create an FTP record, see the **(config) ftp-record** command.
tftp *ip_or_host*	Copies the running configuration to a TFTP server. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or in mnemonic host-name format (for example, myhost.mydomain.com).
filename	Name you want to assign to the file on the server. Include the full path to the file. Enter an unquoted text string with no spaces and a maximum length of 32 characters.
startup-config	Copies the running configuration to the startup configuration file on the CSS disk. In the event of the CSS rebooting, if you do not save changes in the running-config file to the startup-config file, these changes are lost.

Command Modes

SuperUser

Related Commands

(config) ftp-record

## copy script

To copy a script file from the CSS to an FTP or TFTP server, use the **copy script** command. To create a script file, see the **script** command.

copy script *script_file* [**ftp** *ftp_record*|**tftp** *ip_or_host*] *filename*

Syntax Description

script_file	The name of the script file on the CSS. Enter an unquoted text string with no spaces and a maximum length of 32 characters. To see a list of script files, enter: `# copy script ?`
ftp *ftp_record*	Copies a script file to an FTP server. The name of the FTP record file contains the FTP server IP address, username, and password. Enter an unquoted text string with no spaces. To create an FTP record, see the **(config) ftp-record** command.
tftp *ip_or_host*	Copies a script file to a TFTP server. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or in mnemonic host-name format (for example, myhost.mydomain.com).
filename	The name you want to assign to the file on the server. Include the full path to the file. Enter an unquoted text string with no spaces and a maximum length of 32 characters.

Command Modes

SuperUser

Usage Guidelines

A profile file is a special script. You can use the **copy profile** command to copy it.

Related Commands

script
(config) ftp-record

copy ssl

To import or export certificates and private keys from or to an 11500 series CSS, use the **copy ssl** command. A secure location on the CSS disk stores all files imported into the CSS.

copy ssl [**ftp**|**sftp**] *ftp_record* [**import** *filename* [*format*] "*password*" {"*passphrase*"}|**export** *filename2* "*password*"]

Syntax Description

ftp|**sftp**	The FTP or SFTP protocol to transfer the certificate and private key file. Cisco Systems recommends the SFTP protocol as the transport mechanism because it provides the most security. If SSHD access is restricted, or if the license key is not installed, SSHD will not accept connections from SSH clients and the **copy ssl sftp** command will fail, resulting in an error message.
ftp_record	The name of the previously-created FTP record containing the remote server information. To create an FTP record, see the **(config) ftp-record** command.
import	Imports the file from the remote server.
filename	Name of the file you want to import from the server. Include the full path to the file. You can enter a maximum of 128 characters.

format	File format of the certificate to be imported. Once the certificate file is converted to PEM format and DES encoded, it is stored on the CSS SCM in a special (and secure) directory. The valid import file formats are: • **DER** - Binary format encoding of the certificate file in ASN.1 using the Distinguished Encoding Rules (DER-encoded X509 certificate). For example, an imported certificate from a Microsoft Windows NT IIS 4.0 server. • **PEM** - Privacy Enhanced Mail, a base64 encoding of the certificate file (PEM-encoded X509 certificate). For example, an imported certificate from an Apache/SSL UNIX server. • **PKCS12** - Standard from RSA Data Security, Inc. for storing certificates and private keys. For example, an imported certificate from a Microsoft Windows 2000 IIS 5.0 server.
"*password***"**	Password used to DES (Data Encryption Standard) encode the imported certificate or private key. Encoding the imported file prevents unauthorized access to the certificate or private key on the CSS. Enter the password as a quoted string. The password appears in the CSS running configuration as a DES-encoded string.
"*passphrase***"**	(Optional) Passphrase used to encrypt the certificate or key being imported into the CSS. Some certificates or keys may have had a passphrase assigned to encrypt them prior to being imported into the CSS. Enter the passphrase as a quoted text string.
export	Exports the file to the remote server.
filename2	Name you want to assign to the file on the server. Include the full path to the file. Enter an unquoted text string with no spaces and a maximum length of 32 characters.

Command Modes

SuperUser

Usage Guidelines

An imported file can contain certificates, RSA or DSA key pairs, or Diffie-Hellman parameters. You must distinguish whether the files contain certificates, privates keys, or Diffie-Hellman parameters by associating the specific contents to a filename.

Related Commands

(config) ftp-record

copy startup-config

To copy the startup configuration to an FTP or TFTP server or to the running configuration, use the **copy startup-config** command.

copy startup-config [[**ftp** *ftp_record*|**tftp** *ip_or_host*] *filename*|**running-config**]

Syntax Description

ftp *ftp_record*	Copies the startup configuration to an FTP server. The name of the FTP record file contains the FTP server IP address, username, and password. Enter an unquoted text string with no spaces. To create an FTP record, see the **(config) ftp-record** command.
tftp *ip_or_host*	Copies the startup configuration to a TFTP server. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or in mnemonic host-name format (for example, myhost.mydomain.com).
filename	Name you want to assign to the file on the server. Include the full path to the file. Enter an unquoted text string with no spaces and a maximum length of 32 characters.
running-config	Copies the startup configuration and merges with the running configuration file on the CSS disk.

Command Modes

SuperUser

Related Commands

(config) ftp-record

copy tftp

To copy files from a TFTP server to the script directory or overwrite the startup configuration on the CSS, use the **copy tftp** command.

copy tftp *ip_or_host filename* [**script** *script_file*|**startup-config**]

Syntax Description

ip_or_host	IP address or host name of the TFTP server to receive the file. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or in mnemonic host-name format (for example, myhost.mydomain.com).
filename	Name for the file on the TFTP server. Include the full path to the file. Enter an unquoted text string with no spaces.
script *script_file*	Copies a TFTP file to the script directory. To assign a name to the script file on the CSS, enter an unquoted text string with no spaces and a maximum length of 32 characters.
startup-config	Copies a TFTP file to and overwrites the startup configuration.

Command Modes

SuperUser

Related Commands

script

disable

To access User mode, use the **disable** command to exit SuperUser mode. In User mode, you can monitor and display CSS parameters, but not change them.

disable

Command Modes

SuperUser

Usage Guidelines

To log in as a SuperUser from User mode, use the **enable** command.

Related Commands

enable
exit

# disconnect

To disconnect a connected session or line, use the **disconnect** command.

disconnect *session*

Syntax Description

session	The Telnet or console session. To see a list of sessions, enter: `# disconnect ?`

Command Modes

SuperUser

dns resolve

To resolve a host name by querying the configured DNS server on the CSS, use the **dns resolve** command.

dns resolve *host_name*

Syntax Description

host_name	The name of the host you want to resolve. Enter the host name in mnemonic host-name format (for example, myhost.mydomain.com).

Command Modes

All modes

dns-boomerang client zero

To clear the statistics for a configured domain displayed through the **show dns-boomerang client** command, use the **dns-boomerang client zero** command.

dns-boomerang client zero

Command Modes

SuperUser and all configuration modes

Related Commands

show dns-boomerang client

echo

To enable terminal echo and optionally echo a message with or without a line feed, use the **echo** command. This is useful when creating scripts and controlling output. Typical use of this command is in a script file. Use the **no** form of this command to disable terminal echo.

echo {**-n**} {**“***message***”**}

no echo

Syntax Description

-n	(Optional) Echo the message to the terminal without a line feed.
message	(Optional) Echo the message to the terminal with a line feed. Enter a quoted text string, user-defined argument, or status variable. You can include the **\n** characters in the message to produce line feeds.

Command Modes

All modes

Related Commands

input
set
show variable

enable

To log in as a SuperUser in User mode, use the **enable** command.

enable

Command Modes

User

Usage Guidelines

The **enable** command prompts you for a valid username and password.

After you log in with a username that has SuperUser privileges, you can access the full set of CLI commands, including those in User mode. SuperUser commands let you change parameters and configure the CSS. To set SuperUser usernames and passwords, use the **(config) username** command.

Related Commands

disable
exit

endbranch

To terminate a branch block initiated by an **if** or **while** command, use the **endbranch** command. Typical use of this command is in a script file. For more information on scripts, refer to the *Cisco Content Services Administration Guide*.

endbranch

Command Modes

All modes

Related Commands

if
while

exit

Use the **exit** command to exit from:

- The current mode and return to the previous mode. If you are in User or SuperUser mode, this command ends the CLI session and disconnects the line.
- An upper-branch block.
- A current script.

exit {**branch**|**script** {*status*}}

Syntax Description

branch	(Optional) Exits the upper-branch block.
script	(Optional) Exits the current script.
status	(Optional) Integer value placed in the STATUS variable when a script completes execution. If you do not define the STATUS variable, with the exception of the **grep** command, an exit status of 0 indicates that a command was successful. A non-zero value indicates a failure. This value is set automatically by the CLI after each command completes its execution.

Command Modes

All modes

Usage Guidelines

If you are in User or SuperUser mode when you use the **exit** command to exit the current mode, you will exit the session. When you exit a mode, the prompt changes accordingly.

Typically, you use the **exit branch** and **exit script** commands in script files. For more information on scripts, refer to the *Cisco Content Services Administration Guide*.

Related Commands

script

expert

To turn on expert mode, use the **expert** command. In expert mode, the CLI does not ask for confirmation before you execute commands that could delete or radically change operating parameters. Expert mode is off by default. Use the **no** form of this command to reset expert mode to its default setting of off.

expert

no expert

Command Modes

SuperUser

Usage Guidelines

Your user profile contains the expert mode setting when you log in to the CSS. If you change this setting during a CSS session, you can permanently save the setting in your profile by using the **copy running-config** command. Or when you exit a CLI session, you can respond with a **y** when the CSS prompts you that the profile has changed and queries whether you want to save the changes to the user profile.

find ip address

To search the CSS configuration for the specified IP address, use the **find ip address** command. You can include a netmask for subnet (wildcard) searches. This search can help you avoid IP address conflicts when you configure the CSS.

When you use this command, it checks services, source groups, content rules, ACLs, the management port, syslog, APP sessions, and local interfaces for the specified address. If the address is found, the locations of its use are displayed. If no addresses are found, you are returned to the command prompt.

find ip address *ip_or_host* {*subnet_mask*|**range** *number*}

Syntax Description

ip_or_host	IP address you want to find. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or in mnemonic host-name format (for example, myhost.mydomain.com).
subnet_mask	(Optional) IP subnet mask. Enter the mask either: • As a prefix length in CIDR bitcount notation (for example, /24). Do not enter a space to separate the IP address from the prefix length. • In dotted-decimal notation (for example, 255.255.255.0). If you enter a mask of 0.0.0.0, the CSS finds all addresses.
range *number*	(Optional) Defines how many IP addresses that you want to find, starting with the *ip_or_host* address. Enter a number from 1 to 65535. The default is 1. For example, if you enter an IP address of 203.1.1.1 with a range of 10, the CSS tries to find the addresses from 203.1.1.1 through 203.1.1.10.

Command Modes

All modes

flow statistics

To display statistics on currently allocated flows or inactive redundant flows, use the **flow statistics** command.

flow statistics {**dormant**}

Syntax Description

dormant	(Optional) Displays the statistics on inactive redundant flows in an Adaptive Session Redundancy (ASR) configuration on the CSS.

Usage Guidelines

The **flow statistics** command displays the UDP and TCP flows per second, the hits per seconds, and the flow information for each port.

The **flow statistics dormant** command display summary information about redundant dormant flows.

For information about the fields in the **flow statistics dormant** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Command Modes

ACL, global, group, interface, owner, content, service, SuperUser, and User

format

To format a disk in the CSS, use the **format** command.

format *disk_slot* {**quick**}

Syntax Description

disk_slot	Disk you want to format. Enter **0** for the disk in slot 0, or **1** for the disk in slot 1.
quick	(Optional) Reformats the disk without performing cluster verification. Only use the quick format when you are certain of the disk integrity.

Command Modes

SuperUser

Usage Guidelines

When you enter the **format** command, the CSS queries you about formatting the disk.

```
Formatting the disk results in all disk data being permanently erased.
Are you sure you want to continue? (yes,no):
```

Enter either of the following:

- **yes** to reformat the disk.
- **no** to abort the reformat function. If the disk has unrecoverable errors and you do not reformat it, be aware that the file system may be corrupt and functionality is compromised.

function

To create a function and call it within a script, use the **function** command.

function *name* [**begin**|**end**|**call** {**"***values ...***"**}|**return** {**"***values ...***"**}]

Syntax Description

name	Name of the function. Enter a text string with a maximum of 32 characters.
begin	Starts the definition of the function.
end	Ends the definition of the function.
call	Calls the function.
return	Exits the function and optionally sets the value in the RETURN variable.
"*values*"	(Optional) One or more optional alphanumeric values you want to pass into the function or set a value in the RETURN variable. Enter the value(s) in a quoted string.

Command Modes

All modes

Usage Guidelines

The **function** command allows you to define the function once within the script and then call it by its name one or more times to perform its functions. You can define the function either before or after you call it within the script. For more information on scripts, refer to the *Cisco Content Services Administration Guide*.

Related Commands

endbranch
if
input
set
show variable

help

To display CLI help on all or a specified topic, use the **help** command. The CLI also provides other forms of context-sensitive help. See the "Getting CLI Help" section in Chapter 1, Using the Command-Line Interface

help [**commands**|**configuration**|**keys**|**modes**|**variables**]

Syntax Description

commands	Displays help on entering commands.
configuration	Displays help on configuration files.
keys	Displays help on keyboard shortcuts.
modes	Displays help on configuration modes.
variables	Displays help on variables.

Command Modes

All modes

history length

To modify the history buffer length, use the **history length** command. The command-line history buffer stores the most recent CLI commands that you have entered. Use the **no** form of this command to restore the history buffer to the default of 20 lines.

history length *buffer_length*

no history length

Syntax Description

buffer_length	The number of lines in the command-line history buffer. Enter an integer from 0 to 256. The default is 20. To disable the history function, enter **0**.

Command Modes

SuperUser

if

To initiate conditional branch execution of a branch block, use the **if** command. This branch construct is available with an interactive session or within a script. Typically, you use this command in a script. You can nest any number of commands in a branch block including nested branch blocks.

if [*constant*|*variable_name*] {"*operator(s)*" "*operand(s)*"}

Syntax Description

constant	Numeric constant. Enter an integer or user-defined variable.
variable_name	Character string representing a variable. Enter a name with a maximum length of 32 characters.
"*operator*"	(Optional) One or more operations on the operand. Enter a quoted string of one or more of the following operators. Separate multiple operators with a space. • OR — Simple OR operator • > — Greater than operator • AND — Simple AND operator • * — Multiplication operator • MOD — Modulus operator • / — Division operator • >= — Greater than or equal to operator • < — Less than operator • <= — Less than or equal to operator • == — Equality operator • + — Add to variable • - — Subtract from variable • -- — Decrement variable • ++ — Increment variable Numeric value operators are handled one at a time from left to right, using the list of operands from the list as needed. Operators, such as -- and ++, do not require an operand.

"*operand*"	(Optional) One or more strings or arguments, as follows: • For character operators, enter a quoted string of either a string constant or a character argument. • For numeric operators, enter a quoted string of one or more integers or numeric argument. Separate multiple operands with a space.

Command Modes

All modes

Usage Guidelines

For more information on scripts, refer to the *Cisco Content Services Administration Guide*.

Related Commands

endbranch
function
input
set
show variable

input

To create a variable for the command line or script that prompts a user for a value to assign to a variable, use the **input** command. Typically, you use this command in a script. When the user enters the value and enters the carriage return, the value is assigned to the variable.

input *variable_name directory_level*

Syntax Description

variable_name	Character string representing the variable. Enter a string with a maximum length of 32 characters.
directory_level	Directory level for the variable. Enter one of these options: • **archive** - Default archive directory • **log** - Default log directory • **script** - Default script directory based on the boot image • **top** - Root level directory

Command Modes

All modes

license

To enter the software license key, use the **license** command.

license

At the prompt for a license key, enter the number.

Command Modes

SuperUser

lock

To lock the terminal and CLI session, use the **lock** command. Locking the terminal allows you to prevent access to your terminal while maintaining the connection to a CLI session.

lock

When you enter the **lock** command, the screen displays this message:

```
*** Session is locked. Press any key to provide unlock authentication
***
```

To unlock the terminal, press any key. Enter your username and password at the appropriate prompt.

Command Modes

SuperUser

login

To log in to the CSS with a different user identity, use the **login** command.

login

This command prompts you for a valid username and password. To set SuperUser usernames and passwords, see the **(config) username** command.

Command Modes

SuperUser

Related Commands

enable
exit

map

To map the primary and secondary boot record, logging output, archive files, or core dumps to a disk in the CSS (located in slot 0 or slot 1), use the **map** command. Use the **no** form of this command to reset the default mapping for a boot record to the disk in slot 0, or the log output or core dumps to the disk from which the CSS booted.

map [**core**|**log**|**primary-boot**|**secondary-boot**] *disk_slot*
no map core|**log**|**primary-boot**|**secondary-boot**

Syntax Description

core	Maps the core dumps.
log	Maps the logging output.
primary-boot	Maps the primary boot record.
secondary-boot	Maps the secondary boot record.
disk_slot	The slot number for the disk. Enter one of the following: • **0** - The disk in slot 0 • **1** - The disk in slot 1

Command Modes

SuperUser

Usage Guidelines

The **map** command is applicable for an 11500 series CSS with two disks.

Related Commands

show map

modify

To change the value of any numeric variable, use the **modify** command. Typically, you use this command in a script.

modify *variable_name* **“***operator(s)***”** {**“***operand(s)***”**}

Syntax Description

variable_name	A character string representing a variable. Enter a name with a maximum length of 32 characters.
“*operator*”	(Optional) One or more operations on the operand. Enter a quoted string of one or more of the following operators. Separate multiple operators with a space. • OR — Simple OR operator • > — Greater than operator • AND — Simple AND operator • * — Multiplication operator • MOD — Modulus operator • / — Division operator • >= — Greater than or equal to operator • < — Less than operator • <= — Less than or equal to operator • == — Equality operator • + — Add to variable • - — Subtract from variable • -- — Decrement variable • ++ — Increment variable Numeric value operators are handled one at a time from left to right, using the list of operands from the list as needed. Operators, such as -- and ++, do not require an operand.

"*operand*"	(Optional) One or more integers or numeric arguments. Enter a quoted string. Separate multiple operands with a space.

Command Modes

All modes

Usage Guidelines

For more information on scripts, refer to the *Cisco Content Services Administration Guide*.

Related Commands

function
input
set
show variable

no

To negate a command or set it to its default, use the **no** command. Note that some commands do not have a **no** form.

Syntax Description

no admin-shutdown	Restarts all interfaces on the CSS (available in SuperUser mode only)
no alias *mode alias_name*	Deletes an alias, *alias_name*, that you have created for a command in a specific mode, *mode*
no clock timezone	Resets the time zone information to 00:00:0 and the clock time without the time zone offset (available in SuperUser mode only)
no echo	Disables terminal echo (available in all modes)
no expert	Turns off expert mode
no history length	Resets the history buffer to the default of 20 lines (available in all modes)
no map core|log|primary-boot |secondary-boot	Resets the default mapping for a boot record to the disk in slot 0, or the log output or core dumps to the disk from which the CSS booted
no prompt	Resets the prompt to the default prompt (available in User and SuperUser modes)
no proximity refine	Stops the metric refinement process in the Proximity Database (available in SuperUser mode only)
no set *variable_name*	Deletes the user-defined variable, *variable_name* (available in all modes)
no terminal idle	Resets the idle time for this terminal session to the default of 0, disabling the session idle timer (available in User and SuperUser modes)
no terminal length	Resets the number of lines to the default of 25 lines (available in User and SuperUser modes)
no terminal more	Disables support for **more** functions (available in User and SuperUser modes)

no terminal netmask-format	Displays subnet masks in the default dotted-decimal format in the **show** commands (available in User and SuperUser modes)
no terminal timeout	Resets the timeout for a terminal session to the default of 0, disabling the session timeout (available in User and SuperUser modes)

pause

To pause for a specified number of seconds after entering a command, use the **pause** command.

pause *seconds*

Syntax Description

seconds	An integer for the number of seconds to pause

Command Modes

All modes

Usage Guidelines

You can use the **pause** command with an interactive session or within a script. Typically, you use this command in a script. When you enter this command, a message similar to the following appears:

```
Pausing for 20 seconds. Ctrl^C to abort...
```

To interrupt the pause, press **Ctrl-C**.

ping

To send Internet Control Message Protocol (ICMP) echo requests to test network connectivity, use the **ping** command.

ping *ip_or_host* {*number*} {*delay*}

Syntax Description

ip_or_host	IP address for the host you want to test. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or in mnemonic host-name format (for example, myhost.mydomain.com).
number	(Optional) Number of ping messages to send. Enter an integer from 1 to 1000. The default is 1.
delay	(Optional) Delay time between ping messages, in milliseconds. Enter an integer from 1 to 65535. The default is 100.

Command Modes

All modes

prompt

To set or change the CLI prompt, use the **prompt** command. The new prompt persists until you change it or until you reboot the CSS. Use the **no** form of this command to restore the prompt to the default.

prompt *prompt*

no prompt

Syntax Description

prompt	The new prompt. Enter an unquoted text string with no spaces and a maximum length of 12 characters.

Command Modes

User and SuperUser

Usage Guidelines

To save the new prompt as the default, use the **copy running-config** command.

You can include a prompt as a session-based configuration parameter in a profile script.

proximity

To administer and control the operation of the Proximity Database (PDB) in a dedicated CSS 11150 with 256 MB of RAM, use the **proximity** command and its keywords. The keywords for this SuperUser command include:

- **proximity assign** - Overrides the default metric determination processes to provide a local metric or metrics for all zones.
- **proximity assign flush** - Flushes all or a portion of the previously assigned proximity assignments.
- **proximity clear** - Removes the entries from the Proximity Database.
- **proximity commit** - Writes either a portion or all the Proximity Database to the CSS disk or an FTP daemon.

- **proximity refine** - Begins periodic refinement of metric entries within the Proximity Database.
- **proximity reprobe** - Forces a reprobe of existing IP addresses.
- **proximity retrieve** - Loads a database file from the CSS disk or an FTP daemon.

For information about these commands and any associated options, see the **proximity** commands in this section.

proximity assign

To override the default metric determination processes and provide a metric or metrics for all zones, use the **proximity assign** command. All CSSs in the Proximity Database mesh share assigned information. When you use this command, Network Proximity does not perform active probing of the assigned block.

proximity assign *ip_address prefix_length* [**“***local_metric***”|”***metric_list***”**]

Syntax Description

ip_address	IP address you want to associate with the metric information. Enter the address in dotted-decimal format (for example, 192.168.11.1).
prefix_length	IP prefix length used with the IP address. This prefix allows you to assign metrics over a range of IP addresses. Enter the prefix as either: • A prefix length in CIDR bitcount notation (for example, /24). • A subnet mask in dotted-decimal notation (for example, 255.255.255.0).
“*local_metric*”	Single metric to represent the zone where this command is issued. Enter the metric as a quoted number.
“*metric_list*”	List of metrics, in ascending zone order, that represent all zones. Enter the metric list as a string of numbers enclosed in quotes.

Command Modes

SuperUser

Usage Guidelines

The **proximity assign** command is functional only on a Proximity Database CSS in a dedicated CSS 11150 with 256 MB of RAM.

Note This command is not added to the running-config.

Examples

For example, to assign the metric "200" to a zone for all IP addresses within the range 203.0.0.0 to 203.255.255.255, enter:

```
# proximity assign 203.0.0.0/8 "200"
```

To perform the metric assignment for all IP addresses within the range 192.167.0.0 to 192.167.255.255, enter:

```
# proximity assign 192.167.0.0/16 "30 20 40 100 10 5"
```

To view the metric assignments for all IP addresses within the range of 192.167.0.0 to 192.167.255.255, enter:

```
# show proximity assign 192.167.0.0/16
    IP/PrefixHits Zone Metrics
    ----------------------------
    192.167.0.0/1610, 12330, 20, 40, 100, 10, 5
```

Related Commands

proximity assign flush
show proximity assign

proximity assign flush

To remove all or specific existing proximity assignments configured with the **proximity assign** command, use the **proximity assign flush** command.

proximity assign flush {*ip_address ip_prefix*}

Syntax Description

ip_address ip_prefix	(Optional) IP address and IP prefix length for the assignments you want to remove. Enter the address in dotted-decimal format (for example, 192.168.11.1). Enter the prefix as either: • A prefix length in CIDR bitcount notation (for example, /24). • A subnet mask in dotted-decimal notation (for example, 255.255.255.0).

Command Modes

SuperUser

Usage Guidelines

The **proximity assign flush** command is functional only on a Proximity Database CSS in a dedicated CSS 11150 with 256 MB of RAM.

proximity clear

To remove all or specified entries from the proximity database, use the **proximity clear** command.

proximity clear {*ip_address ip_prefix*}

Syntax Description

ip_address ip_prefix	(Optional) IP address and IP prefix length for the assignments you want to remove. Enter the address in dotted-decimal format (for example, 192.168.11.1). Enter the prefix as either: • A prefix length in CIDR bitcount notation (for example, /24). • A subnet mask in dotted-decimal notation (for example, 255.255.255.0).

Command Modes

SuperUser

Usage Guidelines

The **proximity clear** command is functional only on a Proximity Database CSS in a dedicated CSS 11150 with 256 MB of RAM.

proximity commit

To write either a portion or all of the Proximity Database to a file in the log directory on the CSS disk or a file on an FTP server, use the **proximity commit** command. The database output contains metrics for all zones, the current advertisement state, and hit counts. You can retrieve this database by using the **proximity retrieve** command.

proximity commit {*ip_address ip_prefix*|**entire-db**
{**ftp** *ftp_record ftp_filename* {**bin**}|**log** *filename* {**bin**}}}

Syntax Description

ip_address ip_prefix	(Optional) IP address and IP prefix length for the assignments you want to remove. Enter the address in dotted-decimal format (for example, 192.168.11.1). Enter the prefix as either: • A prefix length in CIDR bitcount notation (for example, /24). • A subnet mask in dotted-decimal notation (for example, 255.255.255.0).
entire-db	(Optional) Commits the entire Proximity Database when you want to use additional options to: • Assign a specific name to the database file written to the disk other than the default filename, proximity.db. • Write the database file to an FTP server. By default, the file is written to the CSS disk. • Save the database in binary format. By default, the file is in XML-format.
ftp *ftp_record ftp_filename*	(Optional) Writes a specified file to an FTP server. Enter the name of an existing FTP record for an FTP server. The FTP record file contains the FTP server IP address, username, and password. To create an FTP record, use the **(config) ftp-record** command. Also enter the filename to use when storing the Proximity Database to an FTP server.

log *filename*	(Optional) Writes a specified file to the log directory on the CSS disk. Enter a filename with a maximum of 32 characters. By default, the filename is proximity.db.
bin	(Optional) Stores the database file in compact binary format to disk or an FTP server.

Command Modes

SuperUser

Usage Guidelines

By default, when you enter the **proximity commit** command without any of its options, it writes the entire database to an XML-formatted file named proximity.db in the log directory on the CSS disk. You can optionally have the database encoded using compact binary encoding. You can also have the database written to a file on an FTP server.

Note A binary-encoded database occupies approximately one-third less space than an XML-formatted database.

The **proximity commit** command is functional only on a Proximity Database CSS in a dedicated CSS 11150 with 256 MB of RAM.

Related Commands

proximity retrieve

proximity refine

To initiate automatic or manual refinement of metric entries in the Proximity Database, use the **proximity refine** command. The refinement process updates the metric entries for all clients in the database. To view the automatic probe rates on the CSS, use the **show proximity refine** command. Use the **no** form of this command to stop the automatic refinement process.

proximity refine {**once**}

no proximity refine

Syntax Description

once	(Optional) Initiates the refinement process of metric entries manually. The refinement process occurs only once.

Command Modes

SuperUser

Usage Guidelines

The **proximity refine** command is functional only on a Proximity Database CSS in a dedicated CSS 11150 with 256 MB of RAM.

Related Commands

show proximity refine

proximity reprobe

To reprobe existing IP addresses, use the **proximity reprobe** command. You can use this command to perform an immediate refresh of information contained within the database.

proximity reprobe *ip_address* {*ip_prefix*}

Syntax Description

ip_address	IP address to reprobe. Enter the address in dotted-decimal format (for example, 192.168.11.1).
ip_prefix	(Optional) IP prefix to associate with *ip_address* to perform probing for a block of addresses. Enter the prefix as either: • A prefix length in CIDR bitcount notation (for example, /24). • A subnet mask in dotted-decimal notation (for example, 255.255.255.0).

Command Modes

SuperUser

Usage Guidelines

The **proximity reprobe** command is functional only on a Proximity Database CSS in a dedicated CSS 11150 with 256 MB of RAM.

Note IP addresses configured with the **proximity assign** command are not eligible for reprobing.

proximity retrieve

To load a Proximity Database file from the CSS disk or an FTP server, use the **proximity retrieve** command. The proximity metrics from the database file replace any overlapping existing entries and supplement any non-overlapping entries.

proximity retrieve {**ftp** *ftp_record ftp_filename*|**log** *filename*}

Syntax Description

ftp *ftp_record ftp_filename*	(Optional) Retrieves a file to an FTP server. Enter the name of an existing FTP record for an FTP server. The FTP record file contains the FTP server IP address, username, and password. To create an FTP record, use the **(config) ftp-record** command. Also enter the Proximity Database filename locates on the FTP server.
log *filename*	(Optional) Retrieves a specified file other than the proximity.db file from the log directory on the CSS disk.

Command Modes

SuperUser

Usage Guidelines

By default, when you enter the **proximity retrieve** command without any of its options, it loads the proximity.db database file from the CSS disk. Optionally, you can load a specific database file from the disk or from an FTP server. This command can distinguish between XML and binary database formats automatically.

The **proximity retrieve** command is functional only on a Proximity Database CSS in a dedicated CSS 11150 with 256 MB of RAM.

rcmd

To issue remote CLI commands to a CSS peer, use the **rcmd** command.

rcmd *ip_or_host* **"***CLI_command* {**;***CLI_command...*}**"** {*timeout_response*} {*script_filename*}

Syntax Description

ip_or_host	IP address for the peer. Enter the address in dotted-decimal format (for example, 192.168.11.1) or mnemonic host-name format (for example, myname.mydomain.com).
"*CLI_command***"**	One or more CLI commands you want to issue to the peer. Enter the command, its options, and variables exactly. Enclose the command text string in quotes (""). When entering multiple CLI commands, insert a semicolon (;) character to separate each command.
timeout_reponse	(Optional) Amount of time, in seconds, to wait for the output command response from the peer. Enter an integer from 3 to 300 (5 minutes). The default is 3 seconds.
script_filename	(Optional) Script filename where you want the output to direct when you enter the **rcmd** command. Enter an unquoted text string with no spaces and a maximum of 32 characters. The CSS saves the script in the /scripts directory on the CSS. If you do not include a filename, the CSS directs the output to the screen where you entered the **rcmd** command.

Command Modes

SuperUser

Usage Guidelines

By default, the APP session is configured to allow the CSS to send remote commands to a CSS peer. If this function is disabled, use the **(config) app session** command to enable it.

You cannot issue **grep**, **grep** within a script command, or redirect commands through the **rcmd** command.

Related Commands

(config) app

redundancy force-master

To force the backup CSS to be the master CSS, use the **redundancy force-master** command.

redundancy force-master

Command Modes

SuperUser

Usage Guidelines

You can enter the **redundancy force-master** command on the backup CSS if you did not explicitly designate the master CSS by using the **(config) ip redundancy master** command. If you did, you must unassign the master CSS by using the **(config) no ip redundancy master** command before you can enter the **redundancy force-master** command.

The forced-master CSS remains the master until it goes down and comes back up as the backup, or you manually make the other CSS the master.

The **redundancy force-master** configuration information is not saved to the running configuration.

If you want to designate the other CSS as the master, enter either of the following commands on the current backup CSS:

- Enter the **redundancy force-master** command if you want the current backup CSS to be a negotiated master. If a negotiated master CSS goes down, the backup CSS automatically becomes the master. When the former master CSS comes up again, it becomes the backup CSS.

- Enter the **ip redundancy master** command if you want the current backup to be the designated master. If the designated master CSS goes down and then comes up again, it regains its master status. For example, when the designated master CSS goes down, the backup CSS becomes the master. When the designated master CSS comes up again, it becomes the master again.

Related Commands

show redundancy
(config) ip redundancy

replicate

To start replicating between a publisher and all associated subscribers, use the **replicate** command.

replicate *publisher_name* {*subscriber_name* {**force**}}

Syntax Description

publisher_name	(Optional) Name of an existing publisher service. Resynchronizes any changes to content between the specified publisher and its subscriber services. If the content has not changed, no resynchronization occurs.
subscriber_name	(Optional) Name of the subscriber service associated with the publisher service. Resynchronizes any changes to content between the specified publisher and the specified subscriber service. If the content has not changed, no resynchronization occurs.
force	(Optional) Resynchronizes all content between the specified publisher and the specified subscriber service, whether or not content changes have occurred.

Command Modes

SuperUser

Usage Guidelines

You can use the **replicate** command to replicate content to new subscribers or force resynchronization immediately.

When you configure content replication and staging, you must configure an URL in a content rule to define which files you want replicated. Add the subscriber services to the content rule.

Note If you want all files in all directories replicated, you do not need to create a content rule. Create a content rule to specify only those files you want replicated.

Related Commands

(config-owner-content) url
(config-service) publisher
(config-service) subscriber

## restore

To restore a log, script, or startup configuration files that were previously archived on the CSS, use the **restore** command. The archive directory on the CSS disk stores the archive files.

restore *archive_filename* [**log** {*log_filename*}
|**script** {*script_filename*}|**startup-config**]

Syntax Description

archive_filename	Name of the archived file. Enter an unquoted text string. To see a list of archived files, enter: # **restore ?**
log	Restores an archived file to the log directory.
log_filename	(Optional) Name you want to assign to the restored log file. Enter an unquoted text string with a maximum length of 32 characters.
script	Restores an archived file to the script directory.

script_filename	(Optional) Name you want to assign to the script file. Enter an unquoted text string with a maximum length of 32 characters.
startup-config	Restores an archived file to the startup configuration. The restored file overwrites the startup configuration.

Command Modes

All modes

Usage Guidelines

The archive directory resides on the CSS hard drive. If you booted your CSS from a network-mounted system and your hard drive is not functional, then archive- and restore-related functions are suspended.

Related Commands

archive
copy
script
(config) logging

script

To play or record a script, use the **script** command. For more information on scripts, refer to the *Cisco Content Services Administration Guide*.

script [**play** *script_name* {**"***argument***"**}|**record** *script_name*]

Syntax Description

play	Runs a script.
script_name	Name of the script file. Enter an unquoted text string with no spaces and a maximum of 32 characters. To see a list of script files in the script directory, enter: `# show script`
"*argument*"	(Optional) Argument, such as a variable, text string, or integer, that is used when you play the script. Enter a quoted string with a maximum length of 32 characters.
record	Records a script and saves it to disk.

Command Modes

SuperUser

Related Commands

clear
show script

# send-message

To send a message to a connected session, use the **send-message** command.

send-message *session* **"***message***"**

Syntax Description

session	Connected session or line where you want to send the message. To see a list of connected sessions, enter: `# send-message ?` An asterisk precedes your name in the list.
"*message*"	The message you want to send. Enter a quoted text string with a maximum length of 255 characters.

Command Modes

SuperUser

set

To create user-defined variables, use the **set** command. Typically, you use this command in a script. Use the **no** form of this command to delete a user-defined variable.

set *variable_name* **"***variable_value***"** {**session**}

no set *variable_name*

Syntax Description

variable_name	A character string representing the variable. Enter a string with a maximum length of 32 characters.
"*variable_value*"	A value assigned to the value. There are two types of variables, character and numeric: • To set a numeric variable, enter a quoted string of integers with no spaces. • To set a character variable, enter a quoted string of text characters, integers, and spaces with a maximum length of 128 characters.
session	(Optional) Specifies that this is a session variable. When you save a session variable in a profile script, this variable is created each time a user creates a session.

Command Modes

All modes

Related Commands

modify
show
show variable

show

To display current system information, use the **show** command. The options for this command are:

show acl	Displays access control lists (ACLs)
show aliases	Displays alias commands
show app	Displays Application Peering Protocol (APP) configuration and session information
show app-udp	Displays Application Peering Protocol-UDP (APP-UDP) global statistical information and security configuration settings
show archive	Displays the contents of an archive directory or file
show arp	Displays ARP information
show boot-config	Displays system boot configuration
show bridge	Displays the bridge forwarding table and status, and Port Fast status
show cdp	Displays the global Cisco Discovery Protocol (CDP) information for the CSS
show chassis	Displays the chassis configuration
show circuits	Displays circuit information
show clock	Displays the current time and date on the CSS
show cmd-sched	Displays the state of the command scheduler and information about the scheduled CLI command records
show content	Displays all content entries in the CSS
show core	Displays core dump information
show critical-services	Displays critical services
show dfp	Displays the configuration information for the DFP agents on a CSS
show dfp-reports	Displays the individual weights of load-balanced server/services reported by a configured DFP agent

show dhcp-relay-agent global	Displays disk information
show disk	Displays information about the CSS disk
show disk_slot	Displays the specified archive, log, script, or startup configuration file stored on a specific disk in the CSS
show dns-boomerang client	Displays domain information mapped to a record on the CSS serving as a Content Routing Agent (CRA) for a Cisco Content Router 4430B
show dns-peer	Displays Domain Name System (DNS) peer configuration information
show dns-record	Displays information about the address/name server (A/NS) records configured locally and learned by this CSS
show dns-server	Displays DNS configuration and database information
show domain	Displays the content domain summary information
show dormant flows	Displays dormant flows on the CSS
show dos	Displays detailed information about Denial of Service (DoS) attacks on each CSS Switch Fabric Processor (SFP)
show dql	Displays the domain qualifier lists (DQLs)
show eql	Displays the extension qualifier lists (EQLs)
show ether-errors	Displays the error counters on the Ethernet interfaces
show flow-state-table	Displays the currently configured TCP and UDP ports, their flow states, and their NAT states
show flow-timeout	Displays the default and configured flow timeout values on the CSS
show flows	Displays the flow summary for a source IP address or for a specific source address and its destination IP address on an SFP
show global-portmap	Displays the statistics for global port mapping on a CSS

show group	Displays groups
show gsdb	Displays global sticky database (GSDB) statistics
show gsdb-interface	Displays statistics for the GSDB interface on the CSS
show header-field-group	Displays header-field group information
show history	Displays session command history
show installed-software	Displays currently installed CSS software
show interface	Displays interface information
show ip config	Displays IP global configuration parameters
show ip firewall	Displays configured values of the IP firewall keepalive timeout and the state of each firewall path configured on the CSS
show ip interfaces	Displays configured IP interfaces
show ip routes	Displays IP routing information
show ip statistics	Displays aggregate UDP and TCP statistics for the CSS
show ip summary	Displays a summary of IP global statistics
show isc-ports	Displays Inter-Switch Communications information on the CSS
show keepalive	Displays keepalive status and configuration information
show keepalive-summary	Displays summary information for all keepalives
show lines	Displays currently connected users
show load	Displays the global load configuration on the CSS and the load information for services
show log	Displays a log file
show log-list	Displays a list of all log files
show log-state	Displays logging information
show map	Displays the mapping configuration of the disks in the CSS (installed in slot 0 and slot 1)
show mibii	Displays MIB-II counters

show noflow-portmap	Displays statistics for noflow port mapping on a CSS
show nql	Displays general information about network qualifier lists (NQLs)
show ospf	Displays Open Shortest Path First (OSPF) information
show owner	Displays owner information
show phy	Displays duplex, speed, and descriptions for all interfaces
show profile	Displays the running user profile
show proximity	Displays the activity summary of the proximity database
show proximity assign	Displays the metric assignment of all zones or for a configured IP address range
show proximity cache	Displays the current state of the proximity cache
show proximity metric	Displays proximity metrics associated with client IP addresses
show proximity probe rtt statistics	Displays the round-trip time (RTT) probe module statistics
show proximity refine	Displays information pertaining to a refinement operation in progress for entries in the Proximity Database
show proximity statistics	Displays statistics associated with client IP addresses
show proximity zone	Displays state information for each zone
show publisher	Displays information about publishing services
show radius config	Displays CSS configuration information for the primary and secondary RADIUS servers,
show radius stat	Displays authentication statistics for the primary and secondary RADIUS servers
show redundancy	Displays CSS-to-CSS redundancy status
show redundant-interfaces	Displays a list of all redundant virtual interfaces configured on the CSS
show redundant-vips	Displays a list of all redundant VIPs configured on the CSS

show remap	Displays the configured persistence reset and bypass settings
show rip	Displays global or interface Routing Information Protocol (RIP) statistics and RIP configuration
show rmon	Displays RMON statistics
show rmon-history	Displays RMON history information for Ethernet interfaces in the CSS
show rule	Displays content rules
show rule-summary	Displays a summary of all content rules for all owners
show running-config	Displays the running configuration
show script	Displays a specific script
show service	Displays services
show session-redundant	Displays session redundancy information for the CSS
show sntp global	Displays Simple Network Time Protocol (SNTP) configuration information on the CSS
show sockets	Displays all the socket file descriptors that are currently in use
show sorted running-config	Displays the configuration elements contained within each mode entry in the running-configuration file in alphanumeric order
show sshd	Displays the Secure Shell Host (SSH) daemon configuration
show ssl	Displays SSL associations and statistics on the CSS
show ssl-proxy-list	Displays information about SSL proxy configuration lists
show startup-config	Displays system startup configuration
show startup-errors	Displays errors occurring during startup configuration
show sticky-table all-sticky	Displays all entries of the CSS sticky table based on the advanced load-balancing method for a content rule

show sticky-table l3-sticky	Displays the L3 entries of the CSS sticky table
show sticky-table l4-sticky	Displays the L4 entries of the CSS sticky table
show sticky-table sip-callid-sticky	Displays entries in the sticky table based on Call-ID
show sticky-table ssl-sticky	Displays the SSL entries of the CSS sticky table
show sticky-table wap-sticky	Displays the WAP MSISDN entries of the CSS sticky table
show sticky-stats	Displays a summary of sticky connection statistics for the CSS
show subscriber	Displays information about subscriber services
show summary	Displays summary of relationship between owners, content rules, and services
show system-resources	Displays the CSS installed and available memory
show tacacs-server	Displays the TACACS+ server configuration information
show trunk	Displays VLAN trunk information on configured Gigabit Ethernet ports and their VLANs
show uptime	Displays how long the CSS unit has been running
show urql	Displays general information about the Uniform Resource Locator qualifier list (URQL)
show user-database	Displays configured users
show variable	Displays user variables
show version	Displays the software version on the CSS
show virtual-routers	Displays all virtual routers configured on the CSS
show zone	Displays the current state of each Proximity CAPP Messaging (PCM) negotiation

For more information on these commands and any associated options, see the following commands.

show acl

To display the access control lists (ACLs) and clauses on the CSS, use the **show acl** command. This command also displays the ACL logging state, and displays all circuits with their associated ACLs.

show acl {*index*|**config**}

Syntax Description

index	(Optional) Index number associated with the ACL. Displays the clauses for the specified ACL index number.
config	(Optional) Displays all ACLs, the ACL logging state, and all circuits with their associated ACLs.

Command Modes

All modes

Usage Guidelines

The **show acl** command without an option lists all ACLs and their clauses configured on the CSS.

For information about the fields in the **show acl** command output, refer to the *Cisco Content Services Switch Security Configuration Guide*.

Related Commands

(config) acl
(config-acl) apply
(config-acl) clause
(config-acl) zero counts

show aliases

To display alias commands and associated CLI commands for the current mode or all modes, use the **show aliases** command.

show aliases {**all**}

Syntax Description

all	(Optional) Displays all alias commands for all modes

Command Modes

All modes

Usage Guidelines

The **show aliases** command without an option displays the alias commands and associated CLI commands for the current mode.

Related Commands

alias

show app

To display the Application Peering Protocol (APP) configuration or session information, use the **show app** command. APP is the method in which private communications links are configured between CSSs in the same content domain. A content domain consists of a group of CSSs configured to exchange content information.

show app {**session**|*ip_address*} {**verbose**}

Syntax Description

session	(Optional) Displays the IP session information including the session ID, IP address, and state.
ip_address	(Optional) IP address for a specified peer CSS to display its session information. Enter the address in dotted-decimal format (for example, 192.168.11.1).
verbose	(Optional) Displays detailed information about the IP configuration parameters for the session including the local address, keepalive frequency, authorization and encryption type, frame size, packet activity, and FSM events.

Command Modes

All modes

Usage Guidelines

The **show app** command without an option displays whether APP is enabled, its port number, and frame size setting.

For information about the fields in the **show app** command output, refer to the *Cisco Content Services Switch Global Server Load-Balancing Configuration Guide*.

Related Commands

(config) app

show app-udp

To display the Application Peering Protocol-User Datagram Protocol (APP-UDP) global statistical information and security configuration settings, use the **show app-udp** command.

show app-udp [**global**|**secure**]

Syntax Description

global	Displays global statistical information about the operation of APP-UDP
secure	Displays the current security configuration settings for APP-UDP

Command Modes

All modes

Usage Guidelines

The **show app-udp** command is functional only on the Proximity Database and DNS CSSs.

For information about the fields in the **show app-udp** command output, refer to the *Cisco Content Services Switch Global Server Load-Balancing Configuration Guide*.

Related Commands

(config) app-udp

## show archive

To display the files in the archive directory or the contents of an archive file, use the **show archive** command. Archive files include running- and startup-config files, scripts, and user profiles.

show archive {*filename*}

Syntax Description

filename	(Optional) Name of the archive file you want to display. Enter the filename as an unquoted string. To see a list of archive files, enter: `# show archive ?`

Command Modes

SuperUser and all configuration modes

Related Commands

archive

show arp

To display ARP information, use the **show arp** command.

show arp {**config**|**file**|**management-port**|**summary**|*ip_or_host*}

Syntax Description

config	Displays ARP global configuration parameters. The screen displays the response timeout in seconds and the flush timeout in seconds.
file	Displays the host IP addresses entered at initialization or boot time through ARP.
management-port	Displays the ARP entries from the CSS management port.

summary	Displays the total number of static, dynamic, and all entries in the ARP resolution table. The summary does not include the entries from the CSS management port.
ip_or_host	IP address for the system to display its resolution. Enter the address in dotted-decimal format (for example, 192.168.11.1) or mnemonic host-name format (for example, myname.mydomain.com). You cannot enter an ARP entry derived from the CSS management port.

Command Modes

All modes

Usage Guidelines

The **show arp** command without an option displays the complete ARP resolution table with IP addresses, MAC addresses, and resolution type. The ARP resolution table does not include entries from the CSS Ethernet management port.

For information about the fields in the **show arp** command output, refer to the *Cisco Content Services Switch Routing and Bridging Configuration Guide*.

Related Commands

clear
update arp

show boot-config

To display the CSS boot configuration, use the **show boot-config** command.

show boot-config

Command Modes

All modes

Related Commands

(config-boot) gateway address
(config-boot) ip address
(config-boot) primary
(config-boot) subnet mask

## show bridge

To display the bridging information, use the **show bridge** command.

show bridge [**forwarding** {*vlan_number*}|**status** {*vlan_number*}|**port-fast**]

Syntax Description

forwarding	Displays the bridge forwarding table including the VLAN number, the MAC addresses, and port numbers.
status	Displays the bridge spanning-tree status including the STP state, designated root, bridge ID, and root maximum age, hello time and forward delay, and port information including state, VLAN, root and port cost, and designated root and port number.
vlan_number	Displays the forwarding table or spanning tree status for the specified VLAN number. To see a list of VLAN numbers, enter: `# show bridge [forwarding|status] ?`

port-fast	Displays whether portfast is enabled or disabled on the CSS interfaces. This command also displays whether the Bridge Protocol Data Unit (BPDU) guard feature is enabled or disabled on the CSS, and the state of the interfaces.

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show bridge** command output, refer to the *Cisco Content Services Switch Routing and Bridging Configuration Guide*.

Related Commands

(config) bridge bpdu-guard
(config-if) bridge port-fast

show cdp

To display the global Cisco Discovery Protocol (CDP) information for the CSS, use the **show cdp** command. The information includes the frequency of CDP advertisements, the hold time value, and the last time that a CDP advertisement was sent.

show cdp

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show cdp** command output, refer to the *Cisco Content Services Switch Routing and Bridging Configuration Guide*.

Related Commands

(config) cdp

# show chassis

To display the chassis configuration for all CSSs and the weight and power summary of the session processors on the modules, use the **show chassis** command.

show chassis {**flash**|**inventory**|**session-processors**|**slot** *number*|**verbose**}

Syntax Description

flash	Displays the operational and locked flash version for the CSS 11501, and the CSS 11503 or 11506 SCM and I/O modules. A "*" character before a flash version and build number indicates it is the active flash.
inventory	Displays the physical configuration of the CSS including its part and serial numbers for each component.
session-processors	Displays the weight and power summary of the session processors on the modules in the CSS chassis.
slot *number*	Displays the operational parameters for a slot in a CSS 11503 or 11506. Enter an integer value. To see a list of slots, enter: `# show chassis slot ?`
verbose	Displays detailed information about the chassis configuration.

Command Modes

All modes

Usage Guidelines

The **show chassis** command without an option displays a summary of the chassis configuration.

For information about the fields in the **show chassis** command output, refer to the *Cisco Content Services Switch Administration Guide*.

show circuits

To display circuit information, use the **show circuits** command. A circuit on the CSS is a logical entity that maps IP interfaces to a logical port or group of logical ports.

show circuits {**all**|**name** circuit}

Syntax Description

all	(Optional) Lists all circuits, their states, and their interfaces, regardless of their state
name *circuit*	(Optional) Displays the state and interface information for the specified circuit

Command Modes

All modes

Usage Guidelines

Use the **show circuits** command to list all circuits, their states, and any of their interfaces in the Up state.

Use the **show circuits all** command to list all circuits, their states, and their interfaces, regardless of their state.

For information about the fields in the **show circuits** command output, refer to the *Cisco Content Services Switch Routing and Bridging Configuration Guide*.

show clock

To display the current time and date on the CSS, use the **show clock** command.

show clock

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show clock** command output, refer to the *Cisco Content Services Switch Getting Started Guide*.

Related Commands

clock
(config) date european-date

show cmd-sched

To display the state of the command scheduler and information about the records for the scheduled CLI commands, use the **show cmd-sched** command.

show cmd-sched {**name** record_name}

Syntax Description

name *record_name*	(Optional) Lists information about the specified scheduled CLI command record

Command Modes

All modes

Usage Guidelines

The **show cmd-sched** command without an option displays the command scheduler state and all scheduled CLI command records.

For information about the fields in the **show cmd-sched** command output, refer to the *Cisco Content Services Switch Administration Guide*.

Related Commands

(config) cmd-sched

show content

To display all content entries in the Content Service Database (CSD) for a CSS, use the **show content** command.

show content {*slot_number* {**start-index** *index_number*}}

Syntax Description

slot_number	(Optional) For a CSS 11503 or 11506 only. Displays content from the module located in a specific CSS slot. For the CSS 11503, the available choices are 1 through 3; for the CSS 11506, the available choices are 1 through 6.
start-index *index_number*	(Optional) Displays content entries starting at the specified index number, a maximum of 64k of information. To specify an index number, enter a number from 0 to 4095. To see additional information, enter the **show content** command again, starting from the last displayed index number. If you do not enter the **start-index** option and variable, the displayed entries start at index 0.

Command Modes

All modes

Usage Guidelines

To show all content entries in the Content Service Database for a CSS, use the **show content** command without an option.

For information about the fields in the **show content** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config-owner) content

show core

To display the core dump files stored in the Core directory of the volume root (for example, c:\core) on the hard disk or flash disk, use the **show core** command. If the CSS has two disks, you can display the core files on either disk.

show core {*disk_slot*}

Syntax Description

disk_slot	(Optional) Slot location of a disk in the CSS. The valid entries are: • **0** - The disk in slot 0 • **1** - The disk in slot 1

Command Modes

SuperUser and all configuration modes

Usage Guidelines

Core dump information is for customer support use only.

Related Commands

copy core
(config) dump

show critical-reporter

To display critical reporter configuration information, use the **show critical-reporter** command.

show critical-reporter

Usage Guidelines

For information about the fields in the **show critical-reporter** command output, refer to the *Cisco Content Services Switch Redundancy Configuration Guide*.

Command Modes

All modes

Related Commands

show reporter
(config) reporter

show critical-services

To display a list of all critical services configured on the CSS, use the **show critical-services** command. You can provide an interface IP address option to display only the critical services present on a particular interface. You can also include a virtual router identifier (VRID) to display only the critical service information for a particular virtual router.

show critical-services {*ip_address* {*vrid*}}

Syntax Description

ip_address	(Optional) Address for the redundant interface. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1).
vrid	(Optional) ID for an existing virtual router.

Command Modes

All modes

Usage Guidelines

The **show critical-services** command without an option displays all critical services on the CSS.

For information about the fields in the **show critical-services** command output, refer to the *Cisco Content Services Switch Redundancy Configuration Guide*.

Related Commands

(config-circuit-ip) ip critical-service

show dfp

To display the configuration information for the DFP agents on a CSS, use the **show dfp** command. This command displays a list of either all DFP agents or the DFP agents at the specified IP address or host name arranged by their IP-addresses. Also listed are the port number on which the agent is connected to the DFP manager, the current state of the DFP agent, the keepalive time for the DFP TCP connection, and the DES-encrypted key of the agent, if any.

show dfp {*ip_or_host*}

Syntax Description

ip_or_host	(Optional) Displays the DFP agent or agents running at a specific IP address or host name

Command Modes

All modes

Usage Guidelines

The **show dfp** command without an option displays configuration information for all DFP agents.

For information about the fields in the **show dfp** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config) dfp

show dfp-reports

To view the individual weights of load-balanced services reported by a configured DFP agent, use the **show dfp-reports** command. This command groups the weights by the port number of reported services, the type of protocol, and the IP address of servers.

show dfp-reports {*ip_or_host* {**port** *number* {**protocol** *text* {**ip** *ip_or_host2*}}}}

Syntax Description

ip_or_host	(Optional) IP address or host name of the configured DFP agent. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or a mnemonic host name (for example, myhost.mydomain.com).
port *number*	(Optional) Port number of the load-balanced server or service.
protocol *text*	(Optional) Type of protocol for the load-balanced server or service. Possible values are TCP, UDP, HTTP, or FTP.
ip *ip_or_host2*	(Optional) IP address or host name of the load-balanced service. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or a mnemonic host name (for example, myhost.mydomain.com).

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show dfp-reports** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config) dfp

show dhcp-relay-agent global

To display the Dynamic Host Configuration Protocol (DHCP) configuration information on the CSS, use the **show dhcp-relay-agent global** command.

show dhcp-relay-agent global

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show dhcp-relay-agent global** command output, refer to the *Cisco Content Services Switch Routing and Bridging Configuration Guide*.

Related Commands

(config) dhcp-agent max-hops
(config-circuit) dhcp relay-to
(config-circuit) dhcp-relay-agent

show disk

To display information about the CSS disk, use the **show disk** command. The information includes the size of the disk, the space available, and the number of files, directories, and bad clusters on it. If you have two disks in the CSS, you can display information about either disk.

show disk {*disk_slot*}

Syntax Description

disk_slot	(Optional) Slot location of a disk in the CSS. The valid entries are: • **0** - The disk in slot 0 • **1** - The disk in slot 1

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show disk** command output, refer to the *Cisco Content Services Switch Administration Guide*.

show *disk_slot*

To display the specified archive, log, script, or startup configuration file stored on a specific disk in the CSS, use the **show** *disk_slot* command.

show *disk_slot* [**archive** *filename*|**log** *filename*|**script** *filename* |**startup-config**]

Syntax Description

disk_slot	CSS disk location containing the file you want to display. The valid entries are: • **0** - The disk in slot 0 • **1** - The disk in slot 1
archive *filename*	Displays the content of the specified archive file.
log *filename*	Displays the contents of the specified log file.
script *filename*	Displays the contents of the specified script file.
startup-config	Displays the contents of the startup configuration.

Command Modes

All modes

## show dns-boomerang client

To display domain information mapped to a record on the CSS serving as a Content Routing Agent (CRA) for a Cisco Content Router 4430B, use the **show dns-boomerang client** command.

show dns-boomerang client {**all**|**domain** {*name*}|**global**}

Syntax Description

client	Shows all statistics for all domains mapped to a client record including global statistics.
all	(Optional) Shows all statistics for all domains mapped to a client record including global statistics.
domain	(Optional) Shows the statistics for all domains mapped to a client record. It does not display the global statistics.
domain_name	(Optional) Specific domain name associated with the statistics you wish to view. It does not display the global statistics. To view a list of domain names, enter: `# show dns-boomerang client domain ?`
global	(Optional) Shows the global statistics for the CSS client.

Command Modes

All modes

Usage Guidelines

Entering the **show dns-boomerang client** command displays the same information as entering the **show dns-boomerang client all** command.

Use the **show dns-boomerang client global** command to display the following global statistics:

- Total DNS A-record requests
- Total packets dropped and its subfields

For information about the fields in the **show dns-boomerang client** command output, refer to the *Cisco Content Services Switch Global Server Load Balancing Configuration Guide*.

Related Commands

dns-boomerang client zero
(config) dns-boomerang client

show dns-peer

To display DNS peer configuration information, use the **show dns-peer** command. This command displays the time between sending load reports to CSS DNS peers and the maximum number of DNS names sent to (send slots) and received from (receive slots) CSS DNS peers.

```
show dns-peer
```

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show dns-peer** command output, refer to the *Cisco Content Services Switch Global Server Load-Balancing Configuration Guide*.

Related Commands

(config) app
(config) dns-peer

## show dns-record

To view information about the address/name server (A/NS) records configured locally and learned by the CSS, locally configured acceleration domain records, the DNS record keepalive and load information, and sticky domain records, use the **show dns-record** command.

show dns-record [**accel**|**keepalives**|**load**|**proximity**|**statistics**|**sticky**|**weight**] {*domain_name*}

Syntax Description

accel	Displays statistics associated with acceleration domain records.
keepalives	Displays information about keepalives associated with DNS records.
load	Displays load information associated with DNS records.
proximity	Displays the DNS record PDB hit and miss count information.
statistics	Displays the DNS record statistics.
sticky	Displays statistics associated with sticky domain records.
weight	Displays the configured weight and the number of hits for all domains or the specified domain.
domain_name	(Optional) Specific domain name associated with the DNS record you wish to view. Enter the name as a lower case unquoted text string with no spaces and a maximum of 63 characters. If omitted, the CSS displays all domains. To see a list of domains, enter: `# show dns-record [accel|keepalives|proximity |statistics|sticky|weight] ?`

Command Modes

All modes

Usage Guidelines

The **show dns-record** command is functional only on a CSS with the Enhanced feature set.

For information about the fields in the **show dns-record** command output, refer to the *Cisco Content Services Switch Global Server Load-Balancing Configuration Guide*.

Related Commands

(config) dns-record

show dns-server

To display DNS server configuration and database information, use the **show dns-server** command. You can configure a CSS to send DNS requests to a DNS server on the network.

show dns-server {**accelerate domains**|**dbase**
|**domain-cache** {**summary**}|**forwarder**|**stats**}

Syntax Description

accelerate domains	(Optional) Displays the configuration information for the Client Side Accelerator (CSA) on the CSS
dbase	(Optional) Displays the entries in the DNS database as a result of local configuration of DNS names for content rules or learned DNS names from peer members of the content domain
domain-cache	(Optional) Displays the domain-cache counters and entries
summary	(Optional) Displays the domain-cache counters only
forwarder	(Optional) Displays the statistics on the CSS for the DNS server forwarders
stats	(Optional) Displays the DNS database statistics

Command Modes

All modes

Usage Guidelines

The **show dns-server** command without an option displays the current DNS server configuration on the CSS and statistics about requests and responses. For information about the fields in the **show dns-server** command output, refer to the *Cisco Content Services Switch Global Server Load-Balancing Configuration Guide*.

If the NS Buffers Free or Minimum fields drop below two, increase the responder tasks and buffer counts, and observe the effects on these fields. See the **(config) dns-server** command.

Related Commands

(config) dns-server
(config) dns-server accelerate domains
(config) dns-server domain-cache
(config) dns-server zero

show domain

To display content domain summary information or specified domain information, use the **show domain** command. A content domain is a group of CSSs sharing the same content rules, load, and DNS information with each other.

show domain {*ip_address* {**send**|**receive**}|**hotlist**|**owners** {*ip_address*}|**rules** {*ip_address*}}

Syntax Description

ip_address	The IP address for the peer. Enter the address in dotted-decimal format (for example, 192.168.11.1).
send	Displays only the send load reports and transmit message statistics.
receive	Displays only the receive load reports and receive message statistics.
hotlist	Displays the domain hot list configuration and hit information for domains.
owners	Displays shared owner names.
rules	Displays locally created or negotiated content rule names.

Command Modes

All modes

Usage Guidelines

The **show domain** command without an option displays content domain summary information including the number of domain peers and information about each peer.

For information about the fields in the **show domain** command output, refer to the *Cisco Content Services Switch Global Server Load-Balancing Configuration Guide*.

Related Commands

(config) app session
(config) domain hotlist

show dormant flows

To display the dormant flows in an ASR configuration on the CSS, use the **show dormant flows** command. Dormant flows are flows on the backup CSS that become active if the master CSS fails over and the backup CSS assumes mastership.

show dormant flows {*source_address* {*destination_address*}}

Syntax Description

source_address	(Optional) Source IP address for the flows. Enter the address in dotted-decimal format (for example, 192.168.11.1).
destination_address	(Optional) Destination IP address. Enter the address in dotted-decimal format (for example, 192.168.11.1).

Command Modes

All modes

Usage Guidelines

The **show dormant flows** command without an option displays all dormant flows.

For information about the fields in the **show dormant flows** command output, refer to the *Cisco Content Services Switch Global Server Load-Balancing Configuration Guide*.

show dos

To display detailed information about Denial of Service (DoS) attacks on each CSS session processor (SP) or Switch Fabric Processor (SFP), use the **show dos** command.

show dos {**summary**}

Syntax Description

summary	(Optional) Displays a summary of DoS attacks. The summary includes the total number of attacks, the attack types with their maximum occurrences per second, and the first and last occurrence of an attack.

Command Modes

All modes

Usage Guidelines

Use the **show dos** command to display the following information:

- The total number of attacks since the CSS was booted.
- The types of attacks and the maximum number of these attacks per second.
- The first and last occurrence of an attack.
- The source and destination IP addresses.

A CSS can display a maximum of 50 of the most-recent attack events per SFP or SP. For example:

- A CSS 11501 with one SP can display a maximum of 50 events.
- A CSS 11503 with a maximum of three SPs can display a maximum of 150 events.
- A CSS 11506 with a maximum of six SPs can display a maximum of 300 events.

If multiple attacks occur with the same DoS type, and source and destination address, an attempt is made to merge them as one event. This reduces the number of displayed events.

For information about the fields in the **show dos** command output, refer to the *Cisco Content Services Switch Administration Guide*.

Related Commands

zero dos statistics
(config) snmp trap-type enterprise

## show dql

To display the attributes for the domain qualifier Lists (DQLs) or a specified DQL, use the **show dql** command. A DQL is a collection of domain names that you can assign to a content rule, instead of creating a rule for each address.

show dql {*dql_name*}

Syntax Description

dql_name	(Optional) Name of a specific DQL. To see a list of DQLs, enter: `# show dql ?`

Command Modes

All modes

Usage Guidelines

The **show dql** command without an option displays attributes for all DQLs.

For information about the fields in the **show dql** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config) dql

## show eql

To display the attributes for the extension qualifier lists (EQLs) or a specified EQL, use the **show eql** command. An EQL is a collection of file extensions for content requests joined together through content rules. The CSS uses this list to identify which requests to send to a service.

show eql {*eql_name*}

Syntax Description

eql_name	(Optional) Name of a specific EQL. To see a list of EQLs, enter: `# show eql ?`

Command Modes

All modes

Usage Guidelines

The **show eql** command without an option displays all EQLs and their extensions.

For information about the fields in the **show eql** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config) eql

## show ether-errors

To list the extended 64-bit statistics for errors on Ethernet interfaces in the CSS, use the **show ether-errors** command. The Enterprise ap64Stats MIB defines these statistics. To display the RFC 1398 32-bit statistics, include the **-32** suffix.

show ether-errors{**-32**} {*interface_name*}

Syntax Description

-32	Displays the RFC 1398 32-bit statistics.
interface_name	(Optional) Name of the physical Ethernet interface on the CSS. Enter a case-sensitive unquoted text string. To see a list of interfaces, enter: `# show ether-errors ?`

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show ether-errors** command output, refer to the *Cisco Content Services Switch Routing and Bridging Configuration Guide*.

Related Commands

clear

show flow-state-table

To display the CSS flow state table entries, use the **show flow-state-table** command. The table contains entries for TCP and UDP ports. Each port entry includes the protocol, flow state, NAT state (if applicable), and a hit counter.

show flow-state-table

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show flow-state-table** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config) flow-state
(config) zero flow-state-counters

show flow-timeout

To display the default and configured flow timeout values on the CSS, use the **show flow-timeout** command.

show flow-timeout default|configured

Syntax Description

default	Displays the default timeout values for TCP and UDP ports and applications. The default values are not user-configurable.
configured	Displays the configured flow timeouts. The command output includes the content rule or source group for which you configured the flow timeout value.

Command Modes

Global, Owner, SuperUser, and User modes

Usage Guidelines

For information about the fields in the **show flow-timeout** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config-group) flow-timeout-multiplier
(config-owner-content) flow-timeout-multiplier

show flows

To display the flow summary for a source IP address on a Switch Processor (SP) in the CSS, use the **show flows** command. This information allows you to view flows to ensure the proper operation of firewall load balancing.

show flows {*source_address* {*destination_address*}}

Syntax Description

source_address	(Optional) Source IP address for the flows. Enter the address in dotted-decimal format (for example, 192.168.11.1).
destination_address	(Optional) Destination IP address. Enter the address in dotted-decimal format (for example, 192.168.11.1).

Command Modes

All modes

Usage Guidelines

The **show flows** command allows you to display a maximum of 4096 flows per SP.

This information allows you to:

- Identify which firewall is used for a particular flow
- View flows to ensure the proper operation of firewall load balancing

For information about the fields in the **show flows** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config) ip firewall
(config) ip route

## show global-portmap

To display the statistics for global port mapping on the CSS, use the **global-portmap** command.

show global-portmap [**all-banks** [**all-sps**|**slot** *number1*]
|*bank_number* [**all-sps**|**slot** *number1*]]

Syntax Description

all-banks	Displays the global portmap information for all portmap banks (0 to 15).
all-sps	Displays the global portmap information for all session processors (SPs) on all modules in the CSS.
slot *number1*	Displays global portmap information for the module in the specified slot. For a CSS 11503, enter an integer from 1 to 3. For a CSS 11506, enter an integer from 1 to 6. To display the available active slots in the CSS, enter: `# show global-portmap all-banks slot ?`
bank_number	Displays the global portmap information for the specified bank number. Enter an integer from 0 to 15.

Command Modes

All modes except RMON, URQL, and VLAN configuration modes.

Usage Guidelines

For information about the fields in the **show global-portmap** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config) global-portmap

show group

To display a collection of groups or the attributes for a specified group, use the **show group** command. A group is a collection of local servers that initiate flows from within the local web farm.

show group {*group_name* {**portmap** {**all**|*ip_or_host*}}}

Syntax Description

group_name	(Optional) Displays the attributes for a specified group
portmap	(Optional) Displays the port mapping for the group
all	(Optional) Displays the port mapping for all VIP addresses of the source group port mapper
ip_or_host	(Optional) Displays the port mapping for the specified address of the source group port mapper

Command Modes

User, SuperUser, Global, and Group modes

Usage Guidelines

If you are in group mode, the **show group** command displays the attributes for the current group. The *group_name* variable is not applicable in group mode.

The **show group** command without an option displays a collection of groups and their attributes.

For information about the fields in the **show group** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config) group
(config-group) zero all

show gsdb

To display global sticky database (GSDB) statistics, use the **show gsdb** command.

show gsdb

Command Modes

All modes

Usage Guidelines

The **show gsdb** command functions only on a Proximity Database CSS in a dedicated CSS 11150.

To reset the statistics to zero, use the **(config) gsdb zero** command.

For information about the fields in the **show gsdb** command output, refer to the *Cisco Content Services Switch Global Server Load-Balancing Configuration Guide*.

Related Commands

(config) gsdb

show gsdb-interface

To display statistics for the global sticky database (GSDB) interface on the DNS server CSS, use the **show gsdb-interface** command.

show gsdb-interface

Command Modes

All modes

Usage Guidelines

The **show gsdb-interface** command is part of the Enhanced feature set and is available in all modes. This command is not available on a Proximity database (PDB) or a GSDB.

To reset the statistics to zero, use the **(config) gsdb-interface zero** command.

For information about the fields in the **show gsdb-interface** command output, refer to the *Cisco Content Services Switch Global Server Load-Balancing Configuration Guide*.

Related Commands

(config) gsdb-interface

show header-field-group

To display the configuration for all header-field groups or a specific group, use the **show header-field-group** command.

show header-field-group {**all**|*name*}

Syntax Description

all	(Optional) Displays detailed information about all configured header-field groups
name	(Optional) Displays detailed information about a specified header-field group

Command Modes

All modes

Usage Guidelines

The **show header-field-group** command without an option displays a summary of all configured header-field groups.

For information about the fields in the **show header-field-group** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config) header-field-group
(config-header-field-group) description
(config-header-field-group) header-field

show history

To display the session command history, use the **show history** command. The command-line history buffer stores CLI commands that you previously entered.

show history

Command Modes

All modes

Related Commands

history length

show installed-software

To display a list of currently installed CSS software versions on the CSS disk or the maximum number of software versions you can install on the disk, use the **show installed-software** command. If you have a CSS with two disks, you can display the software on either disk.

show installed-software {*disk_slot*|**version-limit**}

Syntax Description

disk_slot	(Optional) Slot location of the disk in the CSS you want to display. The valid entries are: • **0** - The disk in slot 0 • **1** - The disk in slot 1
version-limit	(Optional) Displays the maximum number of software versions you can install on the disk.

Command Modes

All modes

Usage Guidelines

The **show installed-software** command without an option displays a list of currently installed software on the CSS disk.

Related Commands

version

## show interface

To display information for all interfaces or a specific interface, use the **show interface** command. The interfaces include Ethernet, circuit, and console interfaces.

show interface {*interface_name*}

Syntax Description

interface_name	(Optional) Specific interface in the CSS. To see a list of interfaces in the CSS, enter: `# show interface ?`

Command Modes

All modes

Usage Guidelines

The **show interface** command without an option displays information about all interfaces in the CSS.

For information about the fields in the **show interface** command output, refer to the *Cisco Content Services Switch Routing and Bridging Configuration Guide*.

show ip config

To display IP global configuration parameters, use the **show ip config** command. The parameters shows the state (enabled or disabled) of the source route option, forward IP broadcasts, record route option, and IP route change logging. It also shows the value for the orphaned route timer and the type of Multiple Equal Cost Path algorithm.

show ip config

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show ip config** command output, refer to the *Cisco Content Services Switch Routing and Bridging Configuration Guide*.

Related Commands

(config) ip

show ip firewall

To display the configured values of the IP firewall keepalive timeout and the state of each firewall path configured on the CSS, use the **show ip firewall** command. The display includes the IP firewall keepalive timeout, firewall index, current state of the connection to the remote switch, next hop IP address, remote firewall IP address, length of time since the last keepalive message was transmitted, and length of time since the last keepalive message was transmitted.

show ip firewall

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show ip firewall** command output, refer to the *Cisco Content Services Switch Routing and Bridging Configuration Guide*.

Related Commands

(config) ip

show ip interfaces

To display configured IP interfaces, use the **show ip interfaces** command. The display includes the circuit name and state, IP address, network mask, broadcast address, redundancy, Internet Control Message Protocol (ICMP) settings, and RIP settings.

show ip interfaces

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show ip interfaces** command output, refer to the *Cisco Content Services Switch Routing and Bridging Configuration Guide*.

Related Commands

(config) ip

show ip routes

To display all or specified IP routing information, use the **show ip routes** command.

show ip routes {**local**|**firewall**|**ospf**|**rip**|**static**|**summary**|*ip_or_host* {**to** *ip_or_host*|*mask_or_prefix*}}

Syntax Description

local	(Optional) Displays all local routes.
firewall	(Optional) Displays all firewall routes.
ospf	(Optional) Displays all OSPF routes.
rip	(Optional) Displays all RIP routes.
static	(Optional) Displays all static routes.
summary	(Optional) Displays the number of OSPF (including a breakdown of Intra, Inter, and Ext routes), RIP, local, static, and firewall routes, and the total number of routes.

to	(Optional) Displays information about a route to a destination, a specific route, or routes in a range.
ip_or_host	(Optional) IP address of the host or network prefix. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1). The IP address after the **to** keyword is the last IP address in a range.
mask_or_prefix	(Optional) Subnet address of the specific network. Enter the subnet address in mask or prefix notation (for example, /24).

Command Modes

All modes

Usage Guidelines

The **show ip routes** command without an option displays all routes on the CSS.

For information about the fields in the **show ip routes** command output, refer to the *Cisco Content Services Switch Routing and Bridging Configuration Guide*.

Related Commands

(config) ip

show ip statistics

To display the aggregate TCP statistics for the CSS, use the **show ip statistics** command. These statistics include UDP, TCP, ICMP, and ARP statistics.

show ip statistics

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show ip statistics** command output, refer to the *Cisco Content Services Switch Routing and Bridging Configuration Guide*.

Related Commands

zero ip statistics
(config) ip

show ip summary

To display a summary of IP global statistics, use the **show ip summary** command. The statistics include data on reachable and total routes, reachable and total hosts, memory in use for each, and total IP routing memory in use.

show ip summary

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show ip summary** command output, refer to the *Cisco Content Services Switch Routing and Bridging Configuration Guide*.

Related Commands

(config) ip

show ip-fragment-stats

To display the status, statistics, and error counts associated with IP fragment processing, use the **show ip-fragment-stats** command.

show ip-fragment-stats

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show ip-fragment-stats** command output, refer to the *Cisco Content Services Switch Routing and Bridging Configuration Guide*.

Related Commands

zero ip-fragment-stats
(config) ip-fragment max-assembled-size
(config) ip-fragment min-fragment-size
(config) tcp-ip-fragment-enabled
(config) udp-ip-fragment-enabled

show isc-ports

To display the Inter-Switch Communications (ISC) configuration on the CSS, use the **show isc-ports** command.

show isc-ports

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show isc-ports** command output, refer to the *Cisco Content Services Switch Global Server Load-Balancing Configuration Guide*.

Related Commands

(config-if) isc-port-one
(config-if) isc-port-two

show keepalive

To display keepalive status and configuration information for all keepalives or a specified keepalive, use the **show keepalive** command.

show keepalive {*name*}

Syntax Description

name	(Optional) Name of the keepalive

Command Modes

All modes

Usage Guidelines

The **show keepalive** command without an option displays information for all keepalives.

For information about the fields in the **show keepalive** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config) keepalive

show keepalive-summary

To display summary information for all keepalives, use the **show keepalive-summary**. This information includes the name, status, and IP address.

show keepalive-summary

Command Modes

All modes

Related Commands

(config) keepalive

show lines

To display currently connected lines or sessions, use the **show lines** command. A connected line is a console or Telnet session.

show lines

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show lines** command output, refer to the *Cisco Content Services Switch Administration Guide*.

show load

To display the global load configuration on the CSS and the load information for services, use the **show load** command.

show load {**absolute**}

Syntax Description

absolute	(Optional) Displays a table of values for the absolute load number scale. The values vary depending on the configured value of the **load absolute sensitivity** command. For more information, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide.*

Command Modes

SuperUser

Usage Guidelines

For information about the fields in the **show load** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

# show log

To send the log activity to your current session, or display the contents in a log or trap log file, use the **show log** command.

show log {*log_filename* {**tail** *lines*} {**line-numbers**}}

Syntax Description

log_filename	(Optional) Name of the log file. Enter an unquoted text string with no spaces. To see a list of log files with their dates, enter: `# show log ?` Enter the **traplog** filename to display all SNMP traps that have occurred. A trap log file is an ASCII file in the log directory containing generic and enterprise SNMP traps. By default, the following events generate level critical-2 messages: • Link Down • Cold Start • Warm Start • Service Down • Service Suspended All other SNMP traps generate level notice-5 messages. Even though traps are disabled, the CSS still produces a log message for any event that would normally generate a trap.
tail *lines*	(Optional) Displays the lines at the bottom and most recent portion of the log file. The number of lines start at the end of the log file. Enter a number from 1 to 1000.
line-numbers	(Optional) Includes the line numbers when displaying the contents of the log file.

Command Modes

All modes

Usage Guidelines

The **show log** command without an option sends the log activity to your current session. Press any key to stop sending the activity. This command performs the same function as **(config) logging line**. Note that you cannot run these commands at the same time.

Related Commands

clear
copy log
snmp trap-type generic

show log-list

To display a list of all log files, use the **show log-list** command.

show log-list

Command Modes

All modes

show log-state

To display the state of logging for CSS facilities, use the **show log-state** command.

show log-state

Command Modes

All modes

Related Commands

(config) logging

show map

To display the mapping configuration of the two disks (slot 0 and slot 1) in a CSS, use the **show map** command. This command displays the disk assignment of primary-boot record, secondary-boot record, core dump files, and logging output.

show map

Command Modes

All modes

Related Commands

map

## show mibii

To display the extended 64-bit MIB-II statistics for all interfaces or a specific interface in the CSS, use the **show mibii** command. The Enterprise ap64Stats MIB defines these statistics. To display the RFC 1213 32-bit statistics, include the **-32** suffix.

show mibii{**-32**} {*interface_name*}

Syntax Description

-32	(Optional) Displays the RFC 1213 32-bit statistics.
interface_name	(Optional) Name of an interface. To see a list of interfaces in the CSS, enter: `# show mibii ?`

Command Modes

All modes

Usage Guidelines

The Gigabit Ethernet module port statistics are an aggregation of all ports on the module.

For information about the fields in the **show mibii** command output, refer to the *Cisco Content Services Switch Administration Guide*.

Related Commands

clear

# show noflow-portmap

To display statistics for noflow port mapping on a CSS, use the **show noflow-portmap** command.

show noflow-portmap [**all-sps**|**slot** *number*]

Syntax Description

all-sps	Displays noflow portmap information for all session processors (SPs) in the CSS.
slot *number*	Displays noflow portmap information for the module in the specified chassis slot number. For a CSS 11503, enter an integer from 1 to 3. For a CSS 11506, enter an integer from 1 to 6. To display the available active slots in the CSS, enter: `# show noflow-portmap slot ?`

Command Modes

All modes except RMON, URQL, and VLAN configuration modes

Usage Guidelines

For information about the fields in the **show noflow-portmap** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config) noflow-portmap

# show nql

To display the table entries of the IP addresses for all network qualifier lists (NQLs) or a specified NQL, use the **show nql** command. An NQL is a list of subnet and host IP addresses used in ACL clauses.

show nql {*nql_name*}

Syntax Description

nql_name	(Optional) Name of the NQL. Enter a case-sensitive unquoted text string with no spaces. To see a list of existing NQL names, enter: `# show nql ?`

Command Modes

All modes

Usage Guidelines

If you enter **show nql** command in NQL mode, only the addresses for the current NQL is displayed.

The **show nql** command without an option displays entries for all NQLs.

For information about the fields in the **show nql** command output, refer to the *Cisco Content Services Switch Security Configuration Guide*.

Related Commands

(config) nql

show ospf

To display Open Shortest Path First (OSPF) information, use the **show ospf** command.

Syntax Description

show ospf advertise {*ip_or_host subnet_mask*}	Displays the advertising policy into OSPF. You can optionally display the configuration of ASE routes into OSPF for a specific IP address or host and its subnet address. Enter the *ip_or_host* variable in dotted-decimal format (for example, 192.168.11.1) or mnemonic host-name format (for example, myname.mydomain.com). Enter the *subnet_mask* either: • As a prefix length in CIDR bitcount notation (for example, /24). Do not enter a space to separate the IP address from the prefix length. • In dotted-decimal notation (for example, 255.255.255.0).
show ospf areas	Displays information about OSPF areas.
show ospf ase	Displays Autonomous System (AS) external entries in the link-state database (LSDB).
show ospf global	Displays OSPF global statistics.
show ospf interfaces	Displays OSPF interfaces.
show ospf lsdb {**router**|**network**|**summary**|**asbr_summ**|**external**}	Displays all the OSPF LSDBs or you can specify an individual database.
show ospf neighbors	Displays OSPF neighbors.
show ospf range	Displays OSPF area summary-route configuration information.
show ospf redistribute	Displays the configured redistribution policy into OSPF.

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show ospf** command output, refer to the *Cisco Content Services Switch Routing and Bridging Configuration Guide*.

Related Commands

(config) ospf
(config-circuit-ip) ospf

## show owner

To display the configuration information and statistics for an owner, use the **show owner** command. An owner is an entity that owns web content and is using the CSS to manage access to that content.

show owner {*owner_name* {**statistics**}}

Syntax Description

owner_name	(Optional) Name of a specific owner. Enter a case-sensitive unquoted text string with no spaces. To see a list of existing owner names, enter: `# show owner ?`
statistics	(Optional) Displays the statistics for the specified owner.

Command Modes

ACL, Circuit, Global, Group, Interface, Service, SuperUser, and User modes

Usage Guidelines

The **show owner** command without an option displays configuration information for all owners.

The **show owner** *owner_name* command displays configuration information for the specified owner.

For information about the fields in the **show owner** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config) owner

## show phy

To display duplex and speed values for all physical interfaces or a specific interface, use the **show phy** command.

show phy {*interface*}

Syntax Description

interface	(Optional) Name of the physical interface. Enter a case-sensitive unquoted text string. To see a list of interfaces, enter: # **show phy ?**

Command Modes

All modes

Examples

The **show phy** command without an option displays duplex and speed values for all physical interfaces in the CSS.

For information about the fields in the **show phy** command output, refer to the *Cisco Content Services Switch Administration Guide*.

Related Commands

(config-if) phy

show profile

To display the running user profile, use the **show profile** command.

show profile

Command Modes

All modes

Related Commands

copy profile

show proximity

To display an activity summary of the proximity database, use the **show proximity** command.

show proximity

Command Modes

All modes

Usage Guidelines

The **show proximity** command functions only on a Proximity Database CSS in a dedicated CSS 11150.

For information about the fields in the **show proximity** command output, refer to the *Cisco Content Services Switch Global Server Load-Balancing Configuration Guide*.

show proximity assign

To display the metric assignment of all zones or for a configured IP address range, use the **show proximity assign** command.

show proximity assign {*ip_address ip_prefix*}

Syntax Description

ip_address ip_prefix	(Optional) IP address and IP prefix length to display metrics over a range of IP addresses. Enter the IP address in dotted-decimal format (for example, 192.168.11.1). Enter the prefix as either: • A prefix length in CIDR bitcount notation (for example, /24). • A subnet mask in dotted-decimal notation (for example, 255.255.255.0).

Command Modes

All modes

Usage Guidelines

The **show proximity assign** command is functional only on a Proximity Database CSS in a dedicated CSS 11150.

For information about the fields in the **show proximity assign** command output, refer to the *Cisco Content Services Switch Global Server Load-Balancing Configuration Guide*.

Related Commands

proximity assign

show proximity cache

To display the current state of the cache, use the **show proximity cache** command. This information includes the current cache configuration, entries present, and the cache effectiveness, as related to the percentage of hits.

show proximity cache {**all**|*ip_address ip_prefix*}

Syntax Description

all	(Optional) Displays all cache entries.
ip_address ip_prefix	(Optional) Searches for the IP address and its associated IP prefix in the cache. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1). Enter the prefix as either: • A prefix length in CIDR bitcount notation (for example, /24). • A subnet mask in dotted-decimal notation (for example, 255.255.255.0).

Command Modes

All modes

Usage Guidelines

The **show proximity cache** command without an option displays statistics and configuration information about the cache.

This command is available on a CSS with the Enhanced feature set.

For information about the fields in the **show proximity cache** command output, refer to the *Cisco Content Services Switch Global Load-Balancing Configuration Guide*.

Related Commands

(config) proximity cache-size

show proximity metric

To view the metrics associated with client IP addresses, use the **show proximity metric** command. This command provides output on a Proximity Database and DNS CSS, however, the outputs are not the same. The PDB arranges the order of the output by zone number. The PDNS arranges the order of the output by the metric value.

show proximity metric *ip_address* {*ip_prefix* {**aggregate**}}

Syntax Description

ip_address	Client IP address. Enter the address in dotted-decimal notation (for example, 192.168.11.1).
ip_prefix	(Optional) IP prefix to use with the IP address. This allows you to view metrics over a range of IP addresses, indicated by the prefix. Enter the prefix as either: • A prefix length in CIDR bitcount notation (for example, /24). • A subnet mask in dotted-decimal notation (for example, 255.255.255.0).
aggregate	(Optional) Allows you to view aggregated metrics that are available at both the /16 and /8 level.

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show proximity metric** command output, refer to the *Cisco Content Services Switch Global Load-Balancing Configuration Guide*.

Related Commands

(config) proximity db

show proximity probe rtt statistics

To view the Round-Trip Time (RTT) probe module statistics, use the **show proximity probe rtt statistics** command.

show proximity probe rtt statistics

Command Modes

All modes

Usage Guidelines

The **show proximity probe rtt statistics** command is functional only on a Proximity Database CSS in a dedicated CSS 11150.

For information about the fields in the **show proximity probe rtt statistics** command output, refer to the *Cisco Content Services Switch Global Server Load-Balancing Configuration Guide*.

Related Commands

proximity probe rtt interval
proximity probe rtt method
proximity probe rtt samples
proximity probe rtt tcp-ports

show proximity refine

To display information pertaining to a refinement operation in progress for entries in the Proximity Database, use the **show proximity refine** command. The database manager divides the entries into three classes, N1, N2, and N3. N1 has the most activity, containing the most popular entries. N2 has midlevel activity. N3 contains the least popular entries.

show proximity refine

Command Modes

All modes

Usage Guidelines

The **show proximity refine** command is functional only on a Proximity Database CSS in a dedicated CSS 11150.

For information about the fields in the **show proximity refine** command output, refer to the *Cisco Content Services Switch Global Load-Balancing Configuration Guide*.

Related Commands

proximity refine

show proximity statistics

To view statistics associated with client IP addresses, use the **show proximity statistics** command.

show proximity statistics *ip_address* {*ip_prefix* {**aggregate**}}

Syntax Description

ip_address	The IP address for the statistics you want to display. Enter the address in dotted-decimal notation (for example, 192.168.11.1).
ip_prefix	(Optional) IP prefix to use with the IP address. This allows you to view metrics over a range of IP addresses indicated by the prefix. Enter the prefix as either: • A prefix length in CIDR bitcount notation (for example, /24). • A subnet mask in dotted-decimal notation (for example, 255.255.255.0).
aggregate	(Optional) Allows you to view aggregated statistics that are available at both the /16 and /8 level.

Command Modes

All modes

Usage Guidelines

The **show proximity statistics** command is functional only on a Proximity Database CSS in a dedicated CSS 11150.

For information about the fields in the **show proximity statistics** command output, refer to the *Cisco Content Services Switch Global Load-Balancing Configuration Guide*.

show proximity zone

To view the state information for all zones or a specified zone, use the **show proximity zone** command. This command is similar to the **show zone** command except it provides information from the perspective of the Proximity Database.

show proximity zone {**statistics**} {*number*}

Syntax Description

statistics	(Optional) Displays information about the blocks sent and received for a peer for all zones.
number	(Optional) Displays the state information for the specific zone. Enter a number from 0 to 15.

Command Modes

All modes

Usage Guidelines

The **show proximity zone** command is functional only on a Proximity Database CSS in a dedicated CSS 11150.

For information about the fields in the **show proximity zone** command output, refer to the *Cisco Content Services Switch Global Load-Balancing Configuration Guide*.

show publisher

To display the operational status of all or specific publishing service and content information, use the **show publisher** command.

show publisher {*publisher_name* {*content* {**verbose**}}}

Syntax Description

publisher_name	(Optional) Name of the publishing service
content	(Optional) Name of the content for the publishing service
verbose	(Optional) Displays more detailed content information

Command Modes

All modes

Usage Guidelines

The **show publisher** command without an option displays the operational status of all publishing services.

For information about the fields in the **show publisher** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config-service) publisher

show radius config

To display CSS configuration information for the primary and secondary RADIUS servers, use the **show radius config** command.

show radius config [**all**|**primary**|**secondary**]

Syntax Description

all	Displays the configuration for the primary and secondary RADIUS servers
primary	Displays the configuration for the primary RADIUS server
secondary	Displays the configuration for the secondary RADIUS server

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show radius config** command output, refer to the *Cisco Content Services Switch Security Configuration Guide*.

Related Commands

(config) radius-server

show radius stat

To display authentication statistics for the primary and secondary RADIUS servers, use the **show radius stat** command.

show radius stat [**all**|**primary**|**secondary**]

Syntax Description

all	Displays statistics for the primary and secondary RADIUS servers
primary	Displays statistics for the primary RADIUS server
secondary	Displays statistics for the secondary RADIUS server

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show radius stats** command output, refer to the *Cisco Content Services Switch Security Configuration Guide*.

Related Commands

(config) radius-server

show redundancy

To display CSS-to-CSS redundancy, use the **show redundancy** command.

show redundancy

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show redundancy** command output, refer to the *Cisco Content Services Switch Redundancy Configuration Guide*.

Related Commands

redundancy force-master
(config-if) redundancy-phy
(config) ip redundancy
(config-circuit) redundancy
(config-circuit-ip) redundancy-protocol
(config-service) type redundancy-up

show redundant-interfaces

To display a list of all redundant virtual interfaces configured on the CSS, use the **show redundant-interfaces** command. You can provide an interface IP address option to display only the virtual interfaces present on a particular interface. You can also include a virtual router identification (VRID) to display only the virtual interface information for a particular virtual router. If you have configured the **dns-server** option with the **ip redundant-interface** command, you can also use the **show redundant-interfaces** command to display the status of the DNS server and the number of DNS request packets that the DNS server has processed.

show redundant-interfaces {*ip_address* {*vrid*}}

Syntax Description

ip_address	(Optional) IP address for the redundant interface. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1).
vrid	(Optional) ID for an existing virtual router.

Command Modes

All modes

Usage Guidelines

The **show redundant-interfaces** command without an option displays all redundant interfaces on the CSS.

For information about the fields in the **show redundant-interfaces** command output, refer to the *Cisco Content Services Switch Redundancy Configuration Guide*.

Related Commands

(config-circuit-ip) ip redundant-interface
(config-circuit-ip) ip virtual-router

show redundant-vips

To display a list of all redundant VIPs configured on the CSS, use the **show redundant-vips** command. You can provide an interface IP address option to display only the VIPs present on a particular interface. You can also include a virtual router identification (VRID) to display only the VIP information for a particular virtual router.

show redundant-vips {*ip_address* {*vrid*}}

Syntax Description

ip_address	(Optional) IP address for the redundant interface. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1).
vrid	(Optional) ID for an existing virtual router.

Command Modes

All modes

Usage Guidelines

The **show redundant-vips** command without an option displays all redundant VIPs on the CSS.

For information about the fields in the **show redundant-vips** command output, refer to the *Cisco Content Services Switch Redundancy Configuration Guide*.

Related Commands

(config-circuit-ip) ip redundant-vip
(config-circuit-ip) ip virtual-router

show remap

To display the configured persistence reset and bypass settings, use the **show remap** command.

```
show remap
```

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show remap** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config) bypass persistence
(config) persistence reset

show reporter

To display reporter configurations and statistics for VRID peering or critical phy, use the **show reporter** command.

show reporter

Syntax Description

reporter_name	(Optional) Name of the reporter whose configuration you want to display

Command Modes

All modes

Usage Guidelines

If you enter the **show reporter** command without a reporter name, the output displays the configurations of all configured reporters on the CSS. For information about the fields in the **show reporter** command output, refer to the *Cisco Content Services Switch Redundancy Configuration Guide*.

Related Commands

(config) reporter
(config-reporter) active
(config-reporter) phy
(config-reporter) suspend
(config-reporter) type
(config-reporter) vrid

show rip

To display global or interface Routing Information Protocol (RIP) statistics, use the **show rip** command.

show rip {*ip_address*|**globals**|**statistics** {*ip_address*}}

Syntax Description

ip_address	(Optional) IP address for the RIP interface entry
globals	(Optional) Displays the global RIP statistics
statistics	(Optional) Displays the RIP interface statistics for all RIP interface entries

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show rip** command output, refer to the *Cisco Content Services Switch Routing and Bridging Configuration Guide*.

Related Commands

(config) rip
(config-circuit-ip) rip

## show rmon

To display the extended 64-bit Remote Monitoring (RMON) statistics for a specific Ethernet interface or all Ethernet interfaces in the CSS, use the **show rmon** command. The Enterprise ap64Stats MIB defines these statistics. To display the RFC 1757 32-bit statistics, include the **-32** suffix.

show rmon{**-32**} {*interface_name*}

Syntax Description

-32	(Optional) Displays the RFC 1757 32-bit statistics.
interface_name	(Optional) Name of the physical interface. Enter a case-sensitive unquoted text string. To see a list of interfaces, enter: `# show rmon ?`

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show mon** command output, refer to the *Cisco Content Services Switch Administration Guide*.

Related Commands

clear
(config) rmon-alarm

## show rmon-history

To display RMON history information for a specific Ethernet interface or all Ethernet interfaces in the CSS, use the **show rmon-history** command. By default, the CSS maintains two tables of history statistics. One table contains the last 50 samples at 30 second intervals. The other table contains 50 samples at 30 minute intervals.

show rmon-history {*interface_name* {*history_control_index*}}

Syntax Description

interface_name	(Optional) Name of the interface in the CSS. To see a list of interfaces, enter: `# show rmon-history ?`
history_control_index	(Optional) History control index you wish to display. To see a list of history control indexes associated with a interface, enter: `# show rmon-history interface_name ?`

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show rmon-history** command output, refer to the *Cisco Content Services Switch Administration Guide*.

Related Commands

(config) rmon-history

show rule

To display all content rules for a specific owner or all owners, use the **show rule** command. The screen shows information about the owner and the content rules. If you are in owner mode, the **show rule** command displays the summary for the current owner.

show rule {*owner_name* {*content_rule_name*
{**acl**|**all**|**dns**|**header-field**|**hot-list**|**services**|**statistics**|**sticky**}}}

Syntax Description

owner_name	(Optional) Name of an owner. When you enter a carriage return after the owner name, the CSS displays a summary of attributes for all rules belonging to the owner.
content_rule_name	(Optional) Name of a content rule belonging to the owner. When you enter a carriage return after the rule name, the CSS displays a summary of attributes for the rule.
acl	(Optional) Displays the ACL attributes for the rule.
all	(Optional) Displays all attributes for the rule.
dns	(Optional) Displays the DNS attributes for the rule.
header-field	(Optional) Displays the header-field attributes for the rule.
hot-list	(Optional) Displays the hotlist attributes for the rule.
services	(Optional) Displays the services for the rule.
statistics	(Optional) Displays the statistics for the rule.
sticky	(Optional) Displays the sticky attributes for the rule.

Usage Guidelines

For sticky connections in SuperUser, User, global, or owner configuration mode, you must specify the *owner_name* and the *content_rule_name* before you can enter the **sticky** option. In content configuration mode, you can enter only **show rule sticky**.

Command Modes

Content, global, owner, SuperUser, and User modes

Usage Guidelines

If you are in global, owner, SuperUser, or user mode, the **show rule** command without an option displays a summary of attributes for content rules for all owners. If you are in owner mode, the **show rule** command displays the summary for the current owner.

The summary of attributes includes the rule name, owner, state, type, balance, failover, persistence, param-bypass, IP redundancy, Layer 3, Layer 4, URL, and redirect information.

For information about the fields in the **show rule** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config-owner) content
(config-owner-content) advanced-balance
(config-owner-content) arrowpoint-cookie
(config-owner-content) balance
(config-owner-content) dnsbalance
(config-owner-content) flow-reset-reject
(config-owner-content) hotlist
(config-owner-content) primarySorryServer
(config-owner-content) redirect
(config-owner-content) secondarySorryServer
(config-owner-content) sticky-inact-timeout
(config-owner-content) string
(config-owner-content) zero

show rule-summary

To display a summary of all content rules for all owners, use the **show rule-summary** command. The screen shows information about the VIP address, port, protocol, URL, content rule name, and owner.

show rule-summary

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show rule-summary** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

## show running-config

To display the running configuration, use the **show running-config** command.

Syntax Description

show running-config	Displays all components of the running configuration.
show running-config acl {*index_number*}	Displays ACL information of the running configuration. For information about a specific ACL, include its index number.
show running-config circuit {*name*}	Displays circuit information of the running configuration, including critical reporters. For information about a specific circuit, include its name. To see a list of circuits, enter: `# show running-config circuit ?`
show running-config dql {*name*}	Displays DQL information of the running configuration. For information about a specific DQL, enter *name* as a case-sensitive unquoted text string and a maximum length of 32 characters. To see a list of DQLs, enter: `# show running-config dql ?`

show running-config eql {*name*}	Displays EQL information of the running configuration. For information about a specific EQL, include its name. To see a list of EQLs, enter: `# show running-config eql ?`
show running-config global	Displays the global configuration components of the running configuration.
show running-config group {*group_name*}	Displays the group information of the running configuration. For information about a specific group, enter *group_name* as a case-sensitive unquoted text string and a maximum length of 16 characters. To see a list of groups, enter: `# show running-config group ?`
show running-config header-field-group {*name*}	Displays the header-field group information of the running configuration. For information about a specific group, enter *name* as a case-sensitive unquoted text string and a maximum length of 16 characters. To see a list of header-field groups, enter: `# show running-config header-field-group ?`
show running-config interface *interface_name*	Displays the interface information of the running configuration. • For a CSS 11501, enter *interface_name* in *interface-port* format (for example, e2). • For a CSS 11503 or 11506, enter the interface name in *slot/port* format (for example, 3/1). To see a list of interfaces, enter: `# show running-config interface ?`
show running-config interfaces	Displays all the interface components of the running configuration.
show running-config keepalive {*keepalive_name*}	Displays the keepalive information of the running configuration. For information about a specific keepalive, enter *keepalive_name* as a case-sensitive unquoted text string and a maximum length of 32 characters. To see a list of keepalives, enter: `# show keepalive-summary`

show running-config nql {*name*}	Displays NQL information of the running configuration. For information about a specific NQL, include its name. To see a list of NQLs, enter: `# show running-config nql ?`
show running-config owner {*owner_name*}	Displays the owner information of the running configuration. For information about a specific owner, enter *owner_name* as a case-sensitive unquoted text string and a maximum length of 32 characters. To see a list of owners, enter: `# show running-config owner ?`
show running-config reporter {*reporter_name*}	Displays all reporter configurations on a CSS. For information about a specific reporter configuration, enter *reporter_name* as a case-sensitive unquoted text string with a maximum length of 32 characters.
show running-config rmon-alarm	Displays RMON alarm information of the running configuration.
show running-config rmon-event	Displays RMON event information of the running configuration.
show running-config rmon-history	Displays RMON history information of the running configuration.
show running-config service {*service_name*}	Displays the service information of the running configuration. For information about a specific service, enter *service_name* as a case-sensitive unquoted text string and a maximum length of 32 characters. To see a list of services, enter: `# show running-config service ?`

show running-config ssl-proxy-list {*list_name*}	Displays the components of the running configuration for a valid existing SSL proxy list. For information about a specific list, enter *list_name* as a case-sensitive unquoted text string. To see a list of SSL proxy lists, enter: `# show running-config ssl-proxy-list ?`
show running-config urql {*urql_name*}	Displays the components of the running configuration for a valid existing URQL. For information about a specific URQL, enter *urql_name* as a case-sensitive unquoted text string and a maximum length of 32 characters. To see a list of URQLs, enter: `# show running-config urql ?`

Command Modes

All modes

Related Commands

copy running-config

# show script

To display the files in the script directory or the contents in a specific script, use the **show script** command.

show script {*filename* {**line-numbers**}}

Syntax Description

script_filename	(Optional) Name of a valid script file you want to display. Enter a case-sensitive unquoted text string with a maximum length of 32 characters. To see a list of script names, enter: `# show script ?`
line-numbers	(Optional) Displays the line numbers for each line in the script.

Command Modes

SuperUser and all configuration modes

Related Commands

script

show service

To display service information, use the **show service** command.

show service {*service_name*|**summary**}

Syntax Description

service_name	(Optional) Name of a service. Enter the name as a case-sensitive unquoted text string with a maximum length of 32 characters.
summary	(Optional) Displays summary information for all services. This information includes the service state, connections, weight, and load.

Command Modes

All modes

Usage Guidelines

The **show service** command without an option displays information for all services. Similar to the **show service summary** command, this command also displays the service type, associated content rule, keepalive, the number of state transitions, connections, weight, and load.

If you add a script keepalive to a service, the configured script arguments, any script errors, the script run time, and the use of output parsing appears after the keepalive field.

If you are in service mode, the **show service** command displays the configuration information for the current service.

For information about the fields in the **show service** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

zero service
(config) service
(config-owner-content) zero

show setspan

To display SPAN information, use the **show setspan** command.

show setspan

Syntax Description

Source	Number of the port whose traffic you want to monitor.
Destination	Number of the DSPAN port to which the CSS copies the packets flowing through the SSPAN port. Connect the network analyzer or RMON probe to this port.
Direction	Direction of the traffic that you want to monitor at the source port. The direction can be one of the following: • **copyBoth** - The CSS copies packets that are transmitted and received by the SSPAN port to the DSPAN port. • **copyTxOnly** - The CSS copies only packets transmitted (egress traffic) by the SSPAN port to the DSPAN port. • **copyRxOnly** - The CSS copies only packets received (ingress traffic) by the SSPAN port to the DSPAN port.

Command Modes

All modes

Related Commands

(config) setspan

show session-redundant

To display summary Adaptive Session Redundancy (ASR) information about redundant content rules, services, and source groups on the CSS, use the **show session-redundant** command.

show session-redundant [**all**|**rule**|**service**|**group**]

Syntax Description

all	Displays all information concerning ASR information on the CSS
rule	Displays summary ASR information for redundant content rules
service	Displays summary ASR information for redundant services
group	Displays summary ASR information for redundant source groups

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show session-redundant** command output, refer to the *Cisco Content Services Switch Redundancy Configuration Guide*.

Related Commands

(config-group) redundant-index
(config-owner-content) redundant-index
(config-service) redundant-index

show sntp global

To display Simple Network Time Protocol (SNTP) configuration information on the CSS, use the **show sntp global** command.

show sntp global

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show sntp global** command output, refer to the *Cisco Content Services Switch Getting Started Guide*.

Related Commands

(config) sntp

show sockets

To display all the socket file descriptors that are currently in use, use the **show sockets** command.

show sockets

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show sockets** command output, refer to the *Cisco Content Services Switch Administration Guide*.

Related Commands

socket

show sorted running-config

To sort the configuration elements contained within each mode entry in the running-config file in alphanumeric order, use the **show sorted running-config** command. Sorting configuration elements allows for easier comparison of different running-config files. Note that the CSS does not sort the individual modes and the mode entries in a sorted running-config file.

show sorted running-config

Command Modes

All modes

Usage Guidelines

You cannot save a sorted running-config file as a valid running-config file. All lines begin with an exclamation mark (!) in the sorted running-config file. The exclamation mark is added as a safeguard to protect against the accidental execution of the sorted running-config file as a startup-config file. If you accidently run a sorted running-config file as a startup-config file, the CSS ignores all lines beginning with an exclamation mark (!).

Related Commands

show running-config

show sshd

To display information for the Secure Shell Host (SSH) daemon on the CSS, use the **show sshd** command.

show sshd [**config**|**sessions**|**versions**]

Syntax Description

config	Displays the configuration for the SSH daemon on the CSS.
sessions	Displays a summary of the current active SSHD server sessions. The command only displays data if an SSH client is currently configured.
versions	Displays the current version of the SSHield package that is running in the CSS.

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show sshd** command output, refer to the *Cisco Content Services Switch Security Configuration Guide*.

Related Commands

(config) sshd

# show ssl

To display SSL information on the CSS, use the **show ssl** command.

show ssl [**associate** *association_type* {*name*}|**crl-record** {*name2*}|**files** |**flows** {**slot** *number*}|**statistics** {*component*} {**slot** *number*}|**urlrewrite** {**slot** *number*}]

Syntax Description

associate	Displays information for all SSL associations on the CSS including their names, file names, and if they are being used by a SSL-proxy list.
association_type	Displays information for an association type. Enter one of the following types: • **cert** - Certificate associations • **rsakey** - RSA key pair associations • **dsakey** - DSA key pair associations • **dhparam** - Diffie-Hellman parameter file associations If you do not include a specific name for a type, a summary of information is displayed including the association names, file names, and if they are being used by a list.
name	(Optional) Displays detailed information for the specified name for an association type. To see a list of names for an association type, enter: `# show ssl associate association_type ?`
crl-record {*name2*)	Displays configuration information for all certificate revocation list (CRL) records. Optionally, you can specify the CRL record name (*name2*)to display the configuration for a specific record. The displayed information includes the CRL-record name, URL location, CA certificate for authentication, and the frequency in hours to update the CRL on the CSS.

files	Displays all SSL files on the CSS including their type and file size.
flows	Displays information about the active flows for each VIP address/port and SSL module. The output displays TCP proxy flows, active SSL flows (a subset of TCP proxy flows), and SSL flows occurring in the handshake phase of the protocol (a subset of active SSL flows).
slot *number*	(Optional) Displays the information for the slot location of the SSL module. The possible slots for an SSL module are: • 2 or 3 for a CSS 11503 • 2 to 6 for a CSS 11506 If you do not specify a slot number, information for all SSL modules in the CSS is displayed.
statistics	Displays the counter statistics for all components in all of the CSS SSL Acceleration modules. The components include the SSL application software, the cryptography chip in the SSL module, the OpenSSL software, the session cache, the back-end session cache, and information on client authentication.

component	(Optional) Displays the statistics for the components. Enter one of the following: • **session-cache** - Cache in SSL module when used in SSL termination • **backend-session-cache** - Cache in SSL module when used in backend SSL or SSL initiation • **ssl-proxy-server** - The SSL application software in the CSS • **crypto** - The cryptography chip in the SSL module • **ssl** - The OpenSSL software If you do not specify a component, the CSS displays the counters for all components in the SSL module.
urlrewite	Displays URL rewrite rule statistics for one or more CSS SSL modules. The statistics relate to the number of flows received and evaluated by the SSL module, and the number of HTTP 300-series redirects found and then rewritten by the module.

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show ssl** command output, refer to the *Cisco Content Services Switch SSL Configuration Guide*.

Related Commands

clear
(config) ssl associate
(config) ssl crl-record

## show ssl-proxy-list

To display information about SSL proxy configuration lists, use the **show ssl-proxy-list** command. You can display general information about all SSL proxy lists, detailed information about a specific list, or virtual or backend servers in the list.

show ssl-proxy-list {*list_name* {**ssl-server|backend-server** {*number*}}

Syntax Description

list_name	(Optional) Displays detailed information for all servers in the list. To see a list of names, enter: `# show ssl-proxy-list ?`
ssl-server	(Optional) Displays information for all virtual SSL servers in the list.
backend-server	(Optional) Displays information for all backend SSL servers in the list.
number	(Optional) Displays information for a specific virtual or backend SSL server in a list.

Command Modes

Global, Owner, Content, Service, SuperUser, and User

Usage Guidelines

For information on using the **show ssl-proxy-list** command in ssl-proxy-list configuration mode, see the **(ssl-proxy-list) show ssl-proxy-list** command.

The **show ssl-proxy-list** command without an option displays general information about all configured SSL proxy lists on the CSS.

For information about the fields in the **show ssl-proxy-list** command output, refer to the *Cisco Content Services Switch SSL Configuration Guide*.

Related Commands

(config) ssl-proxy-list
(ssl-proxy-list) description
(ssl-proxy-list) ssl-server

show startup-config

To display the CSS startup configuration (startup-config), use the **show startup-config** command. A startup-config contains configuration information that the CSS uses when it reboots.

show startup-config {**line-numbers**}

Syntax Description

line-numbers	(Optional) Displays the line numbers for each line in the startup-config

Command Modes

All modes

Usage Guidelines

For information about the **show startup-config** command, refer to the *Cisco Content Services Switch Administration Guide*.

Related Commands

copy

show startup-errors

To display errors that occurred when running the startup configuration at initialization time, use the **show startup-errors** command.

show startup-errors

Command Modes

All modes

Related Commands

show rule

show sticky-stats

To display a summary of sticky connection statistics for the CSS, use the **show sticky-stats** command.

show sticky-stats

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show sticky-stats** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

show rule

show sticky-table all-sticky

To display all Layer 3, Layer 4, SSL, and WAP MSISDN sticky entries contained in the CSS sticky table that are based on the advanced load-balancing method for a content rule, use the **show sticky-table all-sticky** command.

show sticky-table all-sticky {**page** *value*}

Syntax Description

page *value*	(Optional) Displays sticky entries for a specific page in the sticky at 100 entries per page. Enter a value between 1 and 5000 to select the page of entries you want to view from the sticky table. To determine the page you want to display, use the Total Number of Used Entries Found value list in the **show sticky-stats** command output and divide by 100 (entries per page).

Command Modes

All modes

Usage Guidelines

The **show sticky-table all-sticky** command without an option displays all entries in the sticky table. For information about the fields in the **show sticky-table all-sticky** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

To display only Layer 3, Layer 4, SSL, or WAP MSISDN sticky entries contained in the CSS sticky table, see the **show sticky-table l3-sticky**, **show sticky-table l4-sticky**, **show sticky-table ssl-sticky**, or **show sticky-table wap-sticky** command.

Related Commands

show rule
show sticky-table l3-sticky
show sticky-table l4-sticky
show sticky-table ssl-sticky
show sticky-table wap-sticky
show sticky-stats

show sticky-table l3-sticky

To display the Layer 3 entries contained in the CSS sticky table based on the advanced load-balancing method for a content rule, use the **show sticky-table l3-sticky** command. Layer 3 sticks a user to a server based on the source IP address.

show sticky-table l3-sticky {**page** *value*|**ipaddress** *ip_address sticky_mask*}

Syntax Description

page *value*	(Optional) Displays Layer 3 sticky entries for a specific page in the sticky table at 100 entries per page. Enter a value between 1 and 5000 to select the page of entries you want to view from the sticky table. To determine the page you want to display, use the Total Number of Used Entries Found value list in the **show sticky-stats** command output and divide by 100 (entries per page).
ipaddress *ip_address sticky_mask*	(Optional) Specifies the IP address of the Layer 3 sticky table entry to be shown. Enter the IP address in dotted-decimal notation (for example, 192.168.2.5). Specify the sticky mask from the content rule for this IP address in dotted-decimal notation (for example, 255.255.255.0). The default sticky mask of a content rule is 255.255.255.255.

Command Modes

All modes

Usage Guidelines

The **show sticky-table l3-sticky** command without an option displays all Layer 3 entries in the sticky table.

For information about the fields in the **show sticky-table l3-sticky** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

show rule
show sticky-stats

show sticky-table l4-sticky

To display the Layer 4 entries contained in the CSS sticky table based on the advanced load-balancing method for a content rule, use the **show sticky-table l4-sticky** command. Layer 4 sticky functions identically to Layer 3 sticky, except that it sticks based on a combination of source IP address and destination port.

show sticky-table l4-sticky {**page** *value*|**ipaddress** *ip_address sticky_mask port*}

Syntax Description

page *value*	(Optional) Displays Layer 4 sticky entries for a specific page in the sticky table at 100 entries per page. Enter a value between 1 and 5000 to select the page of entries you want to view from the sticky table. To determine the page you want to display, use the Total Number of Used Entries Found value list in the **show sticky-stats** command output and divide by 100 (entries per page).
ipaddress *ip_address sticky_mask port*	(Optional) Specifies the IP address and destination port number of the Layer 4 sticky table entry to be shown. Enter the IP address in dotted-decimal notation (for example, 192.168.2.5). Specify the sticky mask from the content rule for this IP address in dotted-decimal notation (for example, 255.255.255.0). The default sticky mask of a content rule is 255.255.255.255.

Command Modes

All modes

Usage Guidelines

The **show sticky-table l4-sticky** command without an option displays all Layer 4 entries in the sticky table. For information about the fields in the **show sticky-table l4-sticky** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

show rule
show sticky-stats

show sticky-table sip-callid-sticky

To display the session Call-ID entries contained in the CSS sticky table that are based on the advanced load-balancing method for a content rule, use the **show sticky-table sip-callid-sticky** command. Call ID is a unique call identifier contained in the SIP messages sent from the client to the SIP server.

show sticky-table sip-callid-sticky {**page** *value*|**Call-ID** *sip_callid*}

Syntax Description

page *value*	(Optional) Displays SIP Call-ID sticky entries for a specific page in the sticky table at 100 entries per page. Enter a value between 1 and 5000 to select the page of entries you want to view from the sticky table. To determine the page you want to display, use the Total Number of Used Entries Found value list in the **show sticky-stats** command output and divide by 100 (entries per page).
Call-ID *sip_callid*	(Optional) Specifies a specific Call ID to display from the sticky table. You can locate the Call-ID number by performing a packet trace.

Command Modes

All modes

Usage Guidelines

The **show sticky-table sip-callid-sticky** command with no option displays all session Call-ID entries in the sticky table.

For information about the fields in the **show sticky-table sip-callid-sticky** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

show rule
show sticky-stats

show sticky-table ssl-sticky

To display the SSL entries contained in the CSS sticky table that are based on the advanced load-balancing method for a content rule, use the **show sticky-table ssl-sticky** command.

show sticky-table ssl-sticky {**rule** *index* {**page** *value*}|
{**time** *number* {**page** *value*}|**sid** *text*|**collision**|**page** *value*}

Syntax Description

rule *index*	(Optional) Displays the SSL entries in the sticky table for the content rule. Enter the index number for the SSL sticky content rule. You can locate the index number for the content rule in the **show rule summary** command.
page *value*	(Optional) Displays SSL sticky entries for a specific page in the sticky table at 100 entries per page. Enter a value between 1 and 5000 to select the page of entries you want to view from the sticky table. To determine the page you want to display, use the Total Number of Used Entries Found value list in the **show sticky-stats** command output and divide by 100 (entries per page).
time *number*	(Optional) Specifies the window of elapsed time (in seconds) in which to display entries from the sticky table. All sticky entries in the table that were referenced within the specified time appear in the show output. Enter the time in seconds.
sid *text*	(Optional) Displays the entries in the sticky table based on SSL Session ID (SID). Enter the SID value as a hexadecimal ASCII string without the 0x prefix. You can locate the SID number by performing a packet trace.
collision	(Optional) Displays the entries in the sticky table that have a collision count (Col Cnt) greater than 0.

Command Modes

All modes

Usage Guidelines

The **show sticky-table ssl-sticky** command without an option displays all SSL entries in the sticky table.

For information about the fields in the **show sticky-table ssl-sticky** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

show rule
show sticky-stats

show sticky-table wap-sticky

To display the MSISDN header field entries contained in the CSS sticky table based on the advanced load-balancing method for a content rule, use the **show sticky-table wap-sticky** command. MSISDN is the header field for wireless clients using the Wireless Application Protocol (WAP).

show sticky-table wap-sticky {**page** *value*|**msisdn** *msisdn_header*}

Syntax Description

page *value*	(Optional) Displays MSISDN sticky entries for a specific page in the sticky table, at 100 entries per page. Enter a value between 1 and 5000 to select the page of entries you want to view from the sticky table. To determine the page you want to display, use the Total Number of Used Entries Found value list in the **show sticky-stats** command output and divide by 100 (entries per page).
msisdn *msisdn_header*	(Optional) Specifies the MSISDN header field to display from the sticky table. Enter the *msisdn_header* as a text string. The MSISDN header field typically contains the wireless phone numbers. You can locate the MSISDN header by performing a packet trace.

Command Modes

All modes

Usage Guidelines

The **show sticky-table wap-sticky** command without an option displays all MSISDN header field entries in the sticky table.

For information about the fields in the **show sticky-table wap-sticky** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

show subscriber

To display the operational status of all subscriber services or subscriber services for a specific publishing service, use the **show subscriber** command.

show subscriber {*publisher_name*}

Syntax Description

publisher_name	(Optional) Name of a publishing service

Command Modes

All modes

Usage Guidelines

The **show subscriber** command without an option displays information about all subscriber services.

For information about the fields in the **show subscriber** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config-service) publisher
(config-service) subscriber

show summary

To display the relationship between owners, content rules, and services, use the **show summary** command.

show sum{**mary**} {*owner_name*}

Syntax Description

owner_name	(Optional) Name of an existing owner. Enter an unquoted string with a maximum length of 32 characters.

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show summary** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

show system-resources

To display information about the memory size in a CSS, use the **show system-resources** command. For a:

- CSS 11501 - Displays information about the size of the installed and the available free memory.
- CSS 11503 or 11506 - Displays information about the size of the installed and free memory available on all modules in the chassis. Optionally, you can display a summary of the CPU utilization by all module.

show system-resources {*slot_number*|**cpu_summary**}

Syntax Description

slot_number	(Optional) Specifies the CSS chassis slot number for which you want to display the system resources.
cpu_summary	(Optional) Displays a summary of the CPU utilization by all modules installed in the CSS chassis.

Command Modes

All modes

Usage Guidelines

The **show system-resources** command without an option displays information about the size of the installed and free memory available on the CSS.

For information about the fields in the **show system-resources** command output, refer to the *Cisco Content Services Switch Administration Guide*.

show tacacs-server

To display the TACACS+ server configuration information, use the **show tacacs-server** command.

show tacacs-server

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show tacacs-server** command output, refer to the *Cisco Content Services Switch Security Administration Guide*.

Related Commands

(config) tacacs-server

show trunk

To display VLAN trunk status information on configured Ethernet ports and their associated VLANs, use the **show trunk** command.

show trunk

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show trunk** command output, refer to the *Cisco Content Services Switch Routing and Bridging Configuration Guide*.

Related Commands

(config-if) trunk
(config-if) vlan
(config-if-vlan) default-vlan

show uptime

To display the length of time the CSS has been running, use the **show uptime** command. The time is displayed in *hour*:*minute*:*second* format. For the CSS 11503 or 11506, this command shows how long each module has been running.

show uptime

Command Modes

All modes

show urql

To display general information about all Uniform Resource Locator qualifier list (URQL) or detailed information about a specific URQL, use the **show urql** command.

show urql {*name*}

Syntax Description

name	(Optional) Name of a specific URQL

Command Modes

All modes

Usage Guidelines

The **show urql** command without an option displays general information about all URQLs including their names, descriptions, create type, state, and the number of content rules associated with each URQL.

The **show urql** *name* command displays detailed information for a specific URQL including its create type, state, and assigned URL entries.

If you use the **show urql** command in URQL mode, the CSS displays the detailed information for the current URQL.

For information about the fields in the **show urql** command output, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config) urql

show user-database

To display a list of all users that have been configured on a CSS and the virtual and console authentication settings, use the **show user-database** command.

show user-database {*user_name*}

Syntax Description

user_name	(Optional) Name of a valid user. Enter a case-sensitive unquoted text string.

Command Modes

All modes

Usage Guidelines

The **show user-database** command without an option displays a list of all users that have been configured on a CSS and the virtual and console authentication settings.

For information about the fields in the **show user-database** command output, refer to the *Cisco Content Services Switch Administration Guide*.

Related Commands

(config) username
(config) username-technician

show variable

To display a list of all or specific user-defined variables, use the **show variable** command.

show variable {*name*}

Syntax Description

name	(Optional) Name of a variable

Command Modes

All modes

Usage Guidelines

The CLI uses the following special variables in its operation to control session behavior and to enhance interaction with CLI commands and the user:

- The USER variable is set automatically to the username starting the CLI session at login time.
- The LINE variable is set automatically to the line that the user is connected to at login time.
- The MODE variable is set automatically to the current mode as the user navigates the hierarchy of CLI modes.
- The STATUS variable is set automatically to return the exit status of the previously-executed CLI command. In most cases, with the exception of the **grep** command, an exit status of 0 indicates a command was successful, and a non-zero value indicates failure.
- The CHECK_STARTUP_ERRORS variable, if set within a profile script, indicates the user should be informed of startup-errors upon login. If the CSS detects a startup-errors file in the log directory, the screen displays the `***Startup Errors occurred on boot.***` message.

- The CONTINUE_ON_ERROR variable controls how a script executing in an interactive CLI session handles a command error. When you set this variable in a script with the **set** command, the execution of a script continues when errors are detected. If you do not set this variable in a script, the script terminates when an error occurs.

  Exercise caution when using this variable. Syntax errors are ignored when it is set. Set this variable in the script where you expect a command to fail and then disable it with the **no set** command.

The **show variable** command without an option displays a list of the user-defined variables and their values on the CSS.

show version

To display the current software version, licenses running on the CSS, and, if applicable, the path to the network-mounted CSS software and configuration path, use the **show version** command. This command also displays the flash version for the CSS.

show version

Command Modes

All modes

Usage Guidelines

For information about the fields in the **show version** command output, refer to the *Cisco Content Services Switch Administration Guide*.

show virtual-routers

To display a list of all virtual routers and critical reporters configured on the CSS, use the **show virtual-routers** command. You can provide an interface IP address to display only the virtual routers present on a particular interface. You can also include a VRID to display only the information for a particular virtual router.

show virtual-routers {*ip_address* {*vrid*}}

Syntax Description

ip_address	(Optional) IP address for the redundant interface. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1).
vrid	(Optional) ID for an existing virtual router.

Command Modes

All modes

Usage Guidelines

The **show virtual-routers** command without an option displays all virtual routers on the CSS.

For information about the fields in the **show virtual-routers** command output, refer to the *Cisco Content Services Switch Global Server Load-Balancing Configuration Guide*.

Related Commands

(config-circuit-ip) ip virtual-router

show zone

To display the current state of all zones or a specified zone, use the **show zone** command.

show zone {*zone* {**verbose**}|**local**|**verbose**}

Syntax Description

zone	(Optional) Zone index of the peer. If you omit this variable, this command displays the states of all zones.
local	(Optional) Displays local zone information including its zone index number, configured description, tier level, and PDB IP address.
verbose	(Optional) Displays extra information per Proximity CAPP Messaging (PCM) negotiation. This information includes a count of transmitted and received PCM_CLIENT_CTL packet types, a count of client packets, and a count of APP transmit errors.

Command Modes

All modes

Usage Guidelines

The **show zone** command is available on a Proximity Database and a DNS CSS.

The **show zone** command without an option displays the state of Client Control Negotiations.

For information about the fields in the **show zone** command output, refer to the *Cisco Content Services Switch Global Load-Balancing Configuration Guide*.

socket

Use the **socket** command and options as socket primitives in a script keepalive. The socket primitives allow for ASCII or hexadecimal send and receive functionality. The options for this command are:

- **socket connect** - Performs either a TCP or UDP connection
- **socket disconnect** - Disconnects from the remote host
- **socket inspect** - Inspects the socket internal data buffer for data
- **socket receive** - Fills the 10K internal buffer with data coming in from the remote host, and then locks the buffer so that no new data is placed in the buffer
- **socket send** - Writes data through a previously-connected TCP connection
- **socket waitfor** - Returns the call immediately upon finding the specified string argument

For more information on these commands and any associated options, see the following commands.

Related Commands

show sockets

socket connect

To perform either a TCP or UDP connection, use the **socket connect** command. A TCP connection performs a TCP connection handshake (SYN, SYN/ACK...) to a specific IP address and port. A UDP connection is a reservation of the host and port. The socket value is received in a ${SOCKET} variable in the script.

Note A maximum of 64sockets can be opened at any one time across all scripts on the CSS.

socket connect host *ip_address* **port** *number* **[tcp {***timeout***} {session}** {**nowait**}|**udp** {**session**}]

Syntax Description

ip_address	Host name or IP address of the remote system.
number	Port number on which to negotiate a connection.
tcp	Defines a connection using TCP.
udp	Defines a connection using UDP.
timeout	(Optional) Timeout value in milliseconds for network establishment. This value applies only to a TCP connection. If the time limit expires before the connection has been successfully made, then the attempt fails. Enter a value from 1 to 60000 ms (1 to 60 seconds). The default is 5000 ms (5 seconds).
session	(Optional) Tells the socket to remain open until the session is finished. Any scripts with open sockets in the session that do not close on their own will remain open until you log out.
nowait	Keyword that tells the socket to send data immediately without waiting to aggregate the data first.

Command Modes

All modes

socket disconnect

To close the connection to the remote host, use the **socket disconnect** command. By default, a reset (RST) is sent to the remote host to reset the connection.

socket disconnect *socket_number* {**graceful**}

Syntax Description

socket_number	Socket file descriptor in integer form. The descriptor is returned from a connection.
graceful	(Optional) Allows a graceful disconnect by sending a FIN (no more data from the sender) rather than an RST to the remote host.

Command Modes

All modes

Related Commands

show sockets

socket inspect

To inspect the socket internal data buffer for data, use the **socket inspect** command. If data is found, this command displays the last 10 KB of data received to standard output. If the characters displayed are nonprintable, they are represented by a period character (.).

socket inspect *socket_number* [**pretty**|**raw**]

Syntax Description

socket_number	Socket file descriptor in integer form. The descriptor is returned from a connection.
pretty	Outputs each line with both hexadecimal and ASCII equivalents for each byte of data. Each line contains 16 bytes. For example, "0x41 0x42 0x43 0x44 0x10 0x05 ABCD.."
raw	Displays the string values as hexadecimal bytes rather than a simple string. For example, "ABCD" becomes "41424344" (1-byte hexadecimal equivalent).

Command Modes

All modes

socket receive

To fill the 10-KB internal buffer with data coming in from the remote host and then lock the buffer so that no new data is placed in the buffer, use the **socket receive** command. You can dump all the data residing in this internal 10-KB buffer to standard output.

Note All previous data in the 10-KB internal buffer is flushed out before filling the buffer with new data.

socket receive *socket_number* {*timeout*} {**raw**}

Syntax Description

socket_number	Socket file descriptor in integer form. The descriptor is returned from a connection.
timeout	(Optional) Timeout value representing the number of milliseconds to wait before locking the internal 10-KB buffer and returning to the user. Enter a value from 1 to 15000 milliseconds. The default value is 100 ms.
raw	(Optional) Causes the text string values to be received and changed to hexadecimal bytes. For example, 0D0A is received as 0x0D 0x0A (carriage return, line feed).

Command Modes

All modes

socket send

To write data through a previously-connected TCP connection or a UDP-reserved host port, use the **socket send** command. Note that the **socket send** command empties the content s of the 10-KB receive buffer.

socket send *socket_number* **"***string***"** {**raw**|**base64**}

Syntax Description

socket_number	Socket file descriptor in integer form. The descriptor is returned from a connection.
"*string***"**	Data to write through the connection. Enter a quoted string with a maximum of 128 characters.
raw	(Optional) Causes the text string values to be changed and transferred as actual hexadecimal bytes rather than a standard ASCII string. For example, 0D0A is sent as 0x0D 0x0A (carriage return, line feed).
base64	(Optional) Base-64 encodes the string before sending it through the connection. The encoding is useful for HTTP basic authentication for connections to a password-protected website.

Command Modes

All modes

socket waitfor

To return the call immediately upon finding the specified string argument or any incoming data, use the **socket waitfor** command. When the specified string or data is found, the command returns a ${STATUS} of 0 (success). Otherwise, it returns 1 (failure). You can view the retrieved data by using the **socket inspect** command.

socket waitfor *socket_number* [**anything** {*timeout*}|**"***string***"** {*timeout*} {**case-sensitive**} {**offset** *bytes*} {**raw**}]

Syntax Description

socket_number	Socket file descriptor in integer form. The descriptor is returned from a connection.
anything	Any incoming data returns the call within the timeout period. If any data is found, the command returns immediately and does not wait the entire timeout period.
timeout	(Optional) Timeout value in milliseconds that the software waits for the string argument to be found. Enter a value from 1 to 15000 milliseconds. The default value is 100 ms.
"*string***"**	Specific string that returns the call within the timeout period. If the string is found, the command returns immediately and does not wait the entire timeout period. Enter a quoted string with a maximum of 128 characters.
case-sensitive	(Optional) Indicates that the string comparison is case-sensitive. For example, User is not equivalent to user.
offset *bytes*	(Optional) Indicates how many bytes into the received data to find the string. For example, a string of "a0" and an offset of 10 searches for "a0" 10 bytes into the received data.
raw	(Optional) Causes the string values to be interpreted as hexadecimal bytes rather then a simple string. For example, 0D0A is sent as 0x0D 0x0A (carriage return, line feed).

Command Modes

All modes

Related Commands

socket inspect

terminal

To set terminal parameters, use the **terminal** command. These parameters control output to the terminal screen. Terminal parameters are user-specific, applying uniquely for the current session. To permanently save changes you made to a terminal parameter, you can use the **copy running-config** command, or when you exit a CLI session, you can respond with **y** when the CSS prompts you that the profile has changed and queries whether you want to save the changes to the user profile. The options for this command are:

- **terminal idle** - Sets the maximum amount of time that the terminal session can be idle before the CSS logs it out
- **terminal length** - Sets the terminal screen output length
- **terminal more** - Enables terminal More command support
- **terminal netmask-format** - Controls the display of subnet masks in **show** commands
- **terminal timeout** - Sets the maximum amount of time that a terminal session can be logged into the CSS

Note To save the setting for these commands for use in other sessions, you can include a terminal parameter as a session-based configuration parameter for a profile script.

For more information on these commands and any associated options, see the following commands.

terminal idle

To set the maximum amount of time that the terminal session can be idle before the CSS logs it out, use the **terminal idle** command. Use the **no** form of this command to set the idle time for the terminal to the default of 0.

terminal idle *number*

no terminal idle

Syntax Description

number	Maximum time in minutes. Enter a number from 0 to 65535. The default is 0, which disables the idle timer. Note that the default idle timer for the session is disabled in the default profile script.

Command Modes

User and SuperUser

terminal length

To set the number of lines of output the CLI displays on the terminal screen, use the **terminal length** command. Use the **no** form of this command to set the number of lines to the default 25 lines.

terminal length *number*

no terminal length

Syntax Description

number	Number of lines of output to display. Enter a number from 2 to 65535. The default is 25.

Command Modes

User and SuperUser

Related Commands

terminal more

terminal more

To enable support for More command functions with the terminal, use the **terminal more** command. Use the **no** form of this command to disable support for More command functions.

terminal more

no terminal more

Note Use Esc-M as a keyboard shortcut to toggle between enabling and disabling *more* support on this session.

Command Modes

User and SuperUser

Related Commands

terminal length

terminal netmask-format

To define the IP subnet mask format when you display the running configuration on the terminal screen, use the **terminal netmask-format** command. Use the **no** form of this command to display subnet masks in the default dotted-decimal format.

terminal netmask-format [**bitcount**|**decimal**|**hexadecimal**]

no terminal netmask-format

Syntax Description

bitcount	Display masks in bit counts (for example, /24).
decimal	Display masks in dotted-decimal format (for example, 255.255.255.0). This is the default format.
hexadecimal	Display masks in hexadecimal format (for example, 0XFFFFFF00).

Command Modes

User and SuperUser

Related Commands

show running-config

terminal timeout

To set the maximum amount of time that a terminal session can be logged into the CSS, use the **terminal timeout** command. Use the **no** form of this command to set the timeout for a terminal session to the default of 0.

terminal timeout *number*

no terminal timeout

Syntax Description

number	Maximum time in minutes. Enter a number from 0 to 65535. The default is 0, which disables the timeout period.

Command Modes

User and SuperUser

Usage Guidelines

The default timeout period for the session is disabled in the default profile script.

traceroute

To trace the connectivity and the path to an IP address, use the **traceroute** command.

traceroute *ip_or_host*

Syntax Description

ip_or_host	The IP address you want to trace. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or in mnemonic host-name format (for example, myhost.mydomain.com).

Command Modes

All modes

update arp

To update the file containing the host IP addresses entered at initialization or boot time through ARP, use the **update arp** command.

update arp file

Command Modes

SuperUser

Usage Guidelines

The **update arp** command forces the CSS to write the current ARP cache to the ARP file on disk.

Related Commands

clear
show arp
(config) arp

var-shift

To remove the first word from a character variable value, leaving the remaining words, use the **var-shift** command. When the last word is removed, the value of the variable becomes “”.

var-shift *variable_name*

Syntax Description

variable_name	A character string representing the variable. Enter a string with a maximum length of 32 characters.

Command Modes

All modes

Usage Guidelines

You can also access words in a character variable by using [*word_number*] notation with the normal variable syntax. The **var-shift** command is typically used within a script.

Related Commands

show variable

version

To display the current software version, licenses running on the CSS, and, if applicable, the path to the network-mounted CSS software and configuration path, use the **version** command. This command also displays the flash version for the CSS.

version

Command Modes

All modes

while

To provide branch looping capabilities within an interactive session or within a script, use the **while** command.

while [*constant*|*variable_name*] {**"***operator(s)***"** **"***operand(s)***"**}

Syntax Description

constant	The number of times to execute the loop. Enter an integer or user-defined variable.
variable_name	A character string representing a variable. Enter a name with a maximum length of 32 characters.
"*operator*"	(Optional) One or more operations on the operand. Enter a quoted string of one or more of the following operators. Separate multiple operators with a space. • OR — Simple OR operator • > — Greater than operator • AND — Simple AND operator • * — Multiplication operator • MOD — Modulus operator • / — Division operator • >= — Greater than or equal to operator • < — Less than operator • <= — Less than or equal to operator • == — Equality operator • + — Add to variable • - — Subtract from variable • -- — Decrement variable • ++ — Increment variable Numeric value operators are handled one at a time from left to right, using the list of operands from the list as needed. Operators, such as -- and ++, do not require an operand.

"*operand*"	(Optional) One or more strings or arguments, as follows: • For character operators, enter a quoted string of either a string constant or a character argument. • For numeric operators, enter a quoted string of one or more integers or numeric argument. Separate multiple operands with a space.

Command Modes

All modes

Usage Guidelines

The **while** command initiates the creation of a branch block. You can include any number of commands in this block including nested blocks. To terminate a branch block, use the **endbranch** command.

Related Commands

endbranch
input
set
show variable

write memory

To copy the running-config to the startup-config and archive the startup-config, use the **write memory** command.

write memory

Command Modes

SuperUser

zero dos statistics

To set the Denial of Service (DoS) statistics for the CSS to zero, use the **zero dos statistics** command. The **show dos** command displays the statistics.

zero dos statistics

Command Modes

All modes

Related Commands

show dos

zero ip-fragment-stats

To set the IP fragment statistics, use the **zero ip-fragment-stats** command. This command sets the values of the statistics in the IP Fragment Statistics and IP Fragment Errors sections of the **show ip-fragment-stats** command output to zero.

zero ip-fragment-stats

Command Modes

All modes

Related Commands

show ip-fragment-stats

zero ip statistics

To set the global IP (TCP/UDP) statistics for the CSS to zero, use the **zero ip statistics** command. The **show ip statistics** command displays the statistics.

zero ip statistics

Command Modes

All modes

Related Commands

show ip statistics

zero reporter state-transitions

To set the reporter State Transitions counter for the CSS to zero, use the **zero reporter state-transitions** command. The **show reporter** command displays the statistics.

zero reporter state-transitions [**all**|**reporter** *reporter_name*]

Syntax Description

all	Sets the State Transitions counter for all reporters to zero
reporter *reporter_name*	Specifies the name of a reporter whose State Transitions statistics you want to set to zero

Command Modes

All modes

Related Commands

show reporter

zero service

To set specified statistics counters for all services on the CSS to zero, use the **zero service** command. The **show service** command displays the counters.

zero service [**total-connections**|**total-reused-connections** |**state-transitions**]

Syntax Description

total-connections	Sets the Total Connections counter for all services to zero
total-reused-connections	Sets the Total Reused Conns counter for all services to zero
state-transitions	Sets the State Transitions counter for all services to zero

Command Modes

All modes

Usage Guidelines

The **zero service** command resets specific counters for all services. To reset counters for a content rule or a specific service on a content rule, use the **(config-owner-content) zero** command.

Related Commands

show service

zero virtual-router state-changes

To set the State Changes field of the **show virtual-routers** command output to zero, use the **zero virtual-router state-changes** command in any mode.

zero virtual-router state-changes [**all**|**circuit** *ip_address* [**all**|**vrid** *number*]]

Syntax Description

all	Sets the State Changes counter of all VRs configured on the CSS to zero
circuit *ip_address*	Specifies a circuit IP address where VRs are configured
all	Sets the State Changes counter of all VRs on the specified circuit to zero
vrid *number*	Sets the State Changes counter of the specified VR on the specified circuit to zero

Command Modes

All modes

Usage Guidelines

The State Changes field records the number of times that a VR changed state since the CSS was booted.

Related Commands

show virtual-routers

Global Configuration Mode Commands

Global configuration mode allows a SuperUser to:

- Configure global CSS parameters.
- Initially access subordinate configuration modes on the CSS. These modes allow you to configure ACLs, boot, circuits and their IP interface addresses, EQLs, physical interfaces, global keepalives, source groups, owners and their content rules, RMON alarm, events and history, and services.

To access global configuration mode, use the **configure** command in SuperUser mode.

This section describes the commands in global configuration mode. For more information on commands for the subordinate configuration modes available on the CSS, see their sections later in this chapter.

For a list of general commands you can use in global configuration mode, see the "General Commands" section.

(config) acl

To access ACL configuration mode, configure an access control list (ACL) on the CSS, and enable or disable all ACLs on the CSS, use the **acl** command. Use the **no** form of this command to delete an ACL.

acl [*index*|**enable**|**disable**]

no acl *index*

Syntax Description

index	Number you want to use to create a new ACL or the number for an existing ACL to access ACL mode. Enter a number from 1 to 99. When you access this mode, the prompt changes to (config-acl [*index*]). For information about commands available in this mode, see the "ACL Configuration Mode Commands" section.

disable	Disables all ACLs on the CSS.
enable	Enables all ACLs on the CSS.

Usage Guidelines

To enable global logging for ACLs, you must enter the **(config) logging subsystem acl level debug-7** command.

Caution When you enable ACL mode, all traffic not configured in an ACL permit clause *will be denied*. ACLs function as a firewall security feature. You must first configure an ACL to permit traffic *before you enable ACL mode*. If you do not permit any traffic, you will lose network connectivity. Note that the console port is not affected.

If you do not configure ACLs on the CSS, all packets passing through the CSS could be allowed onto the entire network. For example, you may want to permit all e-mail traffic, but block Telnet traffic. You can also use ACLs to allow one client to access a part of the network and prevent another client from accessing the same area.

Related Commands

show acl
(config-acl) apply
(config-acl) clause
(config-acl) remove

(config) app

To enable all Application Peering Protocol (APP) sessions, use the **app** command. An APP session is the exchange of content information between a group of configured CSSs. APP provides a guaranteed and private communications channel for this exchange. Use the **no** form of this command to disable all APP sessions.

app

no app

Related Commands

(config) dns-server
(config-owner) dns
(config-owner-content) add dns

(config) app framesz

To set the maximum frame size allowed on an APP channel between CSSs, use the **app framesz** command. Use the **no** form of this command to restore the default frame size to 10240.

app framesz *size*

no app framesz

Syntax Description

size	Maximum frame size. Enter a number from 10240 to 65535. The default is 10240.

(config) app port

To set the TCP port number, use the **app port** command. This port listens for APP connections. Use the **no** form of this command to restore the default port number to 5001.

app port *port_number*

no app port

Syntax Description

port_number	Port number. Enter a number from 1025 to 65535. The default is 5001.

(config) app session

To create an APP session between the CSS and its peer CSS, use the **app session** command. These CSSs are a content domain that share the same content rules, load, and DNS information with each other. Use the **no** form of this command to terminate an APP session.

app session *ip_address* {*ka_freq* {[**authChallenge**|**authNone**] *secret*
{[**encryptMd5hash**|**encryptNone**] {[**rcmdEnable**|**rcmdDisable**]}}}}

no app session *ip_address*

Syntax Description

ip_address	IP address for the peer CSS. Enter the address in dotted-decimal notation (for example, 192.168.11.1).
ka_freq	(Optional) Time in seconds between sending keepalive messages to the peer CSS. Enter an integer from 14 to 255. The default is 14.
authChallenge | **authNone**	(Optional) Authentication method for the session. Enter either **authChallenge** for Challenge Handshake Authentication Protocol (CHAP) method or **authNone** for no authentication method. The default is no authentication.

secret	Secret sent with each packet identifier. Enter an unquoted text string with a maximum of 32 characters. If you entered **authNone** for the authentication method, enter any character as the secret.
encryptMd5hash | **encryptNone**	(Optional) Encryption method for the packets. Enter either **encryptMd5hash** for the MD5 base hashing method or **encryptNone** for the no encryption method. The default is no encryption.
rcmdEnable | **rcmdDisable**	(Optional) Setting for sending remote CLI commands to the peer through the **rcmd** command. Enter either **rcmdEnable** to send CLI commands or **rcmdDisable** to not send CLI commands. The default setting is enabled.

Related Commands

show app
show dns-peer
show dns-server

(config) app-udp

To enable Application Peering Protocol-User Datagram Protocol (APP-UDP) datagram messaging, use the **app-udp** command. Messaging is enabled by default. An APP datagram allows an exchange of information between applications resident on the CSS. Use the **no** form of this command to disable APP-UDP messaging.

app-udp

no app-udp

Usage Guidelines

The **app-udp** command is available on a Proximity Database and a DNS CSS.

Related Commands

show app-udp

(config) app-udp options

To configure encryption with an IP address, use the **app-udp options** command. Use the **no** form of this command to delete the options from an IP address.

app-udp options *ip_address* **encrypt-md5hash** *secret*

no app-udp options *ip_address*

Syntax Description

ip_address	IP address that you want to associate with this group of options. Enter the address in dotted-decimal notation (for example, 192.168.11.1).
secret	String used in encryption and decryption of the MD5 hashing method. Enter an unquoted text string with a maximum of 31 characters. There is no default.

Usage Guidelines

The CSS applies encryption to packets sent to this destination address or when the CSS 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 more specifically configured. Use of the 0.0.0.0 IP address allows you to set a global security configuration that may be applied to an arbitrary number of peers.

Examples

The following 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 CSS encrypts datagrams received from 10.6.3.21 and transmitted to 10.6.3.21 with secret *mySecret*. The CSS subjects all other datagrams, received or transmitted, to the default encryption secret *anotherSecret*.

```
(config) # app-udp options 10.6.3.21 encrypt-md5hash mySecret
(config) # app-udp options 0.0.0.0 encrypt-md5hash anotherSecret
```

Related Commands

(config) app-udp secure

(config) app-udp port

To set the UDP port number, use the **app-udp port** command. This port listens for APP datagrams. Use the **no** form of this command to restore the UDP port number to its default value of 5002.

app-udp port *port_number*

no app-udp port

Syntax Description

port_number	UDP port number. Enter a value from 1025 to 65535. The default is 5002.

(config) app-udp secure

To require the encryption of all inbound APP datagrams, use the **app-udp secure** command. This prevents unauthorized messages from entering the CSS. Use the **no** form of this command to restore the default behavior of allowing the CSS to accept all APP datagrams.

app-udp secure

no app-udp secure

Usage Guidelines

Use the **app-udp secure** command with the **(config) app-udp options** command to specify the secure messages that are accepted. If you use this command without the **(config) app-udp options** command, the CSS drops all incoming data.

Examples

The following commands allow only incoming traffic from 10.6.3.21 encrypted with the secret "mySecret."

```
(config) # app-udp secure
(config) # app-udp options 10.6.3.21 encrypt-md5hash mySecret
```

Related Commands

(config) app-udp options

(config) arp

To define a static ARP mapping IP address to Media Access Control (MAC) address translations necessary for the CSS to send data to network nodes, use the **arp** command. Use the **no** form of this command to delete a static mapping address.

arp *ip_or_host mac_address interface* {*vlan*}

no arp *ip_or_host*

Syntax Description

ip_or_host	IP address of the system for static mapping. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or in mnemonic host-name format (for example, myhost.mydomain.com).
mac_address	MAC address of the system mapped to the IP address. Enter the MAC address in hyphenated-hexadecimal notation (for example, 00-60-97-d5-26-ab).
interface	CSS interface that you want to configure as the egress logical port. For a CSS 11501, enter the interface name in *interface-port* format (for example, e2). For a CSS 11503 or 11506, the interface format is *slot/port* (for example, 3/1). To see a list of interfaces, enter: `arp ip_or_host mac_address ?`
vlan	(Optional) VLAN number configured in a trunked interface on which the ARP address is configured. Enter an integer from 1 to 4094 as the VLAN number.

Usage Guidelines

To show static ARP mapping when you use the **show arp** command, the IP route must exist in the routing table. To view all static ARP entries, use the **show running-config** command.

The CSS discards ARP requests from hosts that are not on the same network as the CSS circuit IP address. Thus, if a CSS and a host are within the same VLAN but configured for different IP networks, the CSS does not respond to ARP requests from the host.

Related Commands

clear
show arp
show running-config
update arp

(config) arp timeout

To set the time in seconds to hold an ARP resolution result in the ARP cache, use the **arp timeout** command. Use the **no** form of this command to restore the default timeout value of 14400 seconds.

arp timeout *timeout_time*

no arp timeout

Syntax Description

timeout_time	Number of seconds to hold an ARP resolution result. To set a timeout period, enter an integer from 60 to 86400 (24 hours). The default is 14400 (4 hours). If you do not want the ARP entries to timeout, enter **none** or 86401.

Usage Guidelines

When you change the timeout value, it only affects new ARP entries. All previous ARP entries retain the old timeout value. To remove all entries with the old timeout value, enter the **clear arp cache** command.

Related Commands

clear arp cache
show arp config

(config) arp wait

To set the time in seconds to wait for an ARP resolution before discarding the packet waiting to be forwarded to the address, use the **arp wait** command. Use the **no** form of this command to restore the default wait time of 5 seconds.

arp wait *wait_time*

no arp wait

Syntax Description

wait_time	Number of seconds to wait for an ARP resolution. Enter an integer from 5 to 30. The default is 5 seconds.

Related Commands

show arp config

(config) boot

To access boot configuration mode, use the **boot** command. Boot configuration mode contains all commands necessary to manage booting the CSS and to maintain the software revision.

boot

Usage Guidelines

When you use the **boot** command to access boot mode, the prompt changes to (config-boot). For information about commands available in this mode, see the "Boot Configuration Mode Commands" section.

(config) bridge

To configure the spanning-tree bridge parameters that apply to the CSS, use the **bridge** command. The options for this global configuration mode command are:

- **bridge aging-time** - Sets the bridge filtering database aging time
- **bridge bpdu-guard** - Enables or disables the Bridge Protocol Data Unit (BPDU) guard feature on the CSS
- **bridge forward-time** - Sets the bridge forward delay time
- **bridge hello-time** - Sets the bridge hello time interval
- **bridge max-age** - Sets the bridge spanning-tree maximum age
- **bridge priority** - Sets the spanning-tree priority for the root bridge on the network
- **bridge spanning-tree** - Enables or disables the bridge spanning tree

For more information on these options and associated variables, see the following commands.

Note For information on bridge commands you can use in interface mode, see the **(config-if) bridge** command.

Related Commands

show bridge
(config) interface
(config-if) bridge

bridge aging-time

To set the spanning-tree bridge filtering database aging time for the CSS, use the **bridge aging-time** command. Use the **no** form of this command to restore the default aging time of 300.

bridge aging-time *timeout*

no bridge aging-time

Syntax Description

timeout	Timeout period in seconds for aging out dynamically learned forwarding information. Enter an integer from 10 to 1000000. The default is 300.

Command Modes

Global configuration mode

Related Commands

show bridge status

bridge bpdu-guard

To globally enable or disable the Bridge Protocol Data Unit (BPDU) guard feature on the CSS, use the **bridge bpdu-guard** command. The command shuts down PortFast-configured interfaces that receive BPDUs rather than putting the interfaces into the spanning-tree blocking state. By default, the BPDU guard feature is disabled.

bridge bpdu-guard [**enabled**|**disabled**]

Syntax Description

enabled	Enables the BPDU guard feature
disable	Disables the BPDU guard feature (default)

Command Modes

Global configuration

Usage Guidelines

The BPDU guard feature affects interfaces that have the PortFast feature enabled on them. PortFast should only be configured on interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt CSS and network operation. An interface with PortFast mode enabled is moved directly to the spanning-tree forwarding state when linkup occurs, without waiting for the standard forward-time delay.

When properly connected to other devices, PortFast-configured interfaces do not receive BPDUs. If a BPDU is received on a PortFast-configured interface, the interface is connected to an invalid device, such as a switch or router, and the BPDU guard feature disables the interface. The BPDU guard feature provides a secure response to invalid connections because you must manually put the interface back in service.

Related Commands

show bridge
(config-if) bridge port-fast

bridge forward-time

To set the spanning-tree bridge forward delay time, use the **bridge forward-time** command. Use the **no** form of this command to restore the default delay time of 4.

bridge forward-time *delay*

no bridge forward-time

Syntax Description

delay	Delay time in seconds that all bridges use for forward delay when this bridge is acting as the root. Enter an integer from 4 to 30. The default is 4.

Command Modes

Global configuration mode

Usage Guidelines

Make sure that the bridge maximum age is less than or equal to
2 x (bridge forward-time – 1 second) and greater than or equal to
2 x (bridge hello-time + 1 second).

Related Commands

show bridge status
(config) bridge max-age

bridge hello-time

To set the bridge hello time interval, use the **bridge hello-time** command. Use the **no** form of this command to restore the default hello time interval of 1.

bridge hello-time *hello*

no bridge hello-time

Syntax Description

hello	Hello time in seconds that all bridges use when this bridge is acting as the root. Enter an integer from 1 to 10. The default is 1.

Command Modes

Global configuration mode

Usage Guidelines

Make sure that the bridge maximum age is greater than or equal to 2 x (bridge hello-time + 1 second) and less than or equal to 2 x (bridge forward-time – 1 second).

Related Commands

show bridge status
(config) bridge max-age

bridge max-age

To set the bridge spanning-tree maximum age, use the **bridge max-age** command. Use the **no** form of this command to restore the default maximum age of 6.

bridge max-age *age*

no bridge max-age

Syntax Description

age	Maximum age in seconds that all bridges use when this bridge is acting as the root. Enter an integer from 6 to 40. The default is 6.

Command Modes

Global configuration mode

Usage Guidelines

Make sure that the bridge maximum age is greater than or equal to
2 x (bridge hello-time + 1 second) and less than or equal to
2 x (bridge forward-time – 1 second).

Related Commands

show bridge status
(config) bridge forward-time
(config) bridge hello-time

bridge priority

To set the priority used by the spanning-tree protocol to choose the root bridge on the network, use the **bridge priority** command. This command can override the root bridge selection in your network. Use the **no** form of this command to restore the default priority of 32768.

bridge priority *priority*

no bridge priority

Syntax Description

priority	Decimal value for the write portion of the bridge ID; the first two octets of the 8-octet bridge ID. The last 6 octets of the bridge ID come from the base bridge address. Enter an integer from 0 to 65535 (0 to ffff, hexadecimal). The default is 32768 (0x8000, hexadecimal).

Command Modes

Global configuration mode

Related Commands

show bridge status

bridge spanning-tree

To enable or disable the spanning tree, use the **bridge spanning-tree** command.

bridge spanning-tree [**disable**|**enable**]

Syntax Description

disable	Disables the spanning tree.
enabled	Enables the spanning tree. This is the default state.

Command Modes

Global configuration mode

Usage Guidelines

Disabling spanning-tree bridging may make your network susceptible to packet storms. When you disable spanning-tree bridging, the CSS drops Bridge Protocol Data Units (BPDUs), but forwards the Cisco Systems 802.1Q BPDUs (tagged with the proprietary 01-00-0c-cc-cc-cc-cd destination MAC address) on an 802.1Q VLAN trunk. The CSS can still operate in an 802.1Q spanning-tree environment as long as you do not require that the CSS put any of its ports into a blocking state.

Related Commands

show bridge status

(config) bypass persistence

To determine if the CSS performs either a service remapping or HTTP redirection operation to reset a bypassed service when a content request matches on a content rule, but a previous request caused the bypass, use the **bypass persistence** command. By default, **bypass persistence** is enabled.

bypass persistence [**disable**|**enable**]

Syntax Description

disable	Performs remapping or redirection to reset the connection according to the setting of the persistence reset method
enable	Does not perform remapping or redirection to reset the connection, and continues to bypass a service

Usage Guidelines

The **bypass persistence** command affects all flows.

Related Commands

show remap
(config) persistence reset
(config-owner-content) persistent

(config) cdp

To configure the global Cisco Discovery Protocol (CDP) parameters on the CSS, use the **cdp** command. The options for this global configuration mode command are:

- **cdp holdTime** - Defines the period of time to hold the CSS CDP information before discarding it
- **cdp run** - Enables CDP on the CSS and the broadcasting of CDPv1 advertisements by the CSS
- **cdp timer** - Specifies how often the CSS sends CDP advertisements to Cisco CDP-compatible devices

For more information on these options and associated variables, see the following commands.

Usage Guidelines

The Cisco Discovery Protocol (CDP) is a media-independent protocol that runs over Layer 2 (the data link layer) on the CSS and other Cisco-manufactured equipment, such as routers, switches, bridges, and access servers. CDP allows the CSS to advertise itself to all other neighboring Cisco CDP-compatible devices on a network.

Note The CSS only transmits CDP advertisements to other CDP-compatible devices on the network; it does not listen for CDP messages from other CDP-compatible devices.

Any Cisco device with CDP support can learn about the CSS by listening to the periodic advertisements transmitted by the CSS and determine when the CSS is active. Network operators and analysts can use this information for configuration monitoring, topology discovery, and fault diagnosis.

CDP advertisements include the following information about the CSS:

- Device ID (CSS base MAC address)
- IP address (CSS management port IP address)
- Ethernet port ID name
- CSS functional capability flag (router, transparent bridge, or switch)

- CSS software version
- CSS platform

CDP advertisements also include time-to-live, or hold-time information, which defines the length of time the receiving device is to hold CDP information before discarding it.

Related Commands

show cdp

cdp holdTime

To define the hold time in the CSS CDP advertisement to receiving devices, use the **cdp holdTime** command. The hold time defines how long the CSS wants the device to hold the CSS CDP information before discarding it. If a device does not receive a CSS CDP advertisement before the hold time expires, it drops the CSS as a neighbor. Use the **no** form of this command to reset the hold time to its default of 180 seconds.

cdp holdTime *seconds*

no cdp holdTime

Syntax Description

seconds	Number of seconds for holding the CSS CDP information. The range is from 10 to 255. The default is 180.

Command Modes

Global configuration mode

cdp run

To enable CDP transmissions to advertise the CSS in the form of CDPv1 packet broadcasts to neighboring Cisco CDP-compatible devices on the network, use the **cdp run** command. By default, CDP advertisement is disabled for the CSS. Use the **no** version of this command to disable the CSS CDP transmissions.

cdp run

no cdp run

Command Modes

Global configuration mode

cdp timer

To specify the interval at which the CSS advertises CDP packets to all receiving CDP-compatible devices, use the **cdp timer** command. Use the **no** form of the command to reset the interval to its default of 60 seconds.

cdp timer *interval*

no cdp timer

Syntax Description

interval	Number of seconds that the CSS advertises CDP packets. The range is from 5 to 254. The default is 60.

Command Modes

Global configuration mode

(config) circuit

To access circuit configuration mode and configure a circuit on the CSS, use the **circuit** command. A circuit on the CSS is a logical entity that maps IP interfaces to a logical port or group of logical ports.

circuit *circuit_name*

Syntax Description

circuit_name	Name of the circuit you want to configure. To see a list of available circuits, enter: `circuit ?`

Usage Guidelines

When you use the **circuit** command to access circuit mode, the prompt changes to (config-circuit [*circuit_name*]). For information about commands available in this mode, see the "Circuit Configuration Mode Commands" section.

Related Commands

show circuits

(config) cmd-sched

To enable command scheduling, use the **cmd-sched** command. Use the **no** form of this command to disable command scheduling.

cmd-sched
no cmd-sched

(config) cmd-sched record

To create a configuration record for the scheduled execution of any CLI commands, including the playing of scripts, use the **cmd-sched record** command. Use the **no** form of this command to delete a configuration record.

cmd-sched record *name minute hour day month weekday* **"***command...***"** {*logfile_name*}

no cmd-sched record

Syntax Description

name	Name of the configuration record. Enter an unquoted text string with a maximum of 16 characters. Any of the following time variables can contain one or some combination of the following values: • A single number to define a single or exact value for the specified time variable • A "*" wildcard character matching any valid number for the specified time variable • A list of numbers separated by commas, with a maximum of 40 characters, to define multiple values for a time variable • Two numbers separated by a dash (-) character indicating a range of values for a time variable
minute	Minute of the hour to execute the command. Valid numbers are from 0 to 59.
hour	Hour of the day. Valid numbers are from 0 to 23.
day	Day of the month. Valid numbers are from 0 to 31.
month	Month of the year. Valid numbers are from 1 to 12.
weekday	Day of the week. Valid numbers are from 1 to 7. Sunday is 1.

"*command...*"	The commands you want to execute. Enter a quoted text string with a maximum of 255 characters. Separate multiple commands with a semicolon (:) character. If the command string includes quoted characters, use a single quote character; any single quoted characters not preceded by a "\" character is converted to double quotes when the commands string is executed.
logfile_name	(Optional) Defines the name of the log file. Enter a text string with a maximum of 32 characters.

Usage Guidelines

The commands that the **cmd-sched record** command executes are referred to as the command string. To schedule commands, you must create a configuration record including when to execute the commands and the command string.

For example, you can use this command to schedule periodic content replication and configuration changes and gather statistics. At the specified time, the command scheduler executes a command string by creating a pseudo login shell where each string is executed. A cmd-sched record is only scheduled for execution upon completion of its shell. Use the **show lines** command to display information about active pseudo shells.

Note To terminate the execution of a command string, you can use the **disconnect** command.

Related Commands

disconnect
show cmd-sched
show lines

(config) console authentication

To configure the primary, secondary, or tertiary console port authentication of locally-defined usernames and passwords logging into the CSS, use the **console authentication** command. Use the **no** form of this command to disable authentication on the console port allowing users to access the CSS without a username and password.

console authentication [**primary** [**local**|**radius**|**tacacs**|**none**]
|**secondary**|**tertiary** [**local**|**radius**|**tacacs**|**none**|**disallowed**]]

no console authentication

Syntax Description

primary	Defines the first authentication method that the CSS uses. The default primary console authentication method is the local user database.
secondary	Defines the second authentication method that the CSS uses if the first method fails. The default secondary console authentication method is to disallow all user access. If you are configuring a TACACS+ server as the primary authentication method, define a secondary authentication method, such as **local**. If you do not configure a secondary method and use the default of **disallowed**, you have the possibility of being locked out of the CSS.
tertiary	Defines the third authentication method that the CSS uses if the second method fails. The default tertiary console authentication method is to disallow all user access.
local	The CSS uses the local user database for authentication.
radius	The CSS uses the configured RADIUS server for authentication.
tacacs	The CSS uses the configured TACACS+ server for authentication.

none	The CSS uses no authentication method. All users can access the CSS.
disallowed	The CSS does not allows access by all users (secondary or tertiary authentication method only). Entering this keyword does not terminate existing connections. To remove users currently logged into the CSS, use the **disconnect** command.

Usage Guidelines

To control access to the CSS, you can configure the CSS to authenticate console users. The CSS can authenticate users by using the local user database, RADIUS server, or TACACS+ server. You can also allow user access without authenticating or disallowing all remote user access to the CSS.

You can set a maximum of three authentication methods: a primary, secondary, or tertiary authentication method. The primary method is the first authentication method that the CSS tries. If the primary authentication method fails, the CSS tries the secondary method. If the secondary method fails, the CSS tries the tertiary method. In the event that the tertiary method also fails, the CSS displays a message that authentication has failed.

Before you can use RADIUS or TACACS+ as the console authentication method, you must enable communication with the RADIUS or TACACS+ security server. Use either the **(config) radius-server** command or the **(config) tacacs-server** command.

Related Commands

show user-database
(config) restrict console
(config) radius-server
(config) tacacs-server
(config) virtual authentication

(config) date european-date

To change the behavior of the **clock date** command to accept date input in the format of day, month, and year, use the **date european-date** command. Use the **no** form of this command to reset the format for the **clock date** command to its default format of month, day, and year.

date european-date

no date european-date

Related Commands

clock
show clock

(config) dfp

To configure a DFP agent listening for DFP connections on an IP address and TCP port combination on a server, and to enable the DFP manager on the CSS, use the **dfp** command. You can configure a maximum of 127 DFP agents for the DFP manager in the CSS. Use the **no** form of this command to disable the DFP agent connection to an IP address.

dfp *ip_or_host* {*port* {**key "***secret***"**|[**des-encrypted** *encrypted_key* |**"***encrypt_key***"**]} {**timeout** *seconds*} {**retry** *count*} {**delay** *time*} {**max-agent-wt** *weight*}

no dfp *ip_or_host* {*port*}

Syntax Description

ip_or_host	IP address or host name of the configured DFP agent. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or a mnemonic host name (for example, myhost.mydomain.com).
port	(Optional) Server TCP port that the configured DFP agent uses to listen for connections from the CSS DFP manager. Valid entries are 0 to 65535. The default is 14001.

key *"md5secret"*	(Optional) MD5 (Message Digest Algorithm Version 5) security key used for encryption to provide a secure data exchange between the CSS DFP load-balancing manager and the DFP agents. MD5 encryption is a one-way hash function that provides strong encryption protection. Enter the secret as a case-sensitive quoted text string (maximum of 64 characters). It can include any printable ASCII character except tabs. Ensure that you configure the same key on each DFP agent for MD5 encryption to function properly.
des-encrypted	(Optional) Defines a Data Encryption Standard (DES) encryption key.
encrypted_key	DES encryption key that the CSS had previously encrypted. The CSS does not reencrypt this key and saves it in the running-config as you entered it. Enter an unquoted case-sensitive text string with no spaces and a maximum of 128 characters.
"*encrypt_key*"	DES encryption key that you want the CSS to encrypt. The CSS saves the encrypted key in the running-config as you entered it. Enter a quoted case-sensitive text string with no spaces and a maximum of 64 characters.
timeout *seconds*	(Optional) Maximum inactivity time period (the keepalive time) for the connection between the CSS DFP manager and the server DFP agent. If the inactivity time period exceeds the timeout value, the DFP manager closes the connection. The DFP manager attempts to reopen the connection as often as specified by the value of the **retry** option. The range is from 1 to 10000 seconds. The default is 3600 seconds (1 hour).
retry *count*	(Optional) Number of times the CSS DFP manager tries to reopen a connection with the server DFP agent. The range is 0 (for continuous retries) to 65535. The default is three retry attempts.

delay *time*	Optional. The delay time, in seconds, between each connection reestablishment attempt. Valid entries are 1 (immediately) to 65535 seconds (18 hours). The default value is 5 seconds.
max-agent-wt *weight*	Optional. Maximum value of the weight reported by a DFP agent. A CSS uses this option to scale the reported weight when the weight range of a DFP agent does not match the weight range of the DFP manager. For example, the DFP manager weight range is 0 to 255. If a DFP agent reports weight in the range 0 to 16, the CSS scales up the agent-reported weight to match the weight range of the DFP manager. If an agent reports weight in the range 0 to 65535, the CSS scales down the agent-reported weight to match the weight range of the DFP manager. If a DFP agent reports a weight greater than the maximum configured weight, then the CSS rejects the weight report and does not use the weight in load-balancing decisions. In this case, the CSS also logs an error in SYSLOG. Enter an integer from 1 to 65535. The default is 255.

Related Commands

show dfp
show dfp-reports

(config) dhcp-agent max-hops

To set the maximum allowable number in the hops field of the BOOTP header, use the **dhcp-agent max-hops** command. The CSS does not forward packets with headers that have a larger number. Use the **no** form of this command to reset the maximum allowable number in the hops field to its default of 4.

dhcp-agent max-hops *number*

no dhcp-agent max-hops

Syntax Description

number	Maximum allowable number in the hops field of the BOOTP header. The range is 1 to 15. The default is 4.

Related Commands

show dhcp-relay-agent global

(config) dns

To enter commands that control the Domain Name System (DNS) client, the facility that translates host names such as myhost.mydomain.com to IP (Internet Protocol) addresses such as 192.168.11.1, use the **dns** command. The options for this global configuration mode command are:

- **dns primary** - Specifies the primary DNS server to use for DNS name resolution
- **dns secondary** - Specifies the secondary DNS server to use for DNS name resolution
- **dns suffix** - Specifies the default suffix to use during a DNS query

For information on these options and associated variables, see the following commands.

Related Commands

show running-config global
(config) dns-server

dns primary

To specify the primary DNS server to use for DNS queries and resolution, use the **dns primary** command. Use the **no** form of this command to remove the primary DNS server.

dns primary *ip_or_host*

no dns primary

Syntax Description

ip_or_host	Default DNS address to use for DNS queries. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1) or the mnemonic host name (for example, myhost.mydomain.com).

Command Modes

Global configuration mode

dns secondary

To specify the secondary DNS server, use the **dns secondary** command. When the primary server fails, the CSS uses the secondary server for DNS name resolution. Use the **no** form of this command to remove a secondary DNS server on a client.

dns secondary *ip_or_host*

no dns secondary *ip_or_host*

Syntax Description

ip_or_host	IP address for the secondary DNS server. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1) or the mnemonic host name (for example, myhost.mydomain.com).

Command Modes

Global configuration mode

Usage Guidelines

You can specify a maximum of two secondary servers. To specify each additional server, repeat the **dns secondary** command. The order in which you enter them is the order in which they are used if the primary DNS server fails.

dns suffix

To specify the default suffix to use when querying the DNS server to resolve a DNS name, use the **dns suffix** command. Use the **no** form of this command to remove the default suffix.

dns suffix *suffix*

no dns suffix

Syntax Description

suffix	Default suffix. Enter an unquoted text string with no spaces and a maximum length of 64 characters (for example, webhoster.com).

Command Modes

Global configuration mode

(config) dns-boomerang client

To configure and enable the Content Routing Agent (CRA) functionality on the CSS, use the **dns-boomerang client** command. The CSS functioning as a CRA improves HTTP response time for a client request. A Cisco Content Router 4430B configured as a Content Routing server redirects a client to the closest (best) replicated-content site represented by a CRA, based on network delay.

The options for this global configuration mode command are:

- **dns-boomerang client cpu-threshold** - Specifies the CPU load threshold for a CSS CRA
- **dns-boomerang client domain** - Creates a client domain record in the CSS CRA domain name server or creates a client alias record
- **dns-boomerang client enable** - Enables the CRA functionality on the CSS

For information on these options and associated variables, see the following commands.

Related Commands

show dns-boomerang client

dns-boomerang client cpu-threshold

To set the CPU load threshold for a CSS CRA, use the **dns-boomerang client cpu-threshold** command. If the CSS CPU load exceeds the configured threshold value, then the CSS drops incoming DNS requests from the Content Router. Use the **no** form of this command to reset the CSS CPU threshold to the default value of 99.

dns-boomerang client cpu-threshold *number*

no dns-boomerang client cpu-threshold

Syntax Description

number	The load threshold value. Enter a number from 1 to 99. The default value is 99.

Command Modes

Global configuration mode

Usage Guidelines

The load threshold value is the percentage of CPU utilization shown in the **show system-resources** command.

Related Commands

show system-resources
(config) dns-boomerang client domain

dns-boomerang client domain

To create a client domain record in the CSS CRA or an alias for the record, use the **dns-boomerang client domain** command. The record maps to each of the domains you associated with the agent when you configured domains on the Content Router. Use the **no** form of this command to remove a client domain or the alias for the domain.

dns-boomerang client domain *dns_name* [**alias** *alias_name*|*ip_or_host* {**“***uri***”**} {**key** [**“***secret***”**|**des-encrypted** *encrypted_key*|**“***encrypt_key***”**]} {**dns-ttl** *number1*} {**ip-ttl** *number2*} {**threshold** *number3*}]

no dns-boomerang client domain *dns_name* {**alias** *alias_name*}

Syntax Description

dns_name	Domain name mapped to the client record. Enter the name as a case-sensitive, unquoted text string with no spaces and a maximum length of 72 characters. For example, www.sample.com.
alias	Creates an alias for an existing client domain. The alias behaves exactly the same as the configured domain.
alias_name	Alias name for the associated DNS name. Enter the name as a case-sensitive unquoted text string with no spaces and a maximum length of 72 characters.

ip_or_host	IP address or host name of the content server or web cache bound to the domain name on the CSS. This address can be a local VIP. Enter the address in dotted-decimal notation (for example, 192.168.11.1) or a mnemonic host name (for example, myhost.mydomain.com).
"*uri*"	(Optional) Defines the URI that the CSS uses for the keepalive probe to the Content Router for a domain. Enter a quoted text string with a maximum of 255 characters. If you do not prepend the URI with a slash (/) character, the CSS prepends it.
key	(Optional) Defines the clear-text secret or DES encryption key on the Content Router.
"*secret*"	Clear-text secret for encrypting packets sent between a Content Router and the CSS client. The secret is the same as the secret on the CR. Enter the secret as a case-sensitive quoted text string with a maximum of 64 characters.
des-encrypted	(Optional) Defines a Data Encryption Standard (DES) encryption key.
encrypted_key	DES encryption key that the CSS had previously encrypted. The CSS does not reencrypt this key and saves it in the running-config as you entered it. Enter an unquoted case-sensitive text string with no spaces and a maximum of 64 characters.
"*encrypt_key*"	DES encryption key that you want the CSS to encrypt. The CSS saves the encrypted key in the running-config as you entered it. Enter a quoted case-sensitive text string with no spaces and a maximum of 16 characters.
dns-ttl *number1*	(Optional) Defines the DNS time-to-live value returned with the DNS responses of the CSS client. This keyword determines the length of time that a domain name server caches the returned information for reuse. Enter an integer from 10 to 2147483647 seconds. The default value is from the Content Router.

ip-ttl *number2*	(Optional) Defines the IP routing time-to-live value in hops that is set in the IP packets for returned CSS client DNS responses. This keyword determines how many router hops a response packet traverses en route to the client's local name server, D-Proxy, before it is discarded. This helps to eliminate the CSS client from longer races. Enter an integer from 1 to 255. The default value is from the Content Router.
threshold *number3*	(Optional) Defines the load threshold for testing the keepalive state of a local VIP. If the load on the associated rule is greater than the threshold, then the CSS drops Content Router requests until the load goes below the threshold. Enter an integer from 2 to 254. The default value is 254.

Command Modes

Global configuration mode

Usage Guidelines

If the matching domain record keepalive messaging succeeds, the CSS uses this record for DNS resolutions and will respond to the D-Proxy on behalf of the Content Router.

dns-boomerang client enable

To enable the Content Routing Agent (CRA) functionality on a CSS, use the **dns-boomerang client enable** command. Use the **no** form of this command to disable the CRA functionality.

dns-boomerang client enable

no dns-boomerang client enable

Command Modes

Global configuration mode

Usage Guidelines

Before you enable the CRA functionality on a CSS, configure a Cisco Content Router 4430B as a Content Routing server and CRAs on the server. For information on configuring the server, refer to the *Cisco Content Router 4430B User Guide*.

(config) dns-peer

To control the DNS peer functionality on the CSS, use the **dns-peer** command. You can configure the CSS as a DNS peer to exchange DNS information over an APP connection to other CSSs. The options for this global configuration mode command are:

- **dns-peer interval** - Sets the time between sending load reports to each CSS DNS peer
- **dns-peer load-variance** - Sets the range of load numbers between peers that a CSS considers to be similar for the least-loaded algorithm in a DNS load-balancing decision
- **dns-peer receive-slots** - Sets the maximum number of DNS names that the CSS can receive from each CSS DNS peer
- **dns-peer send-slots** - Sets the maximum number of DNS names that the CSS can send to each CSS DNS peer

For information on these options and associated variables, see the following commands.

Related Commands

show dns-peer
(config) app
(config) dns
(config-owner) dns
(config-owner-content) add dns

dns-peer interval

To set the time between sending load reports to CSS DNS peers over an APP connection, use the **dns-peer interval** command. Use the **no** form of this command to reset the interval to its default value of 5.

dns-peer interval *number*

no dns-peer interval

Syntax Description

number	Time in seconds between generating load reports. Enter an integer from 5 to 120. The default is 5.

Command Modes

Global configuration mode

dns-peer load-variance

To set the range of load numbers between peers that a CSS considers to be similar for the least-loaded algorithm in a DNS load-balancing decision, use the **dns-peer load-variance** command. If the load numbers of all peers are within the specified range, the CSS calculates the minimum response time of each site, then selects the site with the fastest response time. Use the **no** form of this command to reset the **load-variance** to its default value of 50.

dns-peer load-variance *number*

no dns-peer variance

Syntax Description

number	Upper limit of the range of load numbers considered similar. Enter an integer from 0 to 254. The default is 50.

Command Modes

Global configuration mode

Usage Guidelines

If you configure the absolute load calculation method for GSLB, Cisco Systems recommends that you configure a load variance of 0, regardless of whether you are using zone-based or rule-based DNS load balancing. For information on absolute load calculation, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

dns-peer receive-slots

To set the maximum number of DNS names that the CSS can receive from each CSS DNS peer over an APP connection, use the **dns-peer receive-slots** command. Use the **no** form of this command to reset the maximum number of DNS names received from a peer to its default value of 128.

dns-peer receive-slots *number*

no dns-peer receive-slots

Syntax Description

number	Maximum number of DNS names that can be received from a peer. Enter an integer from 128 to 1024. The default is 128.

Command Modes

Global configuration mode

dns-peer send-slots

To set the maximum DNS names that the CSS can send to each CSS DNS peer, use the **dns-peer send-slots** command. Use the **no** form of this command to reset the maximum number of DNS names sent to a peer to its default value of 128.

dns-peer send-slots *number*

no dns-peer send-slots

Syntax Description

number	Maximum number of DNS names sent to a peer. Enter an integer from 128 to 1024. The default is 128.

Command Modes

Global configuration mode

(config) dns-record

To create a domain record, use the **dns-record** command and its options. This command is not available on a Proximity Database CSS. The command options are:

- **dns-record a** - Creates a domain record on the CSS Zone Domain Name Server mapped directly to an IP address
- **dns-record accel** - Creates a domain acceleration record on the CSS mapped to a content rule through an IP address
- **dns-record ns** - Creates a domain record on the CSS Zone Domain Name Server mapped to a name server IP address
- **dns-record zero** - Resets the DNS record statistics to zero

For information on these options and associated variables, see the following commands.

Related Commands

show dns-record
(config) dns-server {**zone**}

dns-record a

To create a domain record on the CSS Zone Domain Name Server that maps the DNS name to an IP address, use the **dns-record a** command. If a domain *can* be directly translated to an IP address, configure it as an A-record. Use the **no** form of this command to delete a domain address record.

dns-record a *dns_name ip_address* {*ttl_value* {**single|multiple** {**kal-ap-vip|kal-ap|kal-icmp|kal-none** {*ip_address2* {*threshold* {**sticky-disabled|sticky-enabled** {**usedefault|weightedrr|srcip |leastloaded|preferlocal|roundrobin|proximity** {*weight*}}}}}}}}

no dns-record a *dns_name*

Syntax Description

dns_name	DNS name mapped to the address record. Enter the name as a case-sensitive, unquoted text string with no spaces and a maximum of 63 characters.
ip_address	IP address bound to the *dns_name* within the CSS zone. Enter the address in dotted-decimal notation (for example, 192.168.11.1). This is the VIP for which a CSS client sends a **kal-ap-vip** request to itself or another CSS agent for load information.
ttl_value	(Optional) Time to Live (TTL) value in seconds. This value determines how long the DNS client remembers the IP address response to the query. Enter a value from 0 to 65535. The default is 0.
single|multiple	(Optional) Number of records to return on a DNS response message. Enter either **single** or **multiple**. By default, the DNS server returns a single a-record. Setting this parameter to **single** ensures that only one a-record is returned.

kal-ap|kal-icmp| **kal-none**	(Optional) Keepalive message type for this record. The types are: • **kal-ap** - The keepalive message type keyword that specifies the CSS keepalive message. This is the recommended keepalive message type to obtain load information from remote as well as local services based on domains configured on a single content rule. **Note** To use **kal-ap** proximity keepalive messages, lower-level CSSs acting as either data centers or DNS servers must be running the Enhanced feature set. When the Proximity Domain Name Server (PDNS) is directly attached to a server farm, an internal keepalive is used. • **kal-icmp** - The keepalive message type keyword that specifies ICMP echo (ping). To obtain load information from local services only, use the **add dns** *record_name* command in the associated content rule. This is the default setting. • **kal-none** - For no keepalive messaging.
ip_address2	(Optional) IP address of the local interface receiving CSS keepalive messages.
threshold	(Optional) Load threshold used with the CSS proximity keepalive. The CSS considers that this record is in the Down state when the load number is greater than this value. Enter a value from 2 to 254. The default is 254.

sticky-disabled **|sticky-enabled**	(Optional) Disables or enables DNS sticky for the domain. The **sticky-disabled** option disables DNS sticky for the specified domain. This is the default setting.
usedefault	(Optional) Returns domain records using the default DNS load-balancing method configured for the zone.
weightedrr	(Optional) Returns domain records based on the weighted roundrobin load-balancing method. This method uses the *weight* value to determine the zone from which the record should be requested.
srcip	(Optional) Returns domain records using a source IP address hash. For sticky-enabled domains without a GSDB, the CSS uses the srcip method regardless of the configured balance method. For sticky-enabled domains with a GSDB, a CSS uses the configured balance method when the GSDB does not contain an entry for the requested domain.
leastloaded	(Optional) Returns domain records from the zone with the smallest load.
preferlocal	(Optional) Returns local domain records whenever possible. If no local record exists, the CSS uses the balance method configured for the zone with the lowest zone index.
roundrobin	(Optional) Returns domain records by cycling among records available at the different zones to evenly distribute the load.
proximity	(Optional) Returns domain records based on proximity information. If a PDB is not configured or is unavailable in a zone, the CSS applies the default balance method for the selected zone for DNS resolution. This is the default method.

weight	(Optional) Value assigned to a domain in the local zone to determine how many requests the local zone receives for the specified domain compared with other zones in a peer mesh. A domain with a weight of 10 in the local zone will receive twice as many requests as the same domain in another zone with a weight of 5. Use this parameter with the **weighted** roundrobin DNS load-balancing method. CSSs configured as authoritative DNS servers in a peer mesh share domain weights with each other. Enter an integer from 0 to 10 The default is 1. For details on configuring a DNS record with a *weight* of 0, refer to the *Cisco Content Services Switch Global Server Load-Balancing Configuration Guide*.

Command Modes

Global configuration mode

Usage Guidelines

This command is available on a CSS PDNS.

If you need to modify an existing A-record configuration, you must first remove the record using the **no dns-record a** *domain_name* command. Then, recreate the A-record with the change using the **dns-record a** command.

When you enable DNS Sticky through the **sticky-enabled** option, the CSS makes a decision based on one of the following three scenarios:

- In a global server load-balancing (GSLB) environment without a global sticky database (GSDB), the CSS selects a server based on the srcip hash (regardless of the default load-balancing method) and the availability of the domain in the zone mesh. The use of the srcip hash ensures that the CSS selects a consistent zone for a given source IP address.

  In a GSLB environment with a GSDB, the CSS sends a lookup request to the Global Sticky Database for the requesting client’s local DNS server. If the GSDB has an entry in its sticky database for the client’s local DNS server IP address, it returns the appropriate zone index to the CSS. The CSS then returns the associated IP address to the client. Otherwise, the CSS selects a zone based on the default load-balancing method and informs the GSDB about the selected zone.

- In a Network Proximity environment, the CSS configured as a Proximity Domain Name Server (PDNS) first consults the GSDB. If a sticky database entry exists for the client's local DNS server IP address, the PDNS sends the appropriate IP address to the client based on the zone index returned by the GSDB. If the GSDB does not contain an entry for the client's local DNS server IP address, the PDNS consults the Proximity Database (PDB).
- If the PDB contains an entry for the client's local DNS server IP address, the PDNS formulates a response to the client based on the ordered zone index returned by the PDB and keepalive information. The PDNS informs the GSDB about the selected zone (performs a "set" function). If the PDB does not have an entry for the client's local DNS server IP address or the sticky zone is unavailable, the CSS selects a zone based on its default load-balancing method and informs the GSDB about the selected zone.

Note If you configure any sticky domains in a particular zone, you must configure all sticky domains participating in the peer mesh in that same zone. Otherwise, the thrashing of the sticky zone index will cause DNS Sticky to fail.

For details on configuring DNS Sticky, refer to the *Cisco Content Services Switch Global Server Load-Balancing Configuration Guide*.

The CSS uses the following guidelines when selecting a DNS load-balancing method on a domain basis:

- If a local record exists, the CSS uses the configured domain balance method to determine local DNS resolutions. This applies regardless of the local record's keepalive state.
- If no local record exists, the CSS uses the balance method configured for the zone with the lowest zone index.

To provide backup sites in a DNS weighted roundrobin configuration when all domain records with weights from 1 to 10 are unavailable, configure domain records with a weight of zero. When a DNS record has a weight of zero, a CSS does not consider that record for selection when using the weighted roundrobin algorithm unless all of the other records, with weights from 1 to 10, are unavailable. This feature is intended especially for use in disaster recovery sites. For details, refer to the *Cisco Content Service Switch Global Server Load-Balancing Configuration Guide*.

Related Commands

show dns-record

dns-record accel

To create a DNS acceleration record for the domains you want to accelerate on the CSS, use the **dns-record accel** command. Use the **no** form of this command to delete a DNS acceleration record.

dns-record accel *dns_name ip_address* {*ageout*}

no dns-record accel *dns_name*

Syntax Description

dns_name	DNS name you want to map to the acceleration record. Enter a case-sensitive unquoted text string with no spaces and a maximum of 63 characters.
ip_address	IP address of the local content rule that will handle content request for the DNS name during content acceleration.
ageout	(Optional) Number of minutes that the domain remains accelerated. Enter a number from 0 to 525600. The default is 180 minutes. If you enter 0, the accelerated domain record does not age out.

Usage Guidelines

The DNS acceleration record indicates a DNS name that is eligible for content acceleration. The record maps the name to a content rule through an IP address. To enable the acceleration of domains, use the **(config) dns-server accelerate domains** command. The **dns-record accel** command is *not* available on a Proximity Database CSS.

Configure nonaccelerated domains as either A-records or NS-records.

Note If the content rule associated with the acceleration candidate domain is suspended or cannot provide service for content requests, the CSA does not accelerate the domain.

Related Commands

show dns-record accel
(config) dns-server accelerate domains

dns-record ns

To create a domain record on the CSS Zone Domain Name Server that maps the DNS name to a Name Server IP address, use the **dns-record ns** command. If a domain *cannot* be directly translated to an IP address, configure it as an NS-record. Use the **no** form of this command to delete a DNS record.

dns-record ns *dns_name ip_address* {*ttl_value* {**single|multiple** {**kal-ap-vip|kal-ap|kal-icmp|kal-none** {*ip_address2* {*threshold* {**default|forwarder** {**sticky-disabled|sticky-enabled** {*weight* {**usedefault|weightedrr|srcip|leastloaded|preferlocal |roundrobin|proximity**}}}}}}}}}

no dns-record ns *dns_name*

Syntax Description

dns_name	DNS name mapped to the name server record. Enter the name as a case-sensitive, unquoted text string with no spaces and a maximum of 63 characters.
ip_address	IP address of the DNS server bound to the *dns_name* within the CSS zone. Enter the address in dotted-decimal notation (for example, 192.168.11.1).
ttl_value	(Optional) Time to Live (TTL) value in seconds. This value determines how long the DNS client remembers the IP address response to the query. Enter a value from 0 to 65535. The default is 0.
single|multiple	(Optional) Number of records to return on a DNS response message. Enter either **single** or **multiple**. By default, the DNS server returns a single ns-record. Setting this parameter to **single** ensures that only one ns-record is returned.

kal-ap| **kal-icmp**| **kal-none**	(Optional) Keepalive message type for this record. The types are: • **kal-ap** - For the CSS keepalive message. • **kal-icmp** - For an ICMP echo message (ping). This is the default setting. • **kal-none** - For no keepalive messaging.
ip_address2	(Optional) IP address of the local interface receiving CSS keepalive messages.
threshold	(Optional) Load threshold for the record. The CSS considers that the record is in the Down state when the load number is greater than this value. Enter a value from 2 to 254. The default is 254.
default	(Optional) Uses PDB information to return the next most proximate location. When a PDB is not available or configured, the roundrobin method is used.
forwarder	(Optional) Eliminates a potential single point of failure by providing a maximum of two alternative DNS servers called forwarders. A forwarder can be a CSS configured as a DNS server or a fully-functional BIND DNS server. If an optimal miss occurs (the lower-level DNS server indicated in the NS-record is Down), the PDNS sends the DNS request to the primary or secondary forwarder, depending on forwarder health and configuration. An optimal miss occurs when the PDNS cannot return the NS-record for the zone that the PDB indicated was most proximate. For this failover to occur, the local NS-record must be in the Down state, and the PDB has indicated the local zone to be the zone most proximate to the client.
sticky-disabled |**sticky-enable**	(Optional) Disables or enables DNS sticky for the domain. The **sticky-disabled** option disables DNS sticky for the specified domain. This is the default setting.

weight	(Optional) Value assigned to a domain in the local zone to determine how many requests the local zone receives for the specified domain compared with other zones in a peer mesh. A domain with a weight of 10 in the local zone will receive twice as many requests as the same domain in another zone with a weight of 5. Use this parameter with the **weighted** roundrobin DNS load-balancing method. CSSs configured as authoritative DNS servers in a peer mesh share domain weights with each other. Enter an integer from 0 to 10 The default is 1. For details on configuring a DNS record with a *weight* of 0, refer to the *Cisco Content Services Switch Global Server Load-Balancing Configuration Guide*.
usedefault	(Optional) Returns domain records using the default DNS load-balancing method configured for the zone.
weightedrr	(Optional) Returns domain records based on the weighted roundrobin load-balancing method. This method uses the *weight* value to determine the zone from which the record should be requested.
srcip	(Optional) Returns domain records using a source IP address hash. For sticky-enabled domains without a GSDB, the CSS uses the srcip method regardless of the configured balance method. For sticky-enabled domains with a GSDB, a CSS uses the configured balance method when the GSDB does not contain an entry for the requested domain.
leastloaded	(Optional) Returns domain records from the zone with the smallest load.
preferlocal	(Optional) Returns local domain records whenever possible. If no local record exists, the CSS uses the balance method configured for the zone with the lowest zone index.

roundrobin	(Optional) Returns domain records by cycling among records available at the different zones to evenly distribute the load.
proximity	(Optional) Returns domain records based on proximity information. If a PDB is not configured or is unavailable in a zone, the CSS applies the default balance method for the selected zone for DNS resolution. This is the default method.

Command Modes

Global configuration mode

Usage Guidelines

This command is available on a CSS PDNS.

If you need to modify an existing NS-record configuration, you must first remove the record using the **no dns-record ns** *domain_name* command. Recreate the NS-record with the change using the **dns-record ns** command.

When you enable DNS Sticky through the **sticky-enabled** keyword, The CSS makes a decision based on one of the following three scenarios:

- In a global server load-balancing (GSLB) environment without a global sticky database (GSDB), the CSS selects a server based on the srcip hash (regardless of the default load-balancing method) and the availability of the domain in the zone mesh. The use of the srcip hash ensures that the CSS selects a consistent zone for a given source IP address.

  In a GSLB environment with a GSDB, the CSS sends a lookup request to the Global Sticky Database for the requesting client's local DNS server. If the GSDB has an entry in its sticky database for the client's local DNS server IP address, it returns the appropriate zone index to the CSS. The CSS then returns the associated IP address to the client. Otherwise, the CSS selects a zone based on the default load-balancing method and informs the GSDB about the selected zone.

- In a Network Proximity environment, the CSS configured as a Proximity Domain Name Server (PDNS) first consults the GSDB. If a sticky database entry exists for the client's local DNS server IP address, the PDNS sends the appropriate IP address to the client based on the zone index returned by the GSDB. If the GSDB does not contain an entry for the client's local DNS server IP address, the PDNS consults the Proximity Database (PDB).
- If the PDB contains an entry for the client's local DNS server IP address, the PDNS formulates a response to the client based on the ordered zone index returned by the PDB and keepalive information. The PDNS informs the GSDB about the selected zone (performs a "set" function). If the PDB does not have an entry for the client's local DNS server IP address or the sticky zone is unavailable, the CSS selects a zone based on its default load-balancing method and informs the GSDB about the selected zone.

Note If you configure any sticky domains in a particular zone, you must configure all sticky domains participating in the peer mesh in that same zone. Otherwise, the thrashing of the sticky zone index will cause DNS Sticky to fail.

For details on configuring DNS Sticky, refer to the *Cisco Content Services Switch Global Server Load-Balancing Configuration Guide*.

The CSS uses the following guidelines when selecting a DNS load-balancing method on a domain basis:

- If a local record exists, the CSS uses the configured domain balance method to determine local DNS resolutions. This applies regardless of the local record's keepalive state.
- If no local record exists, the CSS uses the balance method configured for the zone with the lowest zone index.

To provide backup sites in a DNS weighted roundrobin configuration when all domain records with weights from 1 to 10 are unavailable, configure domain records with a weight of zero. When a DNS record has a weight of zero, a CSS does not consider that record for selection when using the weighted roundrobin algorithm unless all of the other records, with weights from 1 to 10, are unavailable. This feature is intended especially for use in disaster recovery sites. For details, refer to the *Cisco Content Service Switch Global Server Load-Balancing Configuration Guide*.

Related Commands

show dns-record
(config) dns-server forwarder

dns-record zero

To reset the statistics or counters displayed by the **show dns-record** command to zero for all domain records or a specific domain name, use the **dns-record zero** command.

dns-record zero [**a/ns** {*domain_name*}|**accel** {*domain_name*}]

Syntax Description

a/ns	Resets the statistics for the domain records displayed by the **show dns-record statistics** command and the **show dns-record proximity** command.
domain_name	(Optional) Specified domain name mapped to the DNS record. To view a list of domain names, enter: `dns-record zero [a/ns|accel] ?`
accel	(Optional) Resets the counters for the acceleration records displayed by the **show dns-record accel** command.

Usage Guidelines

The **dns-record zero** command is *not* available on a Proximity Database CSS.

Related Commands

show dns-record
(config) dns-record

(config) dns-server

To enable the DNS server function on the CSS, use the **dns-server** command. The CSS acts as the authoritative name server for the content domain. Use the **no** form of this command to disable DNS server functionality on the CSS.

dns-server

no dns-server

Related Commands

show dns-server
show zone
(config) app
(config) dns
(config-owner) dns
(config-owner-content) add dns

(config) dns-server accelerate domains

To enable the domain acceleration and configure the Client Side Accelerator (CSA) on the CSS, use the **dns-server accelerate domains** command. Use the **no** form of this command to disable domain acceleration.

dns-server accelerate domains {*threshold interval max_number* [**single-location**|**multi-location**]}

no dns-server accelerate domains

Syntax Description

threshold	(Optional) Hits threshold used to determine whether a domain is accelerated. When the hits on the domain are greater than or equal to the threshold, the CSA accelerates the domain. Enter a number from 0 to 65535. The default is 0, indicating that the CSA always accelerates the candidate domains.
interval	Interval in minutes over which the CSA samples the hits on the domain and compares the hits with the threshold. Enter a number from 1 to 3600. The default is 5.
max_number	Maximum number of domains that the CSA can accelerate. Enter a number from 0 to 4096. The default is 1024.
single-location	Allows CSA peers to share content by maintaining the content on the cache farm of a single CSA.
multi-location	Allows multiple CSAs to accelerate the same domain resulting in multiple cache farms maintaining the same content. This can occur when two or more CSAs (located in different POPs) are configured for multi-location and accelerate the same domain. Each cache farm maintains the same content after: • The CSAs accelerate the same domain. • A cache in each POP retrieves the same content from the origin server.

Usage Guidelines

Use the **dns-server accelerate** command to enable the acceleration of domains configured through the **dns-record accel** command.

Related Commands

show dns-server accelerate domains
(config) dns-record accel

(config) dns-server bufferCount

To change the DNS response buffer count on the CSS, use the **dns-server bufferCount** command. Use the **no** form of this command to set the DNS response buffer count to its default value of 50.

dns-server bufferCount *number*

no dns-server bufferCount

Syntax Description

number	Number of buffers allocated for query responses. Enter an integer from 2 to 1000. The default is 50.

Usage Guidelines

Only use the **dns-server bufferCount** command to tune the CSS if the CSS experiences buffer depletion during normal use. If the name server buffers (NS Buffers) drop below two, increase the buffer count and the responder task with the **(config) dns-server respTasks** command. To view the buffers, use the **show dns-server** command.

Related Commands

show dns-server

(config) dns-server domain-cache

To enable domain caching to track DNS request counts and configure the parameters for the domain cache on the CSA, use the **dns-server domain-cache** command. Use the **no** form of this command to disable domain caching.

dns-server domain-cache {*cache_size ageout*|**purge** {*dns_name*}
|**zero** {*dns_name*}}

no dns-server domain-cache

Syntax Description

cache_size	(Optional) Number of domains that the CSA can cache. Enter a number from 1 to 4096. The default is 1024.
ageout	(Optional) Maximum number of seconds that the domain entry remains in cache. Enter a number from 0 to 60. The default is 10 seconds. If you enter 0, the domain entries remain in cache unless they are removed with the **purge** option.
purge	(Optional) Removes all entries or the specified entries in the domain cache.
dns_name	(Optional) DNS entry in the domain cache. To see a list of entries, enter: `dns-server domain-cache [purge|zero] ?`
zero	(Optional) Resets all counters for all entries or the specified entry in the domain cache displayed through the **show dns-server domain-cache** command.

Usage Guidelines

Use the **dns-server domain-cache** command to create the domain cache and enable it. The domain cache records all domains including accelerated domains.

Enabling or disabling the domain cache does not affect domain acceleration. The operation of the domain cache can impact the DNS request/response rate performance. Use the domain cache only when you need to identify potential acceleration candidates.

Related Commands

show dns-server domain-cache

(config) dns-server forwarder

To configure a DNS server forwarder on a CSS, use the **dns-server forwarder** command. The forwarder is an alternative server for resolving DNS requests. In the case of proximity, the forwarder is a CSS in the same zone as the PDB. When the CSS is acting as a CSA, the forwarder is a fully-functional Berkeley Internet Name Domain (BIND) DNS server, not a CSS. Use the **no** form of this command to delete the DNS forwarder.

dns-server forwarder [**primary** *ip_address*|**secondary** *ip_address*|**zero**]

no dns-server forwarder primary|secondary

Syntax Description

primary	Specifies the first choice forwarder. The CSS sends unresolvable requests to the primary forwarder unless it is unavailable, in which case, it uses the secondary forwarder. When the primary forwarder is available again, the CSS resumes sending requests to the primary forwarder.
secondary	Specifies the second choice as the forwarder.
ip_address	IP address for the DNS forwarder. Enter the address in dotted-decimal notation (for example, 192.168.11.1).
zero	Resets the statistics of both forwarders on the CSS. The statistics are displayed through the **show dns-server forwarder** command.

Usage Guidelines

The CSS uses the primary forwarder first. If it is unavailable, the CSS uses the secondary forwarder.

The forwarder receives DNS requests that the CSS cannot resolve, or that contain an unsupported request or record type. The forwarder sends DNS responses to the client transparently through the CSS. To monitor forwarder health, an internal keepalive mechanism sends queries periodically to validate the state of the forwarder.

Related Commands

show dns-server forwarder
(config) dns-record ns

(config) dns-server respTasks

To change the DNS server responder task count, use the **dns-server respTasks** command. These tasks handle responses to incoming DNS query requests. Use the **no** form of this command to set the DNS responder task count to its default value of 2.

dns-server respTasks *number*

no dns-server respTasks

Syntax Description

number	Number of tasks. Enter an integer from 1 to 250. The default is 2.

Usage Guidelines

If you increase the responder task count, also increase the buffer count with the **(config) dns-server bufferCount** command.

(config) dns-server zero

To set the DNS server request and response statistics displayed by the **show dns-server** command to zero, use the **dns-server zero** command.

dns-server zero

Usage Guidelines

The **dns-server zero** command is *not* available on a Proximity Database CSS.

Related Commands

show dns-server
(config) dns-server

(config) dns-server zone

To enable the CSS Zone Domain Name Server (DNS) on a CSS or configure how the CSS handles the least-loaded balance method, use the **dns-server zone** command. This service allows the CSS to respond to DNS requests based upon proximity and shared zone domain availability. Use the **no** form of this command to disable the CSS Proximity Domain Name Server or disable DNS server zone load reporting.

dns-server zone *zoneIndex* {**tier1**|**tier2** {"*description*" {**weightedrr**|**srcip**|**leastloaded**|**preferlocal**|**roundrobin**|*ip_address* {**weightedrr**|**srcip**|**leastloaded**|**preferlocal**|**roundrobin**} {*weight*}}}} |**load** [**reporting**|**frequency** *seconds*|**variance** *number*]

no dns-server zone|**load** [**reporting**|**frequency**|**variance**]

Syntax Description

zoneIndex	Numerical identifier of the Proximity Zone of the CSS. This number should match the *zoneIndex* configured on the Proximity Database in a dedicated CSS 11150. Enter an integer from 0 to 15.
tier1|**tier2**	(Optional) Maximum number of zones the CSS expects to participate in its proximity zone mesh. Enter **tier1** for a maximum of 6 zones, numbered 0 to 5. Enter **tier2** for a maximum of 16 zones, numbered 0 to 15. Tier1 is the default. For CSA applications, the tier you select must be the same as the tier for the other CSAs participating in the mesh.
"*description*"	(Optional) Text description of the CSS zone. Enter a quoted string with a maximum of 20 characters.
ip_address	(Optional) IP address of the PDB. Enter the address in dotted-decimal notation (for example, 192.168.11.1). This enables the DNS server to respond to DNS requests based on proximity. For CSA applications, do not enter an IP address.

weightedrr| **roundrobin** **|srcip** **|leastloaded** **|preferlocal**	(Optional) Balance method to determine the algorithm that the DNS server uses to choose returned records when a PDB is unavailable or not configured. • **weightedrr** - The CSS gives a zone priority over other zones in a peer mesh according to the assigned domain weights. Each CSS in the mesh maintains an internal list of zones ordered from highest to lowest according to weight. The heaviest zone (the zone with the highest weight number) receives DNS requests until it reaches its maximum number of requests, then the next heaviest zone receives DNS requests until it reaches its maximum, and so on. When all the zones have reached their maximum number of requests, the CSS resets the counters and the cycle starts over again. When you add a new DNS zone, each CSS adds the new zones to its list by weight. In this case, the CSSs do not reset their hit counters. This process prevents flooding of the heaviest zone every time you add or remove a zone. For example, a domain with a weight of 10 in the local zone will receive twice as many hits as the same domain with a weight of 5 in another zone. You assign domain weights using the **dns-record** command. • **roundrobin** - The CSS cycles between records available from different zones. This is the default method. • **srcip** - The CSS uses a source IP address hash to select the zone index to return to the client. • **leastloaded** - The CSS reports loads and selects a record from the zone that has the least traffic. • **preferlocal** - The CSS returns a record from the local zone whenever possible. Otherwise, the server uses the roundrobin method.

weight	(Optional) Default weight applied to all DNS records in the zone if you do not configure a weight for individual records using the **dns-record** command. Enter an integer from 0 to 10. The default is 1. To display the weight that you configured on a record using either the **dns-server zone** command or the **dns-record** command, enter the **show dns-record weight** command.
reporting	Enables the processing of local DNS server zone load information and sharing it with peers. The default is enabled.
frequency *seconds*	Specifies the period of time in seconds between processing local DNS server load information and the subsequent delivery of load information to peers. Enter an integer from 5 and 300 seconds (5 minutes). The default is 30 seconds.
variance *number*	Specifies the range of load numbers between zones that will be considered similar. If the load numbers of all zones are within the specified range, the CSS uses response times to identify the least-loaded site. Enter an integer from 0 to 255. The default is 255.

Usage Guidelines

The **dns-server zone** command is available in the CSS Enhanced feature set.

If you need to modify a **dns-server zone** value, you must first disable the DNS server using the **no dns-server** command and then remove the zone using the **no dns-server zone** command. Restore the DNS server zone with the value change, and then reenable the DNS server. To enable or disable the **dns-server zone load reporting** command, you must first disable the DNS server using the **no dns-server** command, and then enter the **dns-server zone load reporting** or the **no dns-server zone load reporting** command.

Note If you configure the absolute load calculation method for GSLB, Cisco Systems recommends that you configure a load variance of 0, regardless of whether you are using zone-based or rule-based DNS load balancing. For information on absolute load calculation, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

(config) dnsflow

To set up either TCP or UDP traffic to DNS server port 53 as a CSS flow or to forward the traffic, use the **flow-state** commands. The **flow-state** commands replace the following **dnsflow** command and options:

Syntax Description

disable	This command option has been deprecated (obsoleted). If you enter **dnsflow disable** at the CLI or if it already exists in your running-config, the CSS automatically converts it to the following **flow-state** commands: • (config)# **flow-state 53 udp flow-disable nat-enable** • (config)# **flow-state 53 tcp flow-disable**
enable	This **dnsflow** command option has been removed from the CLI. Use the **flow-state** commands instead (see Note below).

Note For details about the **flow-state** commands, see the (config) flow-state command.

Command Modes

Global configuration mode

Related Commands

(config) flow-state

(config) domain hotlist

To enable the domain hot list, use the **domain hotlist** command. The domain hot list is disabled by default. A domain hot list lists the most accessed domains on the CSS during a user-defined period of time. Use the **no** form of this command to disable the domain hot list.

domain hotlist

no domain hotlist

Related Commands

show domain hotlist

(config) domain hotlist interval

To configure the interval, in minutes, to refresh the domain hot list and start a new list, use the **domain hotlist interval** command. Use the **no** form of this command to reset the interval to its default setting of 1 minute.

domain hotlist interval *minutes*

no domain hotlist interval

Syntax Description

minutes	Interval in minutes. Enter an integer from 1 to 60. The default is 1.

Related Commands

show domain hotlist

(config) domain hotlist size

To configure the maximum number of domain entries contained in the hot list, use the **domain hotlist size** command. Use the **no** form of this command to reset the maximum size to its default setting of 10 entries.

domain hotlist size *max_entries*

no domain hotlist size

Syntax Description

max_entries	Maximum number of domain hot-list entries. Enter an integer from 1 to 100. The default is 10.

Related Commands

show domain hotlist

(config) domain hotlist threshold

To configure the threshold (the number of domain hits per interval) that must be exceeded for a domain to be considered hot and added to the list, use the **domain hotlist threshold** command. Use the **no** form of this command to reset the threshold to its default setting of 0.

domain hotlist threshold *number*

no domain hotlist threshold

Syntax Description

number	Threshold number. Enter a number from 0 to 65535. The default is 0 which indicates that the threshold is disabled.

Related Commands

show domain hotlist

(config) dql

To access and configure a domain qualifier list (DQL), use the **dql** command. A DQL is a collection of domain names that you can assign to a content rule, instead of creating a rule for each domain.

Use the **no** form of this command to remove an existing DQL.

dql *dql_name*

no dql *existing_dql_name*

Syntax Description

dql_name	Name of a new DQL you want to create or of an existing list. Enter an unquoted text string with no spaces and a maximum of 31 characters. To see a list of existing DQL names, enter: `dql ?`

Usage Guidelines

When you use the **dql** command to access DQL mode, the prompt changes to (config-dql [*name*]). You can also use this command from DQL mode to access another DQL. For information about commands available in this mode, see the "DQL Configuration Mode Commands" section.

Related Commands

show dql
(config-owner-content) url

(config) dump

To enable or disable core dumps when the CSS experiences a fatal error, use the **dump** command. Core dumps are enabled by default.

Note Core dump information is for customer support use only.

dump [**disable**|**enable**]

Syntax Description

disable	Disables core dumps. When the CSS experiences a fatal error and core dumps are disabled, the CSS reboots automatically. The CSS does not write information to the hard disk or flash disk.
enable	Enables core dumps. This is the default setting. When the CSS experiences a fatal error and core dumps are enabled, the CSS: • Writes information about the fatal error to the Core directory of the volume root (for example, c:\core) on either the hard or flash disk. On the hard or flash disk stores one dump file per slot per card type until the disk is full. Files can be 10 to 20 MB in size. • Reboots automatically

Usage Guidelines

For a flash disk-based system, if the core dump file is older than 15 minutes, it may be overwritten. If you want to save the core dump file for later examination, archive it to another directory or disk before it is overwritten. To archive a log file, see the **archive log** command.

Related Commands

show core

(config) eql

To access EQL configuration mode and configure an extension qualifier list (EQL), use the **eql** command. This list is a collection of file extensions for content requests joined together through content rules. The CSS uses this list to identify which requests to send to a service.

Use the **no** form of this command to delete an existing extension list.

eql *eql_name*

no eql *existing_eql_name*

Syntax Description

eql_name	Name of a new extension list you want to create or of an existing list. Enter an unquoted text string with no spaces and a maximum length of 31 characters. To see a list of existing EQL names, enter: **`eql ?`**

Usage Guidelines

When you use the **eql** command to access eql mode, the prompt changes to (config-eql [*name*]). For information about commands available in this mode, see the "EQL Configuration Mode Commands" section.

Related Commands

show eql
(config-owner-content) url

(config) flow-state

To set the flow states of TCP and UDP ports in the CSS flow-state table, use the **flow-state** command. Use the **no** form of the command to disable the flow state.

flow-state *number* **tcp** [**flow-enable**|**flow-disable**]

flow-state *number* **udp** [**flow-enable**|**flow-disable** {**nat-enable**|**nat-disable**}]

no flow-state *number* **tcp**|**udp**

Syntax Description

number	TCP or UDP port number on which you want to configure the flow state.
tcp	Specifies a TCP port.
udp	Specifies a UDP port.
flow-enable	Enables flows on the specified TCP or UDP port. With this option, the CSS performs full content-rule and source-group matching, including Layer 5 (IP address, destination port, and URL) content-based load balancing and sticky.
flow-disable	Disables flows on the specified TCP or UDP port. When you disable flows on a port, the CSS does not perform content rule and source group matching. The benefit is no flow setup overhead.
nat-enable	(Optional) For flow-disabled UDP ports, enables content-rule and source-group lookups for NAT. With this option, you can use Layer 3 (IP address) and Layer 4 (IP address and destination port) content rules and the sticky table (for example, **sticky-srcip**). However, without the benefit of a flow, the CSS cannot spoof the back-end connection, which is required to make Layer 5 content-based decisions.
nat-disable	(Optional) For flow-disabled UDP ports, the CSS does not perform content-rule and source-group lookups for NAT.

Usage Guidelines

By default, Domain Name Service (DNS) port 53 (TCP and UDP) and SIP port 5060 (UDP) are flow-enabled. You can change the flow states of the preconfigured ports, and you can configure any 16 unique TCP or UDP ports and their flow states.You can also set the port address translation (PAT) state for flow-disabled UDP ports only.

For more information, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config) zero flow-state-counters
show flow-state-table

(config) flow permanent

To define a set of TCP or UDP ports that will have permanent connections and will not be reclaimed by the CSS when the flows are inactive, use the **flow permanent** command. By default, the CSS may reclaim TCP/UDP flows that have not received an ACK or content request after approximately 15 seconds. Use the **no** form of this command to disable a permanent connection by setting its port number to 0.

flow permanent [**port**[**1**|**2**|**3**|**4**|**5**|**6**|**7**|**8**|**9**|**10**]] *port_number*

no flow permanent [**port**[**1**|**2**|**3**|**4**|**5**|**6**|**7**|**8**|**9**|**10**]]

Syntax Description

port_number	Number of the port. Enter an integer from 0 to 65535. The default is 0, which disables a permanent connection on the port.

Usage Guidelines

Entering the **flow permanent** command disables Denial of Service protection and reclaiming of ports when there is asymmetrical routing on any flow with the specified transport layer port as a source or destination of a flow.

Do not configure the **flow permanent** command without enabling the **cmd-sched** command to periodically remove the permanent port and allow for cleanup. For details on using the **cmd-sched** command to configure the scheduled execution of any CLI commands, refer to the *Cisco Content Service Switch Administration Guide*.

(config) flow reserve-clean

To define how often the CSS scans flows from reserved Telnet and FTP control ports to reclaim them, use the **flow reserve-clean** command. Control ports have port numbers less than 23. When the CSS determines that one of these ports has a flow with asymmetrical routing, it reclaims the port. Use the **no** form of this command to reset the flow cleanup on Telnet and FTP control ports to its default setting of 10 seconds.

flow reserve-clean *seconds*

no flow reserve-clean

Syntax Description

seconds	Time interval in seconds to scan flows. Enter an integer from 0 to 100. The default is 10. A setting of 0 disables the flow.

(config) flow tcp-mss

To configure the TCP maximum segment size (MSS), use the **flow tcp-mss** command. Use the **no** form of this command to reset the TCP maximum segment size to the default value of 1460 bytes.

flow tcp-mss *size*

Syntax Description

size	Maximum segment size (in bytes) from 1 to 1460. The default is 1460 bytes. Do not define a very small segment size. Smaller payloads may be less efficient due to increased overhead.

Usage Guidelines

The **flow tcp-mss** command applies only when the client is accessing a Layer 5 content rule. The CSS does not negotiate a TCP maximum segment size for Layer 3 or Layer 4 content rules. The MSS is the largest piece of TCP data that the CSS expects to receive from the other end. This command changes the MSS value in the TCP header options field of a SYN segment.

(config) flow tcp-reset-on-vip-unavailable

To configure a CSS to send a TCP RST (reset) to a client when a VIP is unavailable, use the **flow tcp-reset-on-vip-unavailable** command. Use the **no** form of this command to return the CSS behavior to the default of dropping the TCP packet when a VIP is unavailable.

flow tcp-reset-on-vip-unavailable

no flow tcp-reset-on-vip-unavailable

Usage Guidelines

The CSS sends the TCP reset only in response to a TCP packet that is destined for a VIP that the CSS is hosting and only if that VIP is unavailable.

Related Commands

show ip statistics

(config) ftp-record

To create a File Transfer Protocol (FTP) record file to use when accessing an FTP server from the CSS, use the **ftp-record** command. Use the **no** form of this command to delete an FTP record file from the CSS.

ftp-record *ftp_record ip_or_host username* [**"***password***"**
 |**des-password** *des_pwd*] {**base_directory**}

no ftp-record *ftp_record*

Syntax Description

ftp_record	Name for the FTP record file. Enter an unquoted text string with no spaces and a maximum length of 16 characters.
ip_or_host	IP address or host name of the FTP server you want to access. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or a mnemonic host name (for example, myhost.mydomain.com).
username	Valid login username on the FTP server. Enter a case-sensitive unquoted text string with no spaces and a maximum length 16 characters.
"*password***"**	Password for the valid login username on the FTP server. Enter a case-sensitive quoted text string with no spaces and a maximum length of 16 characters.
des-password *des_pwd*	Specifies the Data Encryption Standard (DES) encrypted password for the valid login username on the FTP server. Enter a case-sensitive unquoted text string with no spaces and a maximum length of 64 characters.
base_directory	(Optional) Base directory when using this record. Enter a case-sensitive unquoted text string with no spaces and a maximum length of 64 characters.

Usage Guidelines

The CSS FTP server supports only the active (normal) FTP mode of operation. It does not support the passive FTP mode of operation.

Related Commands

copy ftp
copy log
copy running-config
copy script
copy ssl
(config-boot) primary
(config-boot) secondary

(config) global-portmap

To control the global source-port translation (port mapping) for TCP flows on a CSS, use the **global-portmap** command. Use the **no** form of this command to reset the starting port number and the port range to their default values.

global-portmap base-port *number1* **range** *number2*

no global-portmap

Syntax Description

base-port *number1*	Starting port number for global port mapping on a CSS. Enter an integer from 2016 to 63456. The default is 2016. **Caution** Changing the value of the *number1* variable may cause port conflicts on existing flows.
range *number2*	The total number of ports in the port-map range that the CSS allocates to each of the 16 megamap banks in each SP. Each megamap bank in an SP can use the full range of configured ports. Because of the unique source address hash that the CSS uses to select a megamap bank in an SP, more than one SP can use the same port number without a tuple collision. **Caution** Changing the value of the *number2* variable may cause port conflicts on existing flows. Enter an integer from 2048 to 63488. The default is 63488. If you enter a value that is not a multiple of 32, the CSS rounds up the value to the next possible multiple of 32. If you enter a portmap range that exceeds the number of available ports, you get an error. To determine the number of available ports, subtract the starting port number you specify from 65504.

Usage Guidelines

The global portmapper in a CSS is called the megaportmapper. The megaportmapper database comprises 16 banks of portmap numbers (megamap banks) in each session processor (SP) with unique ranges. A CSS uses a source port hash algorithm to select a megamap bank.

Use the **global-portmap** command to control the global source-port translation (port mapping) for TCP flows on a CSS. This command is always enabled. Use this command to specify the source-port mapping range on:

- A Cisco 11500 series CSS when you configure a service that uses a nondefault destination port number. A CSS changes a TCP destination port number configured on a service in a content rule when a request hits the content rule and the CSS sends a packet to the selected server. The CSS uses the **global portmap** command parameters to translate the corresponding client source port number to distinguish it from other clients requesting the same service.
- A redundant Cisco 11500 series CSS peers in a session-level redundancy configuration. For information on session-level redundancy, refer to the *Cisco Content Services Switch Redundancy Configuration Guide*.
- Any CSS with back-end server remapping enabled (refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*).

Note When you configure a source group, the **portmap** command values take precedence over the **global-portmap** command. For details on configuring the **portmap** command in a source group, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*. Note that the **portmap disable** command has no effect on TCP flows.

Related Commands

show global-portmap
(config-group) portmap

(config) group

To access group configuration mode and configure a group, use the **group** command. A group is a collection of local servers that initiate flows from within the local web farm. For example, after processing a group of real audio transmitters, they all appear on the same source IP address. The CSS lets you treat a group as a virtual server with its own source IP address.

Use the **no** form of this command to delete an existing group.

group *group_name*

no group *existing_group_name*

Syntax Description

group_name	Name of a new group you want to create or of an existing group. Enter an unquoted text string with no spaces and a maximum length of 31 characters. To see a list of existing group names, enter: `group ?`

Usage Guidelines

When you use the **group** command to access group mode, the prompt changes to (config-group [*name*]). For information about commands available in this mode, see the "Group Configuration Mode Commands" section.

Caution Before you use the **no group** command to delete an existing group, make sure you want to permanently delete the group. You cannot undo this command. If you want a prompt before the CSS performs a command, use the **no expert** command.

(config) gsdb

To start the global sticky database (GSDB) on a dedicated CSS 11150 with 256 MB of RAM when you are configuring GSLB with a GSDB or using DNS Sticky in a Network Proximity configuration, or specify a time-to-live (TTL) interval for the GSDB sticky domain entries, use the **gsdb** command. Use the **no** form of this command to disable the GSDB or reset the TTL interval for GSDB entries to 7200 seconds.

gsdb {**ttl** *seconds*}

no gsdb {**ttl**}

Syntax Description

ttl	(Optional) Specifies the time-to-live interval for the GSDB entries.
seconds	(Optional) Time-to-live interval in seconds. The value you enter determines the length of time that GSDB entries are valid. Enter a number from 300 to 1000000. The default value is 7200. Any new request from a D-proxy for a sticky domain that arrives before the timer expires resets the timer.

Usage Guidelines

Because the GSDB is dependent upon the presence of the PDB, you must configure the PDB prior to starting the GSDB.

You do not need to configure a GSDB to use the basic DNS Sticky feature in a global server load-balancing (GSLB) environment. However, a GSDB provides a more robust DNS Sticky and load-balancing configuration. For details on the types of DNS Sticky configurations, refer to the *Cisco Content Services Switch Global Server Load-Balancing Configuration Guide*.

Related Commands

gsdb zero
show gsdb

(config) gsdb zero

To reset the Sticky Lookups and Sticky Sets statistics that are displayed by the **show gsdb** command, use the **gsdb zero** command. This command applies only to a CSS 11150 with 256 MB of RAM that is configured as a global sticky database (GSDB).

The syntax for this global configuration mode command is:

gsdb zero

Related Commands

gsdb
show gsdb

(config) gsdb-interface

To create a primary or secondary interface to the GSDB on the CSS DNS server to communicate with a GSDB, or zero the GSDB interface statistics, use the **gsdb-interface** command. Use the **no** form of this command to remove a primary or secondary GSDB interface.

gsdb-interface [**primary** *ip_address*|**secondary** *ip_address*|**zero**]

no gsdb-interface [**primary**|**secondary**]

Syntax Description

primary	Specifies the primary interface for the GSDB. The CSS uses the primary GSDB for sticky requests.
secondary	Specifies the secondary interface for the GSDB. The CSS uses the secondary interface when the primary interface is unavailable.

ip_address	IP address of the GSDB. Enter the address in dotted-decimal notation (for example, 192.168.11.1). In a Network Proximity configuration, the IP address of the primary sticky interface is typically the same as the IP address of the PDB.
zero	Resets the GSDB interface statistics that are displayed by the **show gsdb-interface** command.

Usage Guidelines

The **gsdb-interface** command is part of the Enhanced feature set.

A GSDB responds with a zone index to sticky queries from CSS DNS servers. All GSDBs participating in a peer mesh share sticky TTL and sticky zone information over APP.

Related Commands

show gsdb-interface

(config) header-field-group

To access header-field-group configuration mode and configure a request header-field group, use the **header-field-group** command. A request header-field group contains a list of defined header-field entries used by the content rule lookup process. Each header-field group is given a unique name so different content rules can use them. A group can contain several header-field entries. Use the **no** form of this command to remove a header-field group.

header-field-group *group_name*

no header-field-group *group_name*

Syntax Description

group_name	Header-field group that you want to configure. You must define a unique name for each header-field group so different content rules can use the groups. Enter a text string with a maximum of 32 characters. To see an existing list of header-field groups, enter: `header-field-group ?`

Usage Guidelines

To access header-field-group configuration mode, use the **header-field-group** command from all configuration modes, except boot and RMON modes. The prompt changes to (config-header-field-group [*group_name*]). You can also use this command in header-field-group mode to access another group. For information about commands available in this mode, see the "Header-Field Group Configuration Mode Commands" section.

Note When there is more than one header-field entry in a group, each header-field entry must be successfully matched before the CSS uses the associated content rule.

Related Commands

show header-field-group
(config-owner-content) header-field-rule

(config) host

To manage entries in the Host table, use the **host** command. The Host table is the static mapping of mnemonic host names to IP address, analogous to the ARP table. Use the **no** form of this command to remove an existing host from the Host table.

host *host_name ip_address*

no host *host_name*

Syntax Description

host_name	Name of the host. Enter an unquoted text string with no spaces and a maximum length of 16 characters. To see a list of host names, enter: `show running-config global`
ip_address	IP address associated with the host name. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).

Usage Guidelines

To add a host to the Host table, the host name must not already exist. To change a current host’s address, remove it and then add it again.

Related Commands

show running-config

(config) idle timeout

To set the maximum amount of time that any Telnet, console, FTP, or web management session can be idle on the CSS before the CSS logs it out, use the **idle timeout** command. Use the **no** form of this command to set the idle timeout for the session connected to the CSS to the default of 0.

idle timeout {**web-mgmt**} *minutes*

no idle timeout {**web-mgmt**}

Syntax Description

web-mgmt	(Optional) Sets the maximum amount of idle time for active web management sessions.
minutes	Maximum time in minutes. Enter a number from 0 to 65535. The default is 0.

Usage Guidelines

The **idle timeout** command without the **web-mgmt** option sets the global timeout for Telnet, console, SSH, and FTP sessions.

You can override the **idle timeout** command with the **terminal** command in SuperUser mode for Telnet, console, SSH, and FTP sessions.

(config) interface

To enter interface configuration mode and configure an interface, use the **interface** command.

interface *interface_name*

Syntax Description

interface_name	CSS interface that you want to configure. For a CSS 11501, enter the interface name in *interface-port* format (for example, e2). For a CSS 11503 or 11506, the interface format is *slot/port* (for example, 3/1). To see a list of valid interfaces for this CSS, enter: **`interface ?`**

Usage Guidelines

When you use the **interface** command to access this mode, the prompt changes to (config-if [*interface_name*]). For information about commands available in this mode, see the "Interface Configuration Mode Commands" section.

(config) ip

To enter global IP configuration commands, use the **ip** command. The options for this global configuration mode command are:

- **ip advanced-route-remap** - Remaps flows using the best available route
- **ip ecmp** - Sets the equal-cost multipath selection algorithm
- **ip firewall** - Configures an index that identifies a physical firewall
- **ip management no-icmp-redirect** - Configures the Ethernet management port to discard ICMP redirect packets
- **ip management route** - Configures a static route for the Ethernet management port
- **ip no-implicit-service** - Does not allow the CSS to start an implicit service for the next hop of static routes
- **ip opportunistic** - Configures opportunistic Layer-3 forwarding

- **ip record-route** - Enables processing of frames with a record-route option
- **ip redundancy** - Enables CSS-to-CSS redundancy
- **ip route** - Configures a static route
- **ip source-route** - Enables processing of source-routed frames
- **ip subnet-broadcast** - Enables forwarding of subnet broadcast addressed frames

For more information on these options and associated variables, see the following commands.

Related Commands

show ip config
show ip summary

ip advanced-route-remap

To configure the CSS to remap flows using the best-available route, use the **ip advanced-route-remap** command. Use the **no** form of this command to disable the remapping of flows using the best-available route.

ip advanced-route-remap

no ip advanced-route-remap

Command Modes

Global configuration mode

ip ecmp

To set the equal-cost multipath selection algorithm and the preferred reverse egress path, use the **ip ecmp** command. Use the **no** form of this command to reset the ingress path of a flow for its preferred reverse egress path.

ip ecmp [**address**|**no-prefer-ingress**|**roundrobin**]

no ip ecmp no-prefer-ingress

Syntax Description

address	Chooses among alternate paths based on IP addresses.
no-prefer-ingress	Does not prefer the ingress path of a flow for its reverse egress path. By default, the ingress path for a flow is its preferred egress path.
roundrobin	Alternates between equal paths in roundrobin fashion.

Command Modes

Global configuration mode

Usage Guidelines

The equal-cost multipath selection algorithm for non-TCP/UDP packets (for example, ICMP) is applied on a packet-by-packet basis. Multipath selection for TCP and UDP is performed on a per-flow basis and all packets for a particular flow take the same path.

ip firewall

To configure an index that identifies a physical firewall, use the **ip firewall** command. Use the **no** form of the **ip firewall** *index* command to delete a firewall index. Use the **no** form of the **ip firewall timeout** command to reset the firewall timeout to the default value of three seconds.

ip firewall [*index local_firewall_address remote_firewall_address remote_switch_address*|**timeout** *seconds*]

no ip firewall [*index*|**timeout**]

Syntax Description

index	Index number to identify the firewall. Enter a number from 1 to 254.
local_firewall_address	IP address of the firewall on a subnet connected to the CSS. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
remote_firewall_address	IP address of the firewall on the remote subnet that connects to the remote switch. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
remote_switch_address	IP address of the remote CSS. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
timeout *seconds*	Number of seconds that the CSS waits to receive a keepalive message from the remote CSS before declaring the firewall to be unreachable. The timeout range is 3 to 16 seconds. The default is 3 seconds.

Command Modes

Global configuration mode

Usage Guidelines

You can configure indices for multiple parallel firewalls allowing for traffic load balancing. To avoid dropping packets, all connections in either direction between a pair of IP addresses cross the same firewall. If a failure occurs on one path, all traffic uses the remaining path.

A CSS must exist on each side of the firewall to control which firewall is selected for each flow. You must configure a firewall index identifier on the remote CSS with the same index number to the same physical firewall.

To configure the firewall route, use the **ip route** command. Firewalls cannot perform Network Address Translation (NAT). If your configuration requires NATing, you must configure a content rule or source group on the CSS to provide this function.

Caution When you delete a firewall index, all routes associated with that index are also deleted.

The two CSS switches at the endpoints of the firewall configuration must use the same firewall keepalive timeout value. Otherwise, routes on one CSS may not fail over simultaneously with those on the other CSS. This could permit asymmetric routing to occur across the firewalls.

Related Commands

ip route

ip management no-icmp-redirect

To configure the CSS to discard ICMP redirect packets on the Ethernet management port, use the **ip management no-icmp-redirect** command. By default, the Ethernet management port accepts all incoming ICMP redirect packets. Use the **no** form of this command to reset the default behavior of accepting ICMP redirect packets on the Ethernet management port.

ip management no-icmp-redirect

no ip management no-icmp-redirect

Command Modes

Global configuration mode

Usage Guidelines

If you do not configure static routes for the Ethernet management port, the CSS disregards any ICMP redirects. However, when you configure static routes for the Ethernet management port, the CSS incorporates the ICMP redirects as entries in the routing table.

To enhance security on the CSS when you configure static routes on the Ethernet management port, we strongly recommend that you configure the CSS Ethernet management port to discard ICMP redirects.

The Ethernet management port never transmits an ICMP redirect.

If you remove a static route when the Ethernet management port is configured to accept ICMP redirect packets, the CSS removes the router entry created by the ICMP redirect associated with the static route from the routing table.

Related Commands

show ip config

ip management route

The ability to configure static routes on the Ethernet management port provides access to the CSS from hosts on subnets that are different from the Ethernet management port subnet. To manage the CSS from a subnet that is different from the Ethernet management port, use the **ip management route** command. By default, this option is disabled. Use the **no** form of this command to disable a static route for the Ethernet Management port.

ip management route *ip_address1 subnet mask ip_address2*

no ip management route *ip_address1 subnet mask ip_address2*

Syntax Description

ip_address1	The destination network address. Enter the IP address in dotted-decimal notation (for example, 192.168.11.0).
subnet_mask	The IP subnet mask. Enter the mask as either: • A prefix length in CIDR bitcount notation (for example, /24). Do not enter a space to separate the IP address from the prefix length. • An IP address in dotted-decimal notation (for example, 255.255.255.0).
ip_address2	The next hop address for the route. Enter the IP address in dotted-decimal notation (for example, 172.16.6.1).

Command Modes

Global configuration mode

Usage Guidelines

You can configure a maximum of eight static routes for the Ethernet management port.

The CSS does not use an internal (implicit) service for the Ethernet management port to periodically poll the next hop address in a static route. The periodic polling of the next hop address with an ICMP echo (or ping) keepalive is performed only when you configure a static route for an Ethernet interface port.

The **rip redistribute static** and **ospf redistribute static** commands do not advertise static routes configured on the Ethernet management port. These two commands only advertise static routes configured on the Ethernet interface ports.

ip no-implicit-service

To stop the CSS from starting an implicit service for the next hop of static routes, use the **ip no-implicit-service** command. By default, this option is disabled. Use the **no** form of this command to reset the default setting.

ip no-implicit-service

no ip no-implicit-service

Command Modes

Global configuration mode

Usage Guidelines

By default, the CSS establishes an implicit (or internal) service for the gateway address when a static route is defined. The **ip no-implicit-service** command specifies that no implicit service is established to the next hop of the static route.

Note When you implement the **ip no-implicit-service** command, it does not affect any previously configured static routes. If you wish to stop the implicit service for a previously configured static route, you must delete and reconfigure that static route.

The purpose of the implicit service to the next hop of a static route is to monitor the availability of the next hop to forward data traffic. When the **ip no-implicit-service** command is in effect, traffic will be forwarded to the next hop even when it is unavailable. Because of the possibility of data loss if the next hop becomes unavailable, use of the **ip no-implicit-service** command is strongly discouraged.

ip opportunistic

To configure the opportunistic Layer 3 forwarding of packets, use the **ip opportunistic** command. Use the **no** form of this command to allow opportunistic Layer 3 forwarding for local destinations.

ip opportunistic [**all**|**disable**]

no ip opportunistic

Syntax Description

all	Allows opportunistic Layer 3 forwarding for all destinations; when the IP destination address matches any routing entry on the CSS. This mode is not recommended for a topology that includes multiple routers and the CSS does not know all the routes that the routers know.
disable	Disables opportunistic Layer 3 forwarding. Layer 3 forwarding only occurs for packets whose destination MAC address belongs to the CSS.

Command Modes

Global configuration mode

Usage Guidelines

Opportunistic Layer 3 forwarding allows the CSS to forward packets according to the IP destination address. The MAC destination address does not need to belong to the CSS. By default, the CSS allows this forwarding for local destinations when the IP destination address belongs to a node that resides on one of the subnets directly attached to the CSS and an ARP resolution is known for this node.

ip record-route

To enable the CSS to process frames with a record-route option, use the **ip record-route** command. Use the **no** form of this command to disable the processing of frames with a record-route option (the default behavior).

ip record-route

no ip record-route

Refer to the *Cisco Content Services Switch Routing and Bridging Configuration Guide* for more information about this command.

Command Modes

Global configuration mode

ip redundancy

To enable CSS-to-CSS redundancy on two CSSs interfaced with a crossover cable, use the **ip redundancy** command. You can also use the **master** option to manually designate which CSS is the master. By default, redundancy is disabled on a CSS. Use the **no** form of the **ip redundancy** command to disable CSS-to-CSS redundancy. Use the **no** form of the **ip redundancy master** to unassign the CSS as the master CSS.

ip redundancy {**master**}

no ip redundancy {**master**}

Syntax Description

master	(Optional) Enables CSS-to-CSS redundancy on the CSS that you want to designate as the master CSS. Do not enter this command on both the master and backup CSSs. You can enter this command option on the CSS: • Whether it was initially booted as the master or the backup. If you enter this command on the backup CSS, it becomes the master and the other CSS automatically becomes the backup CSS. • When CSS-to-CSS redundancy is currently enabled.

Command Modes

Global configuration mode

Usage Guidelines

If you have no requirement to designate a specific CSS as the master, use the **ip redundancy** command with no keyword on each CSS. When you do not manually designate a master CSS, the CSSs negotiate to determine the master and backup. In this negotiation, the master CSS is the CSS that boots first. If both CSSs boot at the same time, the CSS with the higher IP address becomes the master. When the master CSS goes down, the backup CSS automatically becomes the master. When the former master CSS comes up again, it becomes the backup CSS.

To manually designate a CSS as the master CSS, enter the **master** option on it. You can enter this option on a negotiated master or backup. If you enter this option on a master, it remains the master. If you enter this option on the backup CSS, it becomes the master and the other CSS automatically becomes the backup.

Caution Do not enter the **ip redundancy master** command on both the master and backup CSSs. This can cause network problems.

Because the designated master CSS saves its configuration setting in the running-config, if it goes down and then comes up again, it regains its master status. For example, when the master CSS goes down, the backup CSS becomes master. When the former master CSS comes up again, it becomes the master again.

You cannot use the **ip redundancy master** command if you previously used the **(config-if) redundancy-phy** or **(config-service) type redundancy-up** command. Before you can use the **ip redundancy master** command, you must enter the **(config-if) no redundancy-phy** or **(config-service) no type** command.

The **no ip redundancy master** command does not disable CSS-to-CSS redundancy.

The CSS does not support simultaneous CSS-to-CSS redundancy and VIP redundancy configurations.

The CSS does not support a trace route of a redundant IP interface.

Related Commands

redundancy force-master
show redundancy
(config-if) redundancy-phy
(config-circuit) redundancy
(config-circuit-ip) redundancy-protocol

ip route

To configure a static route including routes for firewalls, use the **ip route** command. Use the **no** form of this command to remove a blackhole, static, or firewall route.

ip route *ip_address subnet_mask* [**blackhole**|*ip_address2* {*distance*|**originated-packets**}|**firewall** *index* {*distance*}]

no ip route *ip_address subnet_mask* [**blackhole**|*ip_address2* |**firewall** *index*]

Syntax Description

ip_address	Destination network address. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
subnet_mask	IP subnet mask. Enter the mask as either: • A prefix length in CIDR bitcount notation (for example, /24). Do not enter a space to separate the IP address from the prefix length. • A subnet mask in dotted-decimal notation (for example, 255.255.255.0).
blackhole	Instructs the CSS to drop any packets addressed to the route.
ip_address2	Next hop address for a static route. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
distance	(Optional) Administrative distance. Enter an integer from 1 to 254. A smaller number is preferable. The default value is 1.
firewall	Configures a firewall route.

index	Existing index number for the firewall route. For information on configuring a firewall index, see the **ip firewall** command.
originated-packets	(Optional) Instructs the CSS to use this route for flow and session packets going to and from the CSS (for example, a Telnet session to the CSS). Flows or session packets that go through the CSS (for example, between an attached server and a remote client) do not use this route.

Command Modes

Global configuration mode

Usage Guidelines

The CLI prevents you from configuring IP static routes that *are* firewall routes and IP static routes that *are not* firewall routes to identical destinations using identical administrative costs.

Note Ping responses and SNMP responses do not use the originated-response route. Ping *requests* sent from the CSS use the originated-response route. Ping *responses* sent from the CSS do not use the originated-response route.

ip source-route

To enable the processing of source-routed frames, use the **ip source-route** command. Use the **no** form of this command to disable the processing of source-routed frames (the default behavior).

ip source-route

no ip source-route

Refer to the *Cisco Content Services Switch Routing and Bridging Configuration Guide* for more information about this command.

Command Modes

Global configuration mode

ip subnet-broadcast

To enable the forwarding of subnet broadcast addressed frames, use the **ip subnet-broadcast** command. Use the **no** form of this command to disable the forwarding of subnet broadcast addressed frames (the default behavior).

ip subnet-broadcast

no ip subnet-broadcast

Caution When the forwarding of the subnet broadcast is enabled, it can make the subnet susceptible to "smurf" attacks; an attacker sends an ICMP echo request frame using a subnet broadcast address as a destination and a forged address as the source. If the attack is successful, all the destination subnet hosts reply to the echo and flood the path back to the source. When the subnet broadcast forwarding is disabled, the original echo never reaches the hosts.

Command Modes

Global configuration mode

(config) ip-fragment-enabled

To allow a CSS to flow-process UDP IP fragments, use the **udp-ip-fragment-enabled** command. By default, this feature is disabled. Use the **no** form of the command to reset the default behavior of the CSS to forwarding IP fragments.

Usage Guidelines

The **ip-fragment-enabled** command has been deprecated (obsoleted). If you enter the **ip-fragment-enabled** command at the CLI or if your configuration already contains the **ip-fragment-enabled** command, the CSS automatically converts the command to the **udp-ip-fragment-enabled** command.

Related Commands

(config) udp-ip-fragment-enabled
(config) tcp-ip-fragment-enabled

(config) ip-fragment max-assembled-size

To specify the maximum assembled size, use the **ip-fragment max-assembled-size** command. The maximum assembled size is the total length of an IP packet if all the IP fragments were assembled into the original packet. Assembled IP packets should be no larger than 64 KB.

As the CSS receives the IP fragments, it checks the fragments against the maximum assembled size value. If a fragment IP offset plus the IP payload (data) length is greater than the maximum assembled size, the CSS increments an error counter and discards the packet. Use the **no** form of this command to reset the maximum IP fragment assembled size to the default of 5120 bytes.

ip-fragment max-assembled-size *number*

no ip-fragment max-assembled-size

Syntax Description

number	Specifies the maximum size of an assembled packet in bytes. Enter an integer from 2048 to 65535. The default is 5120 bytes.

Related Commands

zero ip-fragment-stats
show ip-fragment-stats
(config) ip-fragment-enabled
(config) ip-fragment min-fragment-size

(config) ip-fragment min-fragment-size

To specify the smallest IP fragment payload based on your applications, use the **ip-fragment min-fragment-size** command. This command also provides protection against fragment attacks, which can consist of a chain of valid-looking, but very small, fragments. Use the **no** form of this command to reset the minimum IP fragment payload size to the default of 1024 bytes.

ip-fragment min-fragment-size *number*

no ip-fragment min-fragment-size

Syntax Description

number	Specifies the size of the smallest IP fragment payload that the CSS supports in bytes. Enter an integer from 64 to 1024. The default is 1024 bytes.

Related Commands

zero ip-fragment-stats
show ip-fragment-stats
(config) ip-fragment-enabled
(config) ip-fragment max-assembled-size

(config) keepalive

To access keepalive configuration mode and configure the properties for a global keepalive that you can apply to any service, use the **keepalive** command. Use the **no** form of this command to delete an existing keepalive.

keepalive *name*

no keepalive *existing_keepalive_name*

Syntax Description

name	Name of a new keepalive you want to create or of an existing keepalive. Enter an unquoted text string with no spaces and a maximum length of 31 characters. To see a list of existing keepalive names, enter: `keepalive ?`

Usage Guidelines

When you access keepalive mode, the prompt changes to (config-keepalive [*name*]). For information about commands available in this mode, see the "Keepalive Configuration Mode Commands" section.

Related Commands

show keepalive
(config-service) keepalive type named

(config) load

To configure global load parameters for the eligibility and ineligibility of CSS services, use the **load** command. Load is a measurement of a service's ability to handle flows. There are two types of loads: relative load and absolute load.

The CSS calculates relative load by using the variances in normalized response times for each service. You can adjust relative load calculations by changing the load step size, which is the difference in milliseconds between load numbers. The CSS can determine the load step size dynamically or you can configure it.

Absolute load takes into account the actual observed load on a service and allows you to configure the response times that correlate with values within the CSS load number scale. Unlike the relative load number scale, where all the load numbers between 2 and 254 represent equal steps or increases in response times, absolute load creates 16 different divisions or ranges within the CSS load number scale. Ranges are groups of consecutive load numbers that share a common step size (delta) between numbers. For more information on relative load and absolute load, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

The load on a service has a range from 2 to 255, with an eligible load state from 2 to 254. An eligible service is an active service that can receive flows. A service with a lower load receives more flows than a service with a higher load. When a service initially comes up, its load value is 2. A load of 255 indicates that the service is down, as detected through the keepalive.

The **load** command has the following options:

- **load absolute-sensitivity** - Sets the maximum response time upper boundary and the step size of the absolute load number scale
- **load ageout-timer** - Sets the time interval after which load information for a service is considered stale and the service load is reset to 2
- **load calculation** - Sets the method (relative or absolute) that the CSS uses to assign load numbers to all configured services
- **load reporting** - Enables the CSS to generate teardown reports and derive load numbers
- **load step** - Sets the load step of the relative load number scale

- **load teardown-timer** - Sets the maximum time for the CSS before sending a teardown report
- **load threshold** - Sets the load threshold for a service, determining its eligibility to receive flows

For more information on these options and associated variables, see the following commands.

load absolute-sensitivity

To set the maximum response time upper boundary and the step size of the absolute load number scale, use the **load absolute-sensitivity** command. Use the **no** form of this command to set the absolute load sensitivity to the default of 21.

load absolute-sensitivity *number*

no load absolute-sensitivity

Syntax Description

number	Sensitivity of the absolute load number scale. Enter an integer from 1 to 25. The default is 21.

Command Modes

Global configuration mode

Usage Guidelines

Increasing the **load absolute-sensitivity** value increases the maximum response time upper boundary and the absolute load number scale step size (granularity), which reduces the load value for a given service response time. Conversely, decreasing the **load absolute-sensitivity value** decreases the maximum response time upper boundary and the absolute load number scale step size (granularity), which increases the load value for a given service response time.

For *number* values from 1 to 20, the absolute load number ranges are linear, which means that the step sizes are equal among all the ranges. For values from 21 to 25, the ranges are nonlinear, which means different ranges have different step sizes that increase as the range number increases.

Related Commands

show load
(config) load calculation
(config) dns-peer load-variance
(config) dns-server zone

load ageout-timer

To set the time interval in seconds in which stale load information for a service is aged out, use the **load ageout-timer** command. Use the **no** form of this command to set the ageout time to the default of 60.

load ageout-timer *seconds*

no load ageout-timer

Syntax Description

seconds	Number of seconds to age out load information for a service. Enter an integer from 0 to 1000000000. The default is 60. The value of 0 disables the timer.

Command Modes

Global configuration mode

Usage Guidelines

When the ageout timer interval expires, the CSS erases the load information and resets the service load to 2. Load information is stale when the teardown report number recorded on a service has not incremented during the ageout time interval because no flows (long or short) are being torn down on the service.

At the beginning of the time interval, the ageout timer saves the number of the current teardown report. When the CSS generates a new teardown report, the report number in the CSS increments, and any services in the report saves this number. At the end of the ageout time interval, the CSS compares the initial teardown number saved at the beginning of the time interval with the current teardown number saved by each service. If the number of a service is less than or equal to the timer number, the load information is stale. The CSS erases it and resets the service load to 2.

Related Commands

show load
(config) load reporting

load calculation

To set the method that the CSS uses to assign load numbers to all configured services, use the **load calculation** command. Use the **no** form of this command to set the load calculation method to the default of relative.

load calculation relative|absolute

no load calculation

Syntax Description

relative	The CSS assigns load numbers to services based on a comparison with the fastest service.
absolute	The CSS assigns load numbers to services based on pure response times.

Command Modes

Global configuration mode

Usage Guidelines

The default behavior of a CSS is to use the relative load calculation method when assigning loads to services. With relative load, the CSS takes the service with the fastest response time and then compares all other services configured on the CSS with that service. Relative load may suffice in situations where load is not critical to your application and you are generally satisfied with service load assignments.

Consider using absolute load instead of relative load when you have a single CSS serving multiple applications, or when you are using GSLB to balance between multiple CSSs. Absolute load takes into consideration the actual load and response times of all the services in your configuration and fits them into the CSS absolute load number scale. For more information, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Note You must configure the **load reporting** command to enable the CSS to derive loads on services.

Related Commands

show load
(config) load absolute-sensitivity
(config) dns-peer load-variance
(config) dns-server zone

load reporting

To enable the CSS to generate teardown reports and derive load numbers, use the **load reporting** command. A teardown report is a summary of response times for services when flows are being torn down. The CSS uses the teardown report to derive the load number for a service. Use the **no** form of this command to disable load reporting.

load reporting

no load reporting

Command Modes

Global configuration mode

Related Commands

show load

load step

To set the difference in milliseconds between load numbers, use the **load step** command. Use the **no** form of this command to set the load step to the default of 10.

load step *msec* [**dynamic**|**static**]

no load step

Syntax Description

msec	Load step in milliseconds. Enter an integer from 1 to 1000000000. The default is 10.
dynamic	Sets the initial load step. The CSS modifies it after the CSS collects sufficient response time information from the services.
static	Sets a constant load step. This option disables the dynamic calculations made by the CSS.

Command Modes

Global configuration mode

Usage Guidelines

Eligible load numbers have a range from 2 to 254. By default, the CSS dynamically calculates the load step as it accumulates minimum and maximum response times for the services.

When you configure the load step to reduce the flows to a slower service, consider the differences in response times between services. For example:

- Increasing the load step causes the load for services to be closer to each other, thus increasing the number of flows to a slower service.
- Decreasing the load step causes the load for services to be further from each other, thus decreasing the flows to a slower service.

Related Commands

show load
(config) load reporting

load teardown-timer

To set the maximum time between teardown reports, use the **load teardown-timer** command. Use the **no** form of this command to reset the teardown time interval to its default of 20 seconds.

load teardown-timer *seconds*

no load teardown-timer

Syntax Description

seconds	Number of seconds between teardown reports. Enter an integer from 0 to 1000000000. The default is 20. The value of 0 disables the timer.

Command Modes

Global configuration mode

Usage Guidelines

A teardown report is a summary of response times for services when flows are being torn down. The CSS uses the teardown report to derive the load number for a service. When the CSS has sufficient teardown activity for a service, it generates a teardown report and the teardown timer is reset. If a teardown report is not triggered at the end of the teardown timer interval due to insufficient activity, the CSS generate a teardown report based on the current activity. If there is no activity, no report is generated and the timer resets.

Note The teardown timer is overridden when a service is reset. After 10 teardown reports are recorded, the timer is reset to its configured value.

Related Commands

show load
(config) load reporting

load threshold

To define the global load number that the CSS uses to determine if a service is eligible to receive flows, use the **load threshold** command. Use the **no** form of this command to set the load threshold to the default of 254.

load threshold *number*

no load threshold

Syntax Description

number	Threshold number. Enter a number from 2 to 254. The default is 254.

Command Modes

Global configuration mode

Usage Guidelines

If you do not configure a load threshold for the content rule with the **(config-owner-content) load-threshold** command, the rule inherits this global load threshold.

If the service load exceeds the threshold, the service becomes ineligible to receive flows until its load information is stale. Information is stale when the teardown report number recorded on a service has not incremented during the ageout time interval.

Related Commands

show load
(config) load ageout-timer

(config) logging

Use the **logging** command to:

- Select a CSS subsystem and determine which activities to log
- Determine where to send the log activity
- Set the size of the disk buffer, if applicable

By default, the sys.log file on the CSS disk contains the Notice-level activities for all CSS subsystems. The options for this global configuration mode command are:

- **logging buffer** - Sets the size of the disk buffer
- **logging commands enable** - Enables the logging of CLI commands
- **logging disk** - Sends the log activity to a new or existing file on the disk
- **logging host** - Sends the log activity to a host
- **logging line** - Sends the log activity to an active session
- **logging sendmail** - Sends logging messages to an e-mail address
- **logging subsystem** - Selects a CSS subsystem and determine which activities to log
- **logging to-disk** - Disables logging to the sys.log file on the CSS disk

For more information on these options and associated variables, see the following commands.

Related Commands

clear log
show log

logging buffer

To set the size of the disk buffer, use the **logging buffer** command. Use the **no** form of this command to set the disk buffer size to the default of 0.

logging buffer *size*

no logging buffer

Syntax Description

size	Size of the disk buffer in bytes. Enter an integer from 0 to 64000. The default is 0, where the CSS sends the logging information directly to the disk.

Command Modes

Global configuration mode

Usage Guidelines

The **logging buffer** command is only applicable when you configure logging to the CSS disk through the **logging disk** command.

When the log activity information for the subsystem fills the buffer, the CSS empties it into the log file on the disk. The larger you configure the buffer size, the less frequently the CSS empties the buffer.

Related Commands

(config) logging disk

logging commands enable

To enable the CSS to log CLI commands, use the **logging commands enable** command. Use the **no** form of this command to disable the logging of CLI commands.

logging commands enable

no logging commands

Command Modes

Global configuration mode

Usage Guidelines

For the CSS to send CLI commands to the sys. log file, you must set the logging level of the netman subsystem to info-6. For example:

```
(config)# logging subsystem netman info-6
```

logging disk

To log the activity of a subsystem to a new or existing file on the disk, use the **logging disk** command. Use the **no** form of this command to turn off logging to the specified file on the disk and reenable logging to the sys.log file.

logging disk *filename*

no logging disk

Syntax Description

filename	New or existing filename in the log directory where you want to send the log information. The default file is sys.log. Enter an unquoted text string with a maximum length of 32 characters. To see a list of log filenames, enter: `logging disk ?`

Command Modes

Global configuration mode

Usage Guidelines

You can have only one active log file on the disk. If you want to send the log information to a different log file, reenter the **logging disk** command.

Caution Logging to a CSS disk causes the performance of the CSS to degrade.

Related Commands

(config) logging buffer
(config) logging to-disk
(config) logging subsystem

logging host

To send the log activity of a subsystem to the syslog daemon on the host system, use the **logging host** command. Use the **no** form of this command to turn off logging to the syslog daemon on the host.

logging host *ip_or_host* **facility** *number* **log-level** *number*

no logging host *ip_or_host*

Syntax Description

ip_or_host	IP address of the syslog daemon on the host. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1) or the mnemonic host name (for example, myhost.mydomain.com).

facility *number*	Syslog daemon facility level. Enter a number from 0 to 7. For more information on the syslog daemon and facility levels, refer to the syslog daemon documentation that accompanied the host system.
log-level *number*	Logging level of the messages sent to the syslog daemon. Enter one of the following valid log levels for the CSS: fatal-0, alert-1, critical-2, error-3, warning-4 (default), notice-5, info-6, debug-7. The logging levels are listed in order of severity, with a fatal-0 level being the most severe error and an info-6 level being the least severe error. This level must be equal to or less than the log level you configure for the **logging subsystem** command.

Command Modes

Global configuration mode

Usage Guidelines

When you use the **logging host** command, the CSS continues to send logging activity to the sys.log file on the disk. To disable logging to the sys.log file, use the **logging to-disk disable** command.

The log level that you enter must be equal to or less than the logging level set for a CSS subsystem with the **logging subsystem** command. If the level is set to a value greater than the logging level, the CSS displays only the subsystem log messages for the specified subsystem level. The log level is a subset of the subsystem level you set. For example, if you specify **logging subsystem** *netman* **level** *warning-4* and **logging host** <*ip address*> **log-level** *7*. You should expect to see messages only at level 4 or lower sent to the syslog daemon. Although the facility number is set to 7, log messages 5, 6, or 7 would not be displayed in the sys.log file on the CSS or sent to the syslog daemon.

Related Commands

(config) logging subsystem

logging line

To send the log activity of a subsystem to an active CSS session, use the **logging line** command. Use the **no** form of this command to turn off logging to a session.

logging line *session*

no logging line *session*

Syntax Description

session	Valid active session on the CSS. Enter a case-sensitive unquoted text string with a maximum length of 32 characters. To see a list of sessions, enter: `logging line ?`

Command Modes

Global configuration mode

Usage Guidelines

When you use the **logging line** command, the CSS continues to send logging activity to the sys.log file on the disk. To disable logging to the sys.log file, use the **logging to-disk disable** command.

Related Commands

(config) logging subsystem

logging sendmail

To send the log activity of a subsystem to an e-mail address, use the **logging sendmail** command. Use the **no** form of this command to turn off logging to an e-mail address.

logging sendmail *email_address host_address level* {*domain*}

no logging sendmail *email_address*

Syntax Description

email_address	E-mail address for the recipient. Enter a case-sensitive unquoted text string with a maximum length of 30 characters.
host_address	IP address for the SMTP host. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
level	The type of information to log. Enter one of these levels: • **fatal-0 -** Fatal error log messages • **alert-1 -** Alert error log messages • **critical-2** - Critical error log messages • **error-3** - General error log messages • **warning-4 -** Warning error log messages • **notice-5 -** Notice error log messages • **info-6** - Information messages
domain	The domain name for the SMTP host. Enter an unquoted text string with a maximum length of 64 characters (for example, cisco.com). Do not insert an "@" sign before the domain name. The CSS prepends it to the domain name automatically.

Command Modes

Global configuration mode

logging subsystem

To select a CSS subsystem and determine which type of activity to log, use the **logging subsystem** command. Use the **no** form of this command to reset a subsystem logging level to the default setting of warning.

logging subsystem *name* **level** *level*

no logging subsystem *name*

Syntax Description

name Name of a CSS subsystem. Enter one of the following subsystem names:

- **acl** - Access control lists
- **all** - All subsystems
- **app** - Application Peering Protocol (APP)
- **boomerang** - DNS Content Routing Agent
- **buffer** - Buffer Manager
- **chassis** - Chassis Manager
- **circuit** - Circuit Manager
- **csdpeer** - Content Server Database (CSD) Peer
- **dql** - Domain qualifier list (DQL)
- **eql** - Extension qualifier list (EQL)
- **fac** - Flow Admission Control (FAC)
- **flowmgr** - Flow Manager
- **hfg** - Header field group (HFG)
- **ipv4** - Internet Protocol version 4
- **keepalive** - Keepalive
- **netman** - Network Management
- **nql** - Network qualifier list (NQL)
- **ospf** - OSPF

name (cont.)	• **pcm** - Proximity CAPP Messaging (PCM) • **portmapper** - Port Mapper • **proximity** - Proximity • **publish** - Publish • **radius** - Remote Authentication Dial-In User Server (RADIUS) • **replicate** - Replication • **redundancy** - CSS redundancy • **rip** - RIP • **security** - Security Manager • **sntp** - Simple Network Time Protocol (SNTP) • **syssoft** - System software • **urql** - Uniform Resource qualifier list • **vlanmgr** - VLAN Manager • **vpm** - Virtual Pipe Manager • **vrrp** - Virtual Router Redundancy Protocol • **wcc** - Web Conversation Control To see a list of subsystems, enter: **`logging subsystem ?`**

level The log level for the message. Enter one of these levels:

- **fatal-0** - Fatal errors only.
- **alert-1** - Alert errors, including errors at the fatal-0 level.
- **critical-2** - Critical errors, including errors at the alert-1 level.
- **error-3** - Error errors, including errors at the critical-2 level.
- **warning-4** - Warning errors (default), including errors at the error-3 level.
- **notice-5** - Notice messages, including errors at the warning-4 level.
- **info-6** - Informational messages, including errors at the notice-5 level.
- **debug-7** - All errors and messages. Setting the logging level to debug-7 may decrease the performance of the CSS. When you enter this keyword, the CSS prompts you with the following message:

```
Logging at the debug level may degrade the CSS
performance. Continue, [y/n]:
```

Enter **y** to verify that you want to set the log level to debug-7. Enter **n** to cancel the executing of the debug-7 log level.

Command Modes

Global configuration mode

Related Commands

clear log
(config) logging disk
(config) logging host
(config) logging line

logging to-disk

To disable or enable logging to the sys.log file on the CSS disk, use the **logging to-disk** command. By default, the CSS logs to the sys.log file.

logging to-disk [**disable**|**enable**]

Syntax Description

disable	Disables logging to the sys.log file
enable	Reenables logging to the sys.log file

Command Modes

Global configuration mode

Usage Guidelines

Use the **logging to-disk disable** command to prevent excessive writes to the disk or to increase the performance of the CSS. Logging to a file on a CSS disk degrades the performance of the CSS.

The **logging to-disk disable** command affects the sys.log file only. It does not affect a disk log file that you specified through the **logging disk** command. To disable all logging to the CSS disk, use the **no logging disk** command, and enter the **logging to-disk** command to disable logging to the sys.log file.

Related Commands

show log-state
(config) logging buffer
(config) no logging disk
(config) logging subsystem

(config) no

To negate a command or set it to its default, use the **no** command. Not all commands have a **no** form. For information on general **no** commands that you can use in this mode, see the general **no** command.

All of the following options are available in global configuration mode.

Syntax Description

no acl *index*	Deletes an existing ACL
no app	Disables APP on the CSS
no app framesz	Restores the default APP frame size to 10240
no app port	Restores the default APP port number to 5001
no app session *ip_address*	Terminates an APP session
no app-udp	Disables APP-UDP messaging on the CSS
no app-udp options *ip_address*	Deletes the APP-UDP options from the IP address
no app-udp port	Restores the default APP-UDP port number to 5002
no app-udp options *ip_address*	Deletes the APP-UDP options from the IP address
no app-udp secure	Restores the default behavior of accepting all APP datagrams
no arp *ip_or_host*	Removes a static mapping address
no arp timeout	Restores the default timeout of 14400 seconds
no arp wait	Restores the default wait time of 5 seconds
no arrowpoint-cookie rfc2822-compliant	Disables the RFC2822 compliant format for the arrowpoint-cookie expiration time syntax
no bridge aging-time	Restores the default aging time of 300
no bridge forward-time	Restores the default delay time of 4
no bridge hello-time	Restores the default hello time interval of 1
no bridge max-age	Restores the default maximum age of 6
no bridge priority	Restores the default priority of 32768

no cmd-sched	Disables the execution of scheduled CLI commands
no cmd-sched record	Deletes a configuration record for the execution of CLI commands
no console authentication	Sets console authentication to none
no date european-date	Resets the format for the **clock date** command to its default of month, day, and year
no dhcp-relay-agent max-hops	Resets the maximum allowable number in the hops field of the BOOTP header to 4
no dns primary	Removes the primary DNS server
no dns secondary *ip_or_host*	Removes a secondary DNS server
no dns suffix	Removes the default suffix
no dns-boomerang client cpu-threshold	Resets the CSS CPU threshold to the default value of 99
no dns-boomerang client domain *dns_name* {**alias** *alias_name*}	Removes a client domain or the alias for the domain
no dns-boomerang client enable	Disables the Content Routing Agent (CRA) functionality on the CSS
no dns-peer interval	Resets the time between load reports to the CSS DNS peers to its default of 5 seconds
no dns-peer receive-slots	Resets the maximum number of DNS names received from a peer to its default value of 128
no dns-peer send-slots	Resets the maximum number of DNS names sent to a peer to its default value of 128
no dns-peer variance	Resets the **load-variance** to its default value of 50
no dns-record a *dns_name*	Deletes a domain address record
no dns-record accel *dns_name*	Deletes a DNS acceleration record
no dns-record ns *dns_name*	Deletes a domain name server record
no dns-server	Disables the DNS server functionality on the CSS
no dns-server accelerate domains	Disables domain acceleration

no dns-server bufferCount	Restores the default response buffer count to 10
no dns-server domain-cache	Disables domain caching
no dns-server forwarder primary|secondary	Deletes a CSS DNS forwarder
no dns-server respTasks	Restores the default responder task count to 2
no dns-server zone	Disables the CSS Proximity Domain Name Server
no domain hotlist	Disables the domain hot list
no domain hotlist interval	Resets the domain hot-list interval to 1 minute
no domain hotlist size	Resets the maximum number of entries in the domain hotlist to 100
no domain hotlist threshold	Resets the domain hot-list threshold to 0, which disables the threshold
no dql *dql_name*	Deletes the specified DQL
no eql *eql_name*	Deletes the specified EQL
no flow-state *number* **udp|tcp**	Resets the flow state and, for flow-disabled UDP ports, the PAT state of a port to its default settings
no flow permanent port[**1|2|3|4|5|6|7|8|9|10|11|12|13|14|15|16|17|18|19|20**]	Resets a port to its default number of 0
no flow port-reset	Disables Fast and Gigabit Ethernet port resets on the CSS
no flow reserve-clean	Resets the reclaiming of port numbers to 10 seconds
no flow tcp-mss	Resets the TCP maximum segment size to 1460 bytes
no ftp-record *ftp_record*	Deletes an FTP record file from the CSS
no global-portmap	Resets the starting port and range to their default values
no group *existing_group_name*	Deletes an existing group
no gsdb	Disables the GSDB

no gsdb ttl	Resets the time to live for GSDB entries to its default of 7200 seconds
no gsdb-interface [**primary**|**secondary**]	Removes the GSDB primary or secondary interface
no header-field-group *existing_group_name*	Deletes an existing header-field group
no host *host_name*	Removes an existing host from the Host table
no idle timeout	Sets the idle timeout for any session connected to the CSS to the default of 0 (disabled)
no ip advanced-route-remap	Disables the CSS from remapping flows using the best-available route
no ip ecmp no-prefer-ingress	Resets the ECMP ingress path for a flow to be its preferred reverse egress path
no ip firewall *index*	Deletes a configured firewall
no ip management no-icmp-redirect	Resets the CSS to accept ICMP redirect packets on the Ethernet management port
no ip no-implicit-service	Resets the CSS to start an implicit service for the next hop of static routes
no ip opportunistic	Allows opportunistic Layer 3 forwarding for local destinations
no ip record-route	Disables processing of frames with a record-route option
no ip redundancy	Disables CSS-to-CSS redundancy
no ip redundancy master	Unassigns the CSS as the master CSS
no ip route *ip_address subnet_mask ip_address2*	Removes a static route
no ip route *ip_address subnet_mask* **blackhole**	Disables the dropping of packets to a blackhole route
no ip route *ip_address subnet_mask* **firewall** *index*	Removes a firewall route
no ip source-route	Disables processing of source-routed frames
no ip subnet-broadcast	Disables forwarding of subnet broadcast addressed frames
no ip uncond-bridging	Reenables the routing table lookup to override a bridging decision

no ip-fragment max-assembled-size	Resets the maximum IP fragment assembled size to the default of 5120 bytes
no ip-fragment min-fragment-size	Resets the minimum IP fragment payload size to the default of 1024 bytes
no keepalive *name*	Deletes an existing keepalive
no load ageout-timer	Resets the number of ageout time interval for load information to its default value of 60 seconds
no load reporting	Disables load reporting
no load step	Resets the load step to its default value of 10 ms
no load teardown-timer	Resets the teardown time interval to its default value of 20 seconds
no load threshold	Resets the global load threshold to its default value of 254
no logging buffer	Sets the disk buffer size to the default of 0
no logging commands	Disables the logging of CLI commands
no logging disk	Turns off logging to a specified file on disk
no logging host *ip_or_host*	Turns off logging to the syslog daemon on the host
no logging line *session*	Turns off logging to an active CSS session
no logging sendmail *email_address*	Turns off logging to an e-mail address
no logging subsystem *name*	Resets the logging level of a subsystem to the default setting of warning
no noflow-portmap	Resets the starting port and range to their default values
no nql *name*	Deletes an existing NQL
no ospf advertise *ip_address subnet_mask*	Stops advertising of the route as OSPF ASE through the OSPF interfaces
no ospf area *ip_address*	Removes the OSPF area
no ospf as-boundary	Unassigns the CSS as a AS boundary router
no ospf default	Stops advertising the routes originated through OSPF
no ospf enable	Disables OSPF
no ospf equal-cost	Resets the number of equal-cost routes OSPF can use to its default of 15

no ospf range *area_id address mask*	Removes the range to summarize routes at an area border
no ospf redistribute [**firewall**|**local**|**rip**|**static**]	Stops advertising a route of a specific protocol type through OSPF
no ospf router-id	Deletes the OSPF router ID on the CSS
no owner *existing_owner_name*	Deletes an existing owner
no prelogin-banner	Removes a previously configured pre-login banner
no proximity cache-size	Restores the proximity lookup cache size to its default of 16000 entries
no proximity db	Disables the CSS Proximity Database in a dedicated CSS 11150
no proximity probe rtt interval	Resets the delay in seconds between ICMP samples to its default of 1 second
no proximity probe rtt metric-weighting	Resets the percentage of the previous metric value to derive the new metric to its default of 0
no proximity probe rtt samples	Resets the number of ICMP echo requests that the CSS uses for averaging during an initial probe to its default of 2
no proximity probe rtt tcp-ports	Resets the default probe ports for SYN proximity metric discovery
no proximity ttl assigned	Resets the TTL value to its default of 60 minutes
no proximity ttl probe	Resets the TTL value to its default of 0, which disables the caching of responses at the Proximity Database
no radius-server dead-time	Resets the dead-time period to its default of 5 seconds
no radius-server primary	Deletes the primary RADIUS server
no radius-server source-interface	Removes a specified RADIUS server source interface
no radius-server retransmit	Resets the retransmission of authentication request to its default of 3
no radius-server secondary	Deletes the secondary RADIUS server

no radius-server timeout	Resets the time interval that the CSS waits for a reply to a RADIUS request to 10 seconds
no restrict console	Enables access to the CSS from a console
no restrict ftp	Enables FTP access to the CSS
no restrict secure-xml	Enables secure SSL XML access to the CSS
no restrict snmp	Enables SNMP access to the CSS
no restrict ssh	Enables SSHD access to the CSS
no restrict telnet	Enables Telnet access to the CSS
no restrict xml	Enables unsecure XML access to the CSS
no restrict web-mgmt	Enables web management access to the CSS
no rip advertise *ip_address/ip_mask*	Stops advertising a route through all RIP interfaces
no rip equal-cost	Resets the number of equal-cost routes RIP can use to its default of 1
no rip redistribute [**local**|**ospf**|**static**|**firewall**]	Stops advertising routes from other protocols
no rmon-alarm *index*	Deletes an RMON alarm
no rmon-event *index*	Deletes an RMON event
no rmon-history *index*	Deletes an RMON history
no service *service_name*	Deletes an existing service
no setspan src_port *number* **dest_port** *number*	Disables the switched port analyzer (SPAN) feature
no snmp auth-traps	Disables reception of authentication traps
no snmp community *community_name*	Removes a community name and defaults it to Cisco Systems, Content Network Systems
no snmp contact	Removes the contact name
no snmp location	Removes the location and defaults it to Customer Premises
no snmp name	Removes the SNMP name for this system and defaults it to Support
no snmp reload-enable	Disallows an SNMP-based reboot of the CSS
no snmp trap-host *ip_or_host*	Removes a specified trap host

no snmp trap-source	Resets the SNMP source traps to the default of the management port IP address
no snmp trap-type generic	Disables generic traps
no snmp trap-type enterprise	Disables enterprise traps
no snmp trap-type enterprise *dos_attack_type*	Disables the generation of an SNMP enterprise trap for a Denial of Service attack type, as configured with the **(config) snmp trap-type enterprise** command
no snmp trap-type enterprise chmgr-module-transition	Disables the generation of an SNMP enterprise trap when a module is inserted into or removed from the chassis
no snmp trap-type enterprise chmgr-ps-transition	Disables the generation of an SNMP enterprise trap when a power supply changes state
no snmp trap-type enterprise isc-lifetick-failure	Disables the generation of an SNMP enterprise traps on ISC lifetick message failures
no snmp trap-type enterprise isc-state-transition	Disables the generation of an SNMP enterprise trap when an ISC link fails over
no snmp trap-type enterprise login-failure	Disables the generation of an SNMP enterprise trap when a login fails
no snmp trap-type enterprise reload	Disables the generation of an SNMP enterprise trap when the CSS reboots initiated directly through SNMP
no snmp trap-type enterprise redundancy-transition	Disables the generation of an SNMP enterprise trap when a redundant CSS transitions state
no snmp trap-type enterprise reporter transition	Disables the generation of an SNMP enterprise trap when a reporter transitions state
no snmp trap-type enterprise service-transition	Disables the generation of an SNMP enterprise trap when a service transitions state

no sntp poll-interval	Resets the poll interval to its default to 64 seconds
no sntp server	Removes the SNTP server
no sshd keepalive	Disables the SSHD keepalive
no sshd port	Resets the SSHD port number to 22
no sshd server-keybits	Resets the number of bits for the server key to 768
no ssl crl-record *name*	Removes the specified CRL record from the CSS
no tacacs-server *ip_address port*	Removes the TACACS+ server
no tacacs-server account config|non-config	Disables TACACS+ accounting for running and non-running configuration commands
no tacacs-server authorize config|non-config	Disables TACACS+ authorization for running and non-running configuration commands
no tacacs-server key	Removes the global encryption key
no tacacs-server timeout	Resets the TACACS+ server timeout period to its default of 5 second
no urql *name*	Deletes an existing URQL
no username *name*	Deletes an existing username
no virtual authentication	Disables virtual authentication
no vrrp-backup-timer	Resets the timer to the default value of 3 seconds

Command Modes

Global configuration mode

(config) noflow-portmap

To control the port translation (port-mapping) range of DNS UDP source-port numbers greater than 1023 on a CSS, use the **noflow-portmap** command. This command is always enabled. Use the **no** form of this command to reset the starting port number and portmap range to their default values.

noflow-portmap base-port *number1* **range** *number2*

no noflow-portmap

Syntax Description

base-port *number1*	Starting port number for no-flow (DNS flows are disabled) port mapping on a CSS. Enter an integer from 2016 to 63456. The default is 2016. ⚠ **Caution** Changing the value of the *number1* variable may cause port conflicts on existing flows.
range *number2*	**range** *number2* - The total number of ports in the port-map range that the CSS allocates to each SP. Each SP can use the full range of configured ports. ⚠ **Caution** Changing the value of the *number2* variable may cause port conflicts on existing flows. Enter an integer from 2048 to 63488. The default is 63488. If you enter a value that is not a multiple of 32, the CSS rounds up the value to the next possible multiple of 32.

Usage Guidelines

Before a CSS can use the **noflow-portmap** command, you must enter the **dnsflow disable** command to disable DNS flows on the CSS.

The **portmap** command values configured in a source group take precedence over the **noflow-portmap** command values, unless you configure the **portmap disable** command. For details on configuring the **portmap** commands in a source group, refer to *Cisco Content Services Content Load-Balancing Configuration Guide*.

Related Commands

show noflow-portmap
(config) dnsflow
(config-group) portmap

(config) nql

To access network qualifier list (NQL) configuration mode and configure an NQL, use the **nql** command. An NQL is a collection of subnet and host IP addresses which you can assign to an ACL clause, instead of creating a clause for each address. Use the **no** form of this command to remove an existing NQL.

nql *nql_name*

no nql *existing_nql_name*

Syntax Description

nql_name	The name of a new NQL you want to create or of an existing list. Enter an unquoted text string with no spaces and a maximum length of 31 characters. To see a list of existing NQL names, enter: `nql ?`

Command Modes

Global configuration mode

Usage Guidelines

You can access NQL mode from any configuration mode except boot, group, RMON alarm, RMON event, and RMON history configuration modes. The prompt changes to (config-nql [*name*]). You can also use the **nql** command from NQL mode to access another NQL. For information about commands available in this mode, see the "NQL Configuration Mode Commands" section.

You can configure a maximum of 512 networks to an NQL and a maximum of 512 NQLs on the CSS.

(config) ospf

To configure global Open Shortest Path First (OSPF) parameters on the CSS, use the **ospf** command. The options for this global configuration mode command are:

- **ospf advertise** - Advertises a route as OSPF Autonomous System external (ASE) through all OSPF interfaces
- **ospf area** - Configures an OSPF area
- **ospf as-boundary** - Configures the CSS as an Autonomous System (AS) boundary router
- **ospf default** - Advertises default ASE default routes through OSPF
- **ospf enable** - Enables OSPF
- **ospf equal-cost** - Sets the number of equal-cost routes that OSPF can use
- **ospf range** - Configures summarize routes at an area border
- **ospf redistribute** - Advertises other routes through OSPF
- **ospf router-id** - Configures the OSPF router ID

For more detailed information about these options and their variables, see the following sections.

Related Commands

show ospf
(config-circuit-ip) ospf

ospf advertise

To advertise a route as OSPF ASE through all OSPF interfaces, use the **ospf advertise** command. Use the **no** form of this command to stop advertising the route as OSPF ASE through all OSPF interfaces.

ospf advertise *ip_address subnet_mask* {**metric** *number1*} {**tag** *number2*} {**type1**}

no ospf advertise *ip_address subnet_mask*

Syntax Description

ip_address	IP address for the route prefix. Enter an IP address in dotted-decimal notation (for example, 192.168.128.0).
subnet_mask	Subnet mask. Enter the mask as either: • A prefix length in CIDR bitcount notation (for example, /24). Do not enter a space to separate the IP address from the prefix length. • A dotted-decimal notation (for example, 255.255.254.0).
number1	(Optional) Metric to use when advertising a route. Enter a number from 1 to 16777215. The default is 1.
tag *number2*	(Optional) 32-bit tag value to advertise each external route. This is not used by the OSPF protocol itself. You can use it to communicate information between AS boundary routers.
type1	(Optional) Advertises the routes as ASE type1. By default, the type is ASE type2. The difference between type1 and type2 is how the cost is calculated. For a type2 ASE, only the external cost (metric) is considered when comparing multiple paths to the same destination. For type1 ASE, the combination of the external cost and the cost to reach the ASBR is used.

Command Modes

Global configuration mode

Usage Guidelines

Before you enter the **ospf advertise** command, you must configure the CSS as an Autonomous System (AS) boundary router. For more information, see the **ospf as-boundary** command.

The AS boundary router can perform external route summarization to consolidate multiple routes into a single advertisement. For a CSS, this is useful when you want to advertise VIP addresses for content as OSPF AS external (ASE) through all OSPF interfaces.

Note When you configure OSPF to advertise a VIP address as ASE, it continues to advertise the route even when the underlying service is not active or does not exist anymore. However, if you configure the VIP as a redundant VIP within a virtual router, OSPF will stop advertising this VIP when the virtual router state is Down or Backup.

For more information on configuring a redundant VIP within a virtual router, refer to the *Cisco Content Services Switch Redundancy Configuration Guide*. To stop the advertisement of the route, enter the **no ospf advertise** command.

ospf area

To configure an OSPF area, use the **ospf area** command. To remove an OSPF area, disable OSPF and then use the **no** form of this command.

ospf area *area_id* {**stub** {**default-metric** *metric*|**send-summaries**}}

no ospf area *area_id*

Syntax Description

area_id	The OSPF area ID. Enter the ID in dotted-decimal notation (for example, 0.0.0.1). Although an area ID has the same form as an IP address, the area ID address space is its own distinct address space. The area ID of 0.0.0.0 is reserved for the backbone.

stub	(Optional) Allows you to configure the area as a stub area. AS-external link state advertisements are not flooded into stub areas. This reduces the link-state database size and the memory requirements for internal routers in the stub area.
default-metric	(Optional) Sets a metric for the default route advertised into the stub area.
metric	(Optional) Metric value. By default, this value equals the least metric among the interfaces to other areas. Enter an integer from 1 to 16777215.
send-summaries	(Optional) Propagates summary link state advertisements (LSAs) into the stub area.

Command Modes

Global configuration mode

ospf as-boundary

To configure the CSS as an Autonomous System (AS) boundary router, use the **ospf as-boundary** command. An AS boundary router exchanges routing information with routers belonging to other Autonomous Systems. It advertises AS external routing information throughout the Autonomous System. Use the **no** form of this command to unassign the CSS as an AS boundary router.

ospf as-boundary

no ospf as-boundary

Command Modes

Global configuration mode

Usage Guidelines

You can enter the **ospf as-boundary** command only if OSPF is disabled.

ospf default

To advertise default ASE routes through OSPF, use the **ospf default** command. Routers use default routes when no more specific routes exist to AS external destinations. Use the **no** form of this command to shut off the advertising of default ASE routes originated through OSPF.

ospf default {**metric** *number1*} {**tag** *number2*} {**type1**}

no ospf default

Syntax Description

metric *number1*	(Optional) Metric to advertise. Enter a number from 1 to 16777215. The default is 1.
tag *number2*	(Optional) 32-bit tag value to advertise each external route. This is not used by the OSPF protocol itself. You can use it to communicate information between AS boundary routers.
type1	(Optional) Advertises the routes as ASE type1. By default, the type is ASE type2. The difference between type1 and type2 is how the cost is calculated. For a type2 ASE, only the external cost (metric) is considered when comparing multiple paths to the same destination. For type1 ASE, the combination of the external cost and the cost to reach the ASBR is used.

Command Modes

Global configuration mode

Usage Guidelines

Use the **ospf default** command to force an AS boundary router to generate a default route. Normally, AS boundary routers do not generate default routes into the OSPF routing domain.

ospf enable

To enable OSPF, use the **ospf enable** command. Use the **no** form of this command to disable OSPF.

ospf enable

no ospf enable

Command Modes

Global configuration mode

Usage Guidelines

You must configure a router ID before enabling OSPF. For more information, see the **ospf router-id** command.

ospf equal-cost

To configure the number of equal-cost routes that OSPF can use, use the **ospf equal-cost** command. Use the **no** form of this command to reset the number of routes to its default value of 15.

ospf equal-cost *number*

no ospf equal-cost

Syntax Description

number	Number of equal-cost routes. Enter a number from 1 to 15. The default is 15.

Command Modes

Global configuration mode

ospf range

To specify an IP address range to summarize routes at the CSS area border router, use the **ospf range** command. Use the **no** form of this command to remove the range.

ospf range *area_id ip_address mask* {**block**}
no ospf range *area_id ip_address mask*

Syntax Description

area_id	OSPF area ID. Enter the ID in dotted-decimal notation (for example, 0.0.0.1).
ip_address mask	Range of addresses you want to summarize in one range. Enter the IP address and mask in dotted-decimal notation (for example, 192.168.128.0 255.255.224.0). You can also enter the mask in prefix-length format (for example, /24).
block	(Optional) Hides the range from the rest of the autonomous system.

Command Modes

Global configuration mode

Usage Guidelines

You can enter the **ospf range** command only if OSPF is disabled.

Define an address range by specifying an IP address and mask pair that represent networks in the area being summarized. You can also determine whether you want to advertise this range.

The CSS advertises a single summary route or network ranges that cover all the individual networks within its area that fall into the specified range. This summarization applies to inter-area paths, which are paths to destinations in other OSPF areas. This summarization helps control routing table sizes and prevents the constant changing of routes whenever an interface within an area comes online or goes offline. These route changes do not cause route changes in backbone ABRs and other area routers.

ospf redistribute

To advertise routes from other protocols through OSPF, use the **ospf redistribute** command. Redistribution of these routes makes them OSPF external routes. Use the **no** form of this command to shut off the advertising of routes via OSPF.

ospf redistribute *protocol* {**metric** *number1*} {**tag** *number2*} {**type1**}

no ospf redistribute *protocol*

Syntax Description

protocol	The type of route to advertise. Enter one of the following: • **firewall** - Firewall route • **local** - Local route • **rip** - RIP route • **static** - Static route
metric *number1*	(Optional) Metric to advertise. Enter a number from 1 to 16777215. The default is 1.
tag *number2*	(Optional) 32-bit tag value to advertise each external route. This is not used by the OSPF protocol itself. You can use it to communicate information between AS boundary routers.
type1	(Optional) Advertises the routes as ASE type1. By default, the type is ASE type2. The difference between type1 and type2 is how the cost is calculated. For a type2 ASE, only the external cost (metric) is considered when comparing multiple paths to the same destination. For type1 ASE, the combination of the external cost and the cost to reach the ASBR is used.

Command Modes

Global configuration mode

ospf router-id

To configure the OSPF router ID for the CSS, use the **ospf router-id** command. Use the **no** form of this command to delete the router ID on the CSS.

ospf router-id *id_number*

no ospf router-id

Syntax Description

id_number	Router ID 32-bit number that identifies the CSS within the AS. Enter the ID in dotted-decimal notation (for example, 121.23.21.1).

Command Modes

Global configuration mode

Usage Guidelines

Before you can enable OSPF, you must configure the router ID. To change the router ID, you must disable OSPF.

(config) owner

To access owner configuration mode and configure an owner, use the **owner** command. An owner is an entity that owns web content and uses the CSS to manage access to the content through content rules. A maximum of 255 owners can use a single CSS and each owner has a configurable profile. Use the **no** form of this command to delete an existing owner.

owner *owner_name*

no owner *existing_owner_name*

Syntax Description

owner_name	Name of a new owner you want to create or the name of an existing owner. Enter an unquoted text string with no spaces and a maximum length of 31 characters. To see a list of existing owner names, enter: **owner ?**

Usage Guidelines

When you access owner mode, the prompt changes to (config-owner [*owner_name*]). For information about commands available in this mode, see the "Owner Configuration Mode Commands" section.

Caution Before you use the **no owner** command to delete an existing owner, make sure you want to permanently delete the owner and its associated content rules. You cannot undo this command. If you want a prompt before the CSS performs a command, use the **no expert** command.

(config) persistence reset

To choose between an HTTP redirection or a back-end service remapping operation when resetting a connection to a new back-end service, use the **persistence reset** command. This command affects all flow setups that require redirecting or remapping.

persistence reset [**redirect**|**remap**]

Syntax Description

redirect	Causes an HTTP redirection when resetting a connection to a new back-end service. An HTTP redirection resets both sides of the connection.
remap	Uses a back-end remapping operation when resetting a connection to a new back-end service.

Usage Guidelines

The CSS does not use a remapping method when selecting services of type **redirect**.

You cannot use the **persistence reset** command with the **(config-owner-content) redundancy-l4-stateless** command.

If your topology consists of a CSS 11800 using ECMP to the servers and server port NAT configured on the services, to ensure the correct processing of packets either:

- Enable Service Remapping with the **persistence reset remap** command.
- Create source groups for the services in the content rule with the **add destination service** command.

Related Commands

show remap
(config) bypass persistence
(config-owner-content) persistent

(config) prelogin-banner

To configure a banner that appears when you connect to a CSS before you log in, use the **prelogin-banner** command.

prelogin-banner “*filename*”

no prelogin-banner

Syntax Description

filename	Name of the ASCII text file that contains the pre-login banner text. Enter a quoted text string with a maximum of 32 characters.

Usage Guidelines

Create a banner using any text editor (for example, Notepad or Wordpad). Save the file as a text file, and then FTP the file to the CSS script directory. Configure the prelogin-banner command. The next time you connect to the CSS, the pre-login banner appears. For more information, refer to the *Cisco Content Services Switch Administration Guide*.

(config) proximity

To configure proximity on the CSS, use the **proximity** command and its options. The command options are:

- **proximity cache-remove** - Removes entries from the proximity lookup cache
- **proximity cache-size** - Sets the entry size for the proximity lookup cache
- **proximity db** - Enables the Proximity Database (PDB) in a dedicated CSS 11150
- **proximity probe rtt interval** - Configures the delay in seconds between ICMP samples
- **proximity probe rtt method** - Configures the primary method to be used for proximity metric discovery
- **proximity probe rtt metric-weighting** - Configures the percentage of the previously stored metric value in the database that is used to determine the new metric value
- **proximity probe rtt samples** - Configures the number of ICMP requests to send
- **proximity probe rtt tcp-ports** - Configures the probe defaults for SYN proximity metric discovery
- **proximity ttl** - Sets the Time-to-Live value for each Proximity Database response

For more information, see the following commands.

proximity cache-remove

To remove entries from the proximity lookup cache, use the **proximity cache-remove** command. The prefix length parameter allows you to remove multiple entries in a single operation.

proximity cache-remove [*ip_address ip_prefix*|**all**]

Syntax Description

ip_address	IP address to remove from the cache.
ip_prefix	IP prefix length to be associated with *ip_address* for removal. Enter the prefix as either: • A prefix length in CIDR bitcount notation (for example, /24) • A subnet mask in dotted-decimal notation (for example, 255.255.255.0)
all	Removes all entries from the proximity cache.

Command Modes

Global configuration mode

Usage Guidelines

The **proximity cache-remove** command is functional on a CSS with the Enhanced feature set.

Related Commands

show proximity cache

proximity cache-size

To set the size of the proximity lookup cache, use the **proximity cache-size** command. Use the **no** form of this command to restore the default cache size of 16000 entries.

proximity cache-size *cache_size*

no proximity cache-size

Syntax Description

cache_size	Size of the cache. Enter a size between 0 and 48,000. The default value is 16000 entries. Entering a value of 0 disables the cache.

Command Modes

Global configuration mode

Usage Guidelines

The **proximity cache-size** command is functional on a CSS with the Enhanced feature set. By default, the cache supports approximately 16,000 entries using 1 MB of CSS memory. You can increase or decrease the entries, depending upon your CSS configuration.

Note Dynamically modifying the cache size results in flushing the existing entries.

Related Commands

show proximity cache
(config) proximity cache-remove

proximity db

To enable the Proximity Database (PDB) on the CSS, use the **proximity db** command. This service allows the CSS to respond to proximity lookup requests and enables proximity probing. Use the **no** form of this command to disable the CSS Proximity Database.

proximity db *zoneIndex* {**tier1|tier2** {**“***description***”**}}

no proximity db

Syntax Description

zoneIndex	Numeric identifier of the proximity zone of the CSS. This number should match the *zoneIndex* configured on the PDNS. Enter an integer from 0 to 15. There is no default.
tier1|tier2	(Optional) Maximum number of zones the CSS expects to participate in its proximity zone mesh. Enter **tier1** for a maximum of 6 zones, 0 through 5. Enter **tier2** for a maximum of 16 zones, 0 through 15. The **tier1** option is the default.
“*description***”**	(Optional) Text description of this CSS zone. Enter a quoted string with a maximum of 20 characters.

Command Modes

Global configuration mode

Usage Guidelines

The **proximity db** command is functional only on a Proximity Database CSS in a dedicated CSS 11150.

proximity probe rtt interval

To configure the delay in seconds between samples for the configured probe method, use the **proximity probe rtt interval** command. Use the **no** form of this command to reset the delay between samples to its default value of 1 second.

proximity probe rtt interval *seconds*

no proximity probe rtt interval

Syntax Description

seconds	Length of time in seconds to delay between samples. Enter a number from 1 to 10. The default is 1.

Command Modes

Global configuration mode

Usage Guidelines

The **proximity probe rtt interval** command is functional only on a Proximity Database CSS in a dedicated CSS 11150.

proximity probe rtt method

To configure the primary and secondary methods to be used for proximity metric discovery, use the **proximity probe rtt method** command. The discovery method uses ICMP Echo requests or a TCP SYN, SYN-ACK, RST sequence to the configured TCP ports as the Round-Trip Time (RTT) discovery method.

proximity probe rtt method [**icmp tcp**|**icmp**|**tcp icmp**|**tcp**]

Syntax Description

icmp tcp	Configures the ICMP as the primary discovery method and TCP as the secondary method (default)
icmp	Configures the ICMP as the primary discovery method only
tcp icmp	Configures the TCP as the primary discovery method and ICMP as the secondary method
tcp	Configures the TCP as the primary discovery method only

Command Modes

Global configuration mode

Usage Guidelines

The **proximity probe rtt method** command is functional only on a Proximity Database CSS in a dedicated CSS 11150.

proximity probe rtt metric-weighting

To configure the percentage of the previously stored metric value in the database that is used to determine the new metric value, use the **proximity probe rtt metric-weighting** command. Use the **no** form of this command to reset the percentage to its default value of 0.

proximity probe rtt metric-weighting *number*

no proximity probe rtt metric-weighting

Syntax Description

number	Percentage of the previous metric value used. Enter a number from 0 to 99. The default is 0.

Command Modes

Global configuration mode

Usage Guidelines

This command is functional only on a Proximity Database CSS in a dedicated CSS 11150.

The **proximity probe rtt metric-weighting** command allows the PDB to smooth network metric variation caused by network congestion and flash crowds.

proximity probe rtt samples

To configure the number of ICMP requests to send for each configured probe method, use the **proximity probe rtt samples** command. Use the **no** form of this command to reset the number of requests to its default value of 2.

proximity probe rtt samples *number*

no proximity probe rtt samples

Syntax Description

number	Number of requests that the CSS uses for averaging during an initial probe. Enter a number from 1 to 30. The default is 2.

Command Modes

Global configuration mode

Usage Guidelines

This command is functional only on a Proximity Database CSS in a dedicated CSS 11150.

proximity probe rtt tcp-ports

To configure the probe ports for SYN proximity metric discovery, use the **proximity probe rtt tcp-ports** command. Use the **no** form of this command to reset the probe ports to their default values.

proximity probe rtt tcp-ports *port_number1* {*port_number2* {*port_number3* {*port_number4*}}}

no proximity probe rtt tcp-ports

Syntax Description

port_number	Maximum of four port numbers to be tried, in order of preference. Enter a number from 0 to 65535. The default for the ports are as follows: • *port_number1* is 23, Telnet port • *port_number2* is 21, FTP port • *port_number3* is 80, HTTP port • *port_number4* is 0, this port is not tried

Command Modes

Global configuration mode

Usage Guidelines

This command is functional only on a Proximity Database CSS in a dedicated CSS 11150.

proximity ttl

To set the time-to-live (TTL) value, in minutes, for each Proximity Database response, use the **proximity ttl** command. This value informs the proximity DNS how long to cache the response. Use the **no** form of this command to reset the TTL value to its default value.

proximity ttl [**assigned** *assigned_minutes*|**probe** *probe_minutes*]

no proximity ttl [**assigned**|**probe**]

Syntax Description

assigned	Sets the TTL value for client addresses that are assigned to the Proximity Database.
assigned_minutes	TTL value in minutes for client addresses that are assigned to the Proximity Database. Enter a number from 0 to 255. The default value is 60.
probe	Sets the TTL value for client addresses that are being probed.
probe_minutes	TTL value in minutes for client addresses that are being probed. Enter a number from 0 to 255. The default value is 0, which disables the caching of responses at the Proximity Database.

Command Modes

Global configuration mode

Usage Guidelines

This command is functional only on a Proximity Database CSS in a dedicated CSS 11150.

(config) radius-server

To configure the CSS as a RADIUS server client, use the **radius-server** command and its options. The command options are:

- **radius-server dead-time** - Sets the time interval to send probe access-request packets to verify that the RADIUS server is available and can receive authentication requests
- **radius-server primary** - Configures the primary RADIUS server
- **radius-server retransmit** - Sets the number of authentication request retransmissions to a timed-out RADIUS server before the server is considered dead
- **radius-server secondary** - Configures the CSS with the secondary RADIUS server information
- **radius-server source interface** - Specifies the IP interface where RADIUS packets are transmitted to and from the RADIUS server.
- **radius-server source interface** - Configures the time interval that the CSS waits before retransmitting an authentication request

For more information, see the following commands.

radius-server dead-time

To set the time interval to send probe access-request packets to verify that the RADIUS server is available and can receive authentication requests, use the **radius-server dead-time** command. Use the **no** form of this command to reset the dead-time period to its default of 5 seconds.

radius-server dead-time *seconds*

no radius-server dead-time

Syntax Description

seconds	The time period in seconds. Enter a number from 0 to 255. The default is 5. If you enter 0, the dead time is disabled and the CSS does not send probe access-request packets to the nonresponsive server.

Usage Guidelines

The dead-time interval starts when the server does not respond to the number of authentication request retransmissions configured through the **radius-server retransmit** command. When the server responds to a probe access-request packet, the CSS transmits the authentication request to the server.

This command applies to primary and secondary servers.

Command Modes

Global configuration mode

Related Commands

show radius config
(config) radius-server retransmit

radius-server primary

To configure the remote primary RADIUS server that authenticates user information from the CSS client, use the **radius-server primary** command. Use the **no** form of this command to delete the primary RADIUS server.

radius-server primary *ip_or_host* **secret** *string* {**auth-port** *number*}

no radius-server primary

Syntax Description

ip_or_host	IP address or the host name for the primary RADIUS server.
secret *string*	Defines the secret string for authentication transactions between the RADIUS server and the CSS. Enter a case-sensitive string with a maximum of 16 characters.
auth-port *number*	(Optional) Defines the UDP port on the primary RADIUS server that receives authentication packets from RADIUS clients. Enter a number from 0 to 65535. The default port is 1645.

Usage Guidelines

When you configure a primary server and enable RADIUS console or virtual authentication on the CSS, the CSS enables the RADIUS protocol, allowing the CSS to become a RADIUS client.

Command Modes

Global configuration mode

Related Commands

show radius config
show radius stat
(config) console authentication
(config) radius-server dead-time
(config) radius-server source interface
(config) radius-server source interface
(config) virtual authentication

radius-server retransmit

To configure the number of times that the CSS retransmits an authentication request to an active RADIUS server after the timeout interval occurred, use the **radius-server retransmit** command. Use the **no** form of this command to reset the retransmission of authentication request to its default of 3.

radius-server retransmit *number*

no radius-server retransmit

Syntax Description

number	Number of times that the CSS retransmits an authentication request. Enter a number from 1 to 30. The default number is 3.

Usage Guidelines

If the RADIUS server does not respond to the CSS retransmitted requests, the CSS considers the server as dead, stops transmitting to the server, and starts the dead timer as defined through the **radius-server dead-time** command.

If a secondary server is configured, the CSS transmits the requests to the secondary server. If the secondary server does not respond to the request, the CSS considers it dead and starts the dead timer.

If there is no active server, the CSS stops transmitting request until one of the servers becomes alive.

Command Modes

Global configuration mode

Related Commands

show radius config
show radius stat
(config) radius-server dead-time

radius-server secondary

To configure the remote secondary RADIUS server, use the **radius-server secondary** command. When the primary server becomes unavailable, the CSS directs authentication requests to the secondary server. Use the **no** form of this command to delete the secondary RADIUS server.

radius-server secondary *host_or_ip* **secret** *text* {**auth-port** *number*}

no radius-server secondary

Syntax Description

ip_or_host	IP address or the host name for the secondary RADIUS server.
secret *string*	Defines the secret string for authentication transactions between the RADIUS server and the CSS. Enter a case-sensitive string with a maximum of 16 characters.
auth-port *number*	(Optional) Defines the UDP port on the secondary RADIUS server that receives authentication packets from clients. Enter a number from 0 to 65535. The default is 1645.

Command Modes

Global configuration mode

Related Commands

show radius config
show radius stat
(config) radius-server dead-time
(config) radius-server source interface
(config) radius-server source interface

radius-server source interface

To specify the IP interface of the CSS RADIUS client, use the **radius-server source-interface** command. Some RADIUS servers require that the **radius-server source-interface** command be configured in order to accept authentication from the RADIUS client. Note that this IP interface address is used for the NAS-IP-Address RADIUS attribute in the RADIUS Authentication Request.

radius-server source-interface *ip_or_host*

no radius-server source-interface

Syntax Description

ip_or_host	IP address or host name for the CSS RADIUS client. Enter the address in either dotted-decimal IP notation (for example, 192.168.11.1) or mnemonic host-name format (for example, myhost.mydomain.com).

Command Modes

Global configuration mode

Related Commands

show radius config
show radius stat
(config) radius-server dead-time
(config) radius-server source interface

radius-server timeout

To specify the time interval that the CSS waits for a reply to a RADIUS request before retransmitting requests to the RADIUS server, use the **radius-server timeout** command. Configure the number of retransmitted requests to the server through the **radius-server retransmit** command. Use the **no** form of this command to reset the interval to its default of 10 seconds.

radius-server timeout *time*

no radius-server timeout

Syntax Description

time	Time interval in seconds. Enter a number from 1 to 255. The default interval is 10.

Usage Guidelines

This command applies to the primary and secondary RADIUS servers.

Command Modes

Global configuration mode

Related Commands

show radius config
show radius stat
(config) radius-server retransmit

(config) replication file-error

To specify how the CSS handles file errors during content replication, use the **replication file-error** command.

replication file-error retry|skip

Syntax Description

retry	(Default) Replication pauses while the CSS periodically attempts to replicate a missing file
skip	The CSS skips the missing file and continues the replication process

Usage Guidelines

Under certain rare circumstances, it is possible for the CSS to encounter a file error during content replication. A file error can occur when an application or a user deletes a file from the publisher tree during a replication operation. If such an event occurs, the scan does not detect the deleted file and during replication the CSS may keep retrying the file until another scan occurs or the file becomes available.

Command Modes

Global configuration mode

Related Commands

replicate

(config) reporter

To create a reporter and enter reporter configuration mode, use the **reporter** command. A reporter is a software monitoring agent that a CSS uses to check and report the state of critical interfaces. You can also use a reporter to synchronize the states of the virtual routers that you associate with it.

reporter *reporter_name*

no reporter *reporter_name*

Syntax Description

reporter_name	Name of the reporter you are creating. Enter an unquoted text string with no spaces from 1 to 31 characters.

Command Modes

Global configuration mode

Usage Guidelines

When you enter the **reporter** command to access reporter configuration mode, the prompt changes to (config-reporter [*reporter_name*]). For information about commands available in this mode, see the "Reporter Configuration Mode Commands" section.

For more information about configuring and using a reporter, refer to the *Cisco Content Services Switch Redundancy Configuration Guide*.

Related Commands

(config-reporter) type
(config-reporter) vrid
(config-reporter) phy
(config-reporter) active
(config-reporter) suspend
show reporter

(config) restrict

To disable Telnet, SNMP, SSH, console, FTP, user database, secure or unsecure XML, or web management access to the CSS, use the **restrict** command. Use the **no** form of this command to enable access to the CSS.

restrict [**console**|**ftp**|**secure-xml**|**snmp**|**ssh**|**telnet**|**user-database**|**xml** |**web-mgmt**]

no restrict [**console**|**ftp**|**secure-xml**|**snmp**|**ssh**|**telnet**|**user-database**|**xml** |**web-mgmt**]

Syntax Description

console	Disables console access to the CSS. By default, this access is enabled.
ftp	Disables FTP access to the CSS. By default, this access is enabled.
secure-xml	Disables the transfer of XML configuration files to the CSS through secure SSL connections. By default, this access is disabled.
snmp	Disables SNMP access to the CSS. By default, this access is enabled.
ssh	Disables SSH access to the CSS. By default, this access is enabled.
telnet	Disables Telnet access to the CSS. By default, this access is enabled.
user-database	Disables users from clearing the running-config and creating or modifying usernames. Only administrator and technician users can perform these tasks. By default, this access is enabled.
xml	Disables the transfer of XML configuration files to the CSS through unsecure connections. By default, this access is disabled.
web-mgmt	Disables web management access to the CSS. By default, this access is disabled.

Command Modes

Global configuration mode

Usage Guidelines

Disable Telnet access when you want to use the Secure Shell Host (SSH) server.

If you enable secure XML through the **no restrict secure-xml** command, the CSS listens for connection requests on port 443. The client application can use SSL v2/3 or v3. However, the CSS performs all negotiations using SSL v3. The CSS requires a Secure Management license key to negotiate a secure connection using SSL strong encryption. Without the key, the CSS uses SSL weak encryption.

If you enable unsecure XML through the **no restrict xml** command, the CSS listens for XML connections on port 80.

Entering the **restrict** command does not prevent the CSS from listening for connection attempts on the restricted port. The CSS completes the TCP 3-way handshake and then terminates the connection with an error to prevent any data transfer from occurring. For UDP SNMP connections, the CSS simply discards the packets.

To secure restricted ports from unauthorized access, configure additional ACL clauses to deny packets destined to the ports, while permitting normal flow-through traffic. You can also use ACLs to secure the CSS.

Related Commands

show user-database
(config) sshd
(config) username

(config) rip

To configure the Routing Information Protocol (RIP) parameters on the CSS, use the **rip** command. The default mode is to send RIP version 2 (v2) and receive either version. The options for this global configuration mode command are:

- **rip advertise** - Advertises a route through RIP on the CSS
- **rip equal-cost** - Sets the number of equal-cost routes
- **rip redistribute** - Advertises routes from other protocols through RIP

For information on these options and associated variables, see the following commands. For information on additional **rip** command options in IP mode, see the **(config-circuit-ip) rip** command.

rip advertise

To advertise a route through RIP on the CSS, use the **rip advertise** command. Use the **no** form of this command to stop advertising a route through all RIP interfaces.

rip advertise *ip_address ip_mask_prefix* {*metric*}

no rip advertise *ip_address ip_mask_prefix*

Syntax Description

ip_address	IP address for the route prefix. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1).
ip_mask_prefix	IP mask. Enter the mask as either: • A prefix length in CIDR bitcount notation (for example, /24). Do not enter a space to separate the IP address from the prefix length. • A subnet mask in dotted-decimal notation (for example, 255.255.255.0).
metric	(Optional) Metric to use when advertising this route. Enter a number from 1 to 15. The default is 1.

Command Modes

Global configuration mode

rip equal-cost

To set the maximum number of routes RIP can use, use the **rip equal-cost** command. Use the **no** form of this command to reset the number of routes to the default of 1.

rip equal-cost *number*

no rip equal-cost

Syntax Description

number	Maximum number of routes. Enter a number from 1 to 15. The default is 1.

Command Modes

Global configuration mode

rip redistribute

To advertise routes from other protocols through RIP, use the **rip redistribute** command. By default, RIP advertises RIP routes and local routes for interfaces running RIP. This command advertises other routes. Use the **no** form of this command to stop advertising routes.

rip redistribute [**firewall**|**local**|**ospf**|**static**] {*metric*}

no rip redistribute [**firewall**|**local**|**ospf**|**static**]

Syntax Description

firewall	Advertises firewall routes through RIP.
local	Advertises local routes.
ospf	Advertises OSPF routes.
static	Advertises static routes.
metric	(Optional) Metric to use when advertising the route. Enter a number from 1 to 15. The default is 1.

Command Modes

Global configuration mode

(config) rmon-alarm

To enter RMON alarm configuration mode, use the **rmon-alarm** command. An RMON alarm allows you to monitor every SNMP object in the CSS for a desired transitory state. Use the **no** form of this command to delete an RMON alarm.

rmon-alarm *index*

no rmon-alarm *index*

Syntax Description

index	RMON alarm index number. Enter an integer from 1 to 65535. The RMON alarm index 65535 is administratively predefined and cannot be modified. If you enter this index number, a message similar to the following appears: `%% Index internally used. Administrative control not allowed.`

Usage Guidelines

When you use the **rmon-alarm** command to access this mode, the prompt changes to (config-rmonalarm [*index*]). For information about commands available in this mode, see the "RMON Alarm Configuration Mode Commands" section.

(config) rmon-event

To enter RMON event configuration mode, use the **rmon-event** command. An RMON event is associated with an RMON alarm. It defines what should occur when an RMON alarm is triggered. Use the **no** form of this command to delete an RMON event.

rmon-event *index*

no rmon-event *index*

Syntax Description

index	RMON event index number. Enter an integer from 1 to 65535. The RMON event index 65535 is administratively predefined and cannot be modified. If you enter this index number, a message similar to the following appears: `%% Index internally used. Administrative control not allowed.`

Usage Guidelines

When you use the **rmon-event** command to access this mode, the prompt changes to (config-rmonevent [*index*]). For information about commands available in this mode, see the "RMON Event Configuration Mode Commands" section.

(config) rmon-history

To enter RMON history configuration mode, use the **rmon-history** command. Use the **no** form of this command to delete an RMON history.

rmon-history *index*

no rmon-history *index*

Syntax Description

index	RMON history index number. Enter an integer from 1 to 65535. Some history index numbers are administratively predefined and cannot be modified. If you enter an index number under administrative control, a message similar to the following appears: `%% Index internally used. Administrative control not allowed.`

Usage Guidelines

When you use the **rmon-history** command to access this mode, the prompt changes to (config-rmonhistory [*index*]). For information about commands available in this mode, see the "RMON History Configuration Mode Commands" section.

(config) service

To access service configuration mode and configure a service, use the **service** command. A service is an entity that contains and provides Internet content. It is identified by a name, an IP address, and optimally, a protocol and a port number. When you create a service, you can apply content rules to it. The rules allow the CSS to direct or deny requests for content from the service.

Use the **no** form of this command to delete an existing service.

service *service_name*

no service *service_name*

Syntax Description

service_name	The name of a new service you want to create or an existing service you want to modify. Enter an unquoted text string with no spaces and a maximum length of 31 characters. To see a list of existing service names, enter: **`service ?`**

Usage Guidelines

When you use the **service** command to access service mode, the prompt changes to (config-service [*name*]). For information about commands available in this mode, see the "Service Configuration Mode Commands" section.

Related Commands

(config-service) ip address
(config-service) port

(config) setspan

To configure switched port analyzer (SPAN) on a CSS, use the **setspan** command. This command instructs the CSS to monitor all incoming and/or outgoing traffic on a specified SSPAN port by copying the packets to a specified DSPAN port on the same module in the CSS. This command is disabled by default.

Use the **no** form of the command to reset the default SPAN state to disabled.

setspan src_port *number* **dest_port** *number* **copyBoth|copyTxOnly|copyRxOnly**

no setspan src_port *number* **dest_port** *number* **copyBoth|copyTxOnly|copyRxOnly**

Syntax Description

src_port *number*	Source port keyword and number of the SSPAN port (in slot/port format) that you want to monitor. The CSS copies all packets that are received or transmitted on this port to the DSPAN port.
dest_port *number*	Destination port keyword and number of the DSPAN port (in slot/port format) where you want to connect the network analyzer, protocol analyzer, or RMON probe. The CSS copies the packets that flow through the SSPAN port to the DSPAN port that you specify. The DSPAN port must reside on the same module as the SSPAN port.
copyBoth	CSS copies to the DSPAN port packets that the SSPAN port transmits to the network (egress traffic) and receives from the network (ingress traffic).
copyTxOnly	CSS copies to the DSPAN port only those packets that the SSPAN port transmits to the network.
copyRxOnly	CSS copies to the DSPAN port only those packets that the SSPAN port receives from the network.

Usage Guidelines

Once you configure a port as a DSPAN port, the CSS removes it from all VLANs and ignores ingress traffic on that port. In addition, the DSPAN port does not participate in Spanning Tree Protocol (STP) or routing protocols such as RIP and OSPF.

Note If the combined bandwidth of the ingress and egress traffic of the SSPAN port exceeds the bandwidth of the DSPAN port, the DSPAN port may become oversubscribed.

Related Commands

show setspan

(config) snmp

To configure Simple Network Management Protocol (SNMP) parameters, use the **snmp** command. The options for this global configuration mode command are:

- **snmp auth-traps** - Enables reception of SNMP authentication traps
- **snmp community** - Sets or modifies SNMP community names and access properties
- **snmp contact** - Sets or modifies the SNMP system contact name
- **snmp location** - Sets or modifies the SNMP system location
- **snmp name** - Sets or modifies the SNMP name for this system
- **snmp reload-enable** - allows SNMP-based reset of the CSS
- **snmp trap-host** - Sets or modifies the SNMP host to receive traps from this system
- **snmp trap-source** - Sets the source IP address in the traps generated by the CSS
- **snmp trap-type enterprise** - Enables SNMP enterprise trap types
- **snmp trap-type generic** - Enables SNMP generic trap types

Note The CSS supports SNMP version 2C (SNMPv2C), known as "community-based SNMP," and standard Management Information Base (MIB-II) objects, along with an extensive set of enterprise objects. You can use any compatible network management system to monitor and control a CSS.

The CSS generates traps in SNMP version 1 (SNMP v1) format.

For more information on these options and associated variables, see the following commands.

Related Commands

(config) restrict telnet
(config) rmon-alarm
(config) rmon-event
(config) rmon-history

snmp auth-traps

To enable reception of SNMP authentication traps, use the **snmp auth-traps** command. Use the **no** form of this command to disable reception of authentication traps.

snmp auth-traps

no snmp auth-traps

Usage Guidelines

The CSS generates these traps when an SNMP management station attempts to access your system with invalid community names. The CSS generates traps in SNMP v1 format.

Command Modes

Global configuration mode

Related Commands

snmp trap-type generic

snmp community

To set or modify SNMP community names and access properties, use the **snmp community** command. You may specify as many community names as you wish. Use the **no** form of this command to remove a community name and set it to Cisco Systems, Content Network Systems.

snmp community *community_name* [**read-only**|**read-write**]

no snmp community *community_name*

Syntax Description

community_name	SNMP community name for this system. Enter an unquoted text string with no space and a maximum length of 12 characters.
read-only	Allows read-only access for this community.
read-write	Allows read-write access for this community.

Command Modes

Global configuration mode

snmp contact

To set or modify the contact name for the SNMP system, use the **snmp contact** command. You can specify only one contact name. Use the **no** form of this command to remove the contact name.

snmp contact "*contact_name***"**

no snmp contact

Syntax Description

"*contact_name*"	Name of the contact person for this system. You can also include information on how to contact the person; for example, a phone number or e-mail address. Enter a quoted text string with a maximum of 255 characters including spaces.

Command Modes

Global configuration mode

snmp location

To set or modify the SNMP system location, use the **snmp location** command. You can specify only one location. Use the **no** form of this command to remove the location and set it to Customer Premises.

snmp location "*location***"**

no snmp location

Syntax Description

"*location*"	Physical location of this system. Enter a quoted text string with a maximum length of 255 characters.

Command Modes

Global configuration mode

snmp name

To set or modify the SNMP name for this system, use the **snmp name** command. You can specify only one name. Use the **no** form of this command to remove the SNMP name for this system and set it to Support.

snmp name "*name***"**

no snmp name

Syntax Description

"*name*"	Unique name assigned to this system by the system administrator. The standard convention is the system's fully-qualified domain name (for example, user.domain.com). Enter a quoted text string with a maximum of 255 characters.

Command Modes

Global configuration mode

snmp reload-enable

To allow the rebooting of the CSS through SNMP, use the **snmp reload-enable** command. Use the **no** form of this command to disallow a CSS reboot through SNMP (default behavior).

snmp reload-enable {*reload_value*}

no snmp reload-enable

Syntax Description

reload_value	Object used to control apSnmpExtReloadSet, providing the SNMP-based reboot. When the object is set to 0, an SNMP reboot is not allowed. When the object is set between 1 to 2^{32}, a reboot may be caused with any write value to apSnmpExtReloadSet. For security purposes, this object always returns 0 when read.

Command Modes

Global configuration mode

Usage Guidelines

When you use the **snmp reload-enable** command, it allows any SNMP write to the reload object to force a CSS reboot. The reload object name is apSnmpExtReloadSet (1.3.6.1.4.1.2467.1.22.7). You can find this object in the enterprise MIB, snmpext.mib. When you include a reload value, an SNMP write equal to the *reload_value* forces a CSS reboot.

snmp trap-host

To set or modify the SNMP host to receive traps from this system, use the **snmp trap-host** command. Use the **no** form of this command to remove a specified trap host.

snmp trap-host *ip_or_host community_name* **snmpv2**

no snmp trap-host *ip_or_host*

Syntax Description

ip_or_host	IP address or host name of an SNMP host that has been configured to receive traps. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or in mnemonic host-name format (for example, myhost.mydomain.com). You can specify a maximum of five hosts.
community_name	Community name to use when sending traps to the specified SNMP host. Enter an unquoted text string with no spaces and a maximum length of 12 characters.
snmpv2	Specifies that traps be sent to the host in SNMP v2C format.

Usage Guidelines The CSS generates traps in SNMP v1 format.

Command Modes Global configuration mode

snmp trap-source

To set the source IP address in the traps generated by the CSS, use the **snmp trap-source** command. Use the **no** form of this command to return SNMP source traps to the default of the management port IP address.

snmp trap-source [**egress-port**|**management**|**specified** *source_ip_address*]

no snmp trap-source

Syntax Description

egress-port	Obtains the source IP address for the SNMP traps from the VLAN circuit IP address configured on the egress port used to send the trap. You do not need to enter an IP address because the address is determined dynamically by the CSS.
management	Places the management port IP address in the source IP field of the trap. This is the default setting.
specified *source_ip address*	Allows you to enter the IP address to be used in the source IP field of the traps. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).

Command Modes

Global configuration mode

snmp trap-type enterprise

To enable SNMP enterprise traps and configure trap types, use the **snmp trap-type enterprise** command. Use the **no** form of this command to disable all or a specific trap. Use the **no snmp trap-type enterprise** command to disable all traps.

snmp trap-type enterprise {*dos_attack_type* {**trap-threshold** *threshold_value*}|**chmgr-module-transition**|**chmgr-ps-transition** |**isc-lifetick-failure**|**login-failure**|**reload**|**redundancy-transition** |**reporter-transition**|**service-transition**}

no snmp trap-type enterprise {*dos_attack_type* |**chmgr-module-transition**|**chmgr-ps-transition**|**isc-lifetick-failure** |**login-failure**|**reload**|**redundancy-transition** |**reporter-transition**|**service-transition**}

Syntax Description

enterprise	When you use this keyword alone, it enables enterprise traps. You must enable enterprise traps before you configure an enterprise trap option.
dos_attack_type	(Optional) Generates SNMP enterprise traps when a Denial of Service (DoS) attack event occurs. One trap is generated each second when the number of attacks during that second exceeds the threshold for the configured DoS attack type. The options are as follows: • **dos-illegal-attack** generates traps for illegal addresses, either source or destination. Illegal addresses are loopback source addresses, broadcast source addresses, loopback destination addresses, multicast source addresses, or source addresses that you own. The default trap threshold for this type of attack is 1 per second. • **dos-land-attack** generates traps for packets that have identical source and destination addresses. The default trap threshold for this type of attack is 1 per second. • **dos-smurf-attack** generates traps when the number of pings with a broadcast destination address exceeds the threshold value. The default trap threshold for this type of attack is 1 per second. • **dos-syn-attack** generates traps when the number of TCP connections that are initiated by a source, but not followed with an acknowledgment (ACK) frame to complete the three-way TCP handshake, exceeds the threshold value. The default trap threshold for this type of attack is 10 per second.
trap-threshold *threshold_value*	(Optional) Overrides a default trap threshold. For the *threshold_value*, enter a number from 1 to 65535.

chmgr-module-transition	(Optional) Generates SNMP enterprise traps if a module (for example, SCM, FEM, GEM) is inserted into or removed from a powered-on CSS 11503 or 11506 chassis.
chmgr-ps-transition	(Optional) Generates SNMP enterprise traps when the CSS 11503 or 11506 power supply changes state (powered off, on, or removed from the CSS chassis).
isc-lifetick-failure	(Optional) Generates SNMP enterprise traps when an ISC lifetick message failure occurs on a CSS.
login-failure	(Optional) Generates SNMP enterprise traps when a CSS login failure occurs. An alert-level log message is also generated.
reload	(Optional) Generates SNMP enterprise traps when a CSS reboot occurs. A trap is generated when a reboot is initiated directly through SNMP.
redundancy-transition	(Optional) Generates SNMP enterprise traps when the CSS redundancy transitions state.
reporter-transition	(Optional) Generates SNMP enterprise traps when the CSS reporter transitions state (for example, the reporter is activated or suspended, or the VRID peering virtual routers or critical phy interfaces change state).
service-transition	(Optional) Generates SNMP enterprise traps when a CSS service transitions state. A trap is generated when a service fails and when a failed service resumes proper operation.

Command Modes

Global configuration mode

Usage Guidelines

You must enable enterprise traps before you configure an enterprise trap option. You can enable the CSS to generate enterprise traps when DoS attack events occur, a login fails, or a CSS service transitions state.

The CSS generates traps in SNMP v1 format.

Related Commands

snmp auth-traps
snmp trap-host
show log traplog

snmp trap-type generic

To enable SNMP generic trap types, use the **snmp trap-type generic** command. The generic SNMP traps consist of cold start, warm start, link down, and link up. Use the **no** form of this command to disable a generic trap.

snmp trap-type generic

no snmp trap-type generic

Command Modes

Global configuration mode

Usage Guidelines

The CSS generates traps in SNMP v1 format.

Related Commands

snmp auth-traps
snmp trap-host
show log traplog

(config) sntp

To configure the SNTP server on the CSS, use the **sntp** command. You can configure one SNTP server. Use the **no** form of this command to remove the SNTP server or reset the poll interval.

sntp [**server** *ip_address* {**version** *number*}|**poll-interval** *seconds*]

no sntp [**server**|**poll-interval**]

Syntax Description

server *ip_address*	Defines the SNTP server. Enter the IP address for the server.
version *number*	Defines the version of the SNTP server. For the *number* value, enter a number from 1 to 4. The default version is 1.
poll-interval *seconds*	Defines the poll interval in seconds between SNTP request messages. For the *seconds* value, enter a number from 16 to 16284. The default is 64.

Command Modes

Global configuration mode

Usage Guidelines

Before you synchronize the CSS with an SNTP server, make sure you configure the proper time zone for the CSS (for example, to EST). Also make sure that the time difference between the CSS internal clock and the SNTP server clock is less than 24 hours. Otherwise, the CSS will not synchronize its clock with the SNTP server.

Related Commands

clock
show sntp global

(config) spanning-packets

To configure the number of packets spanned for the search of the HTTP Header termination string, use the **spanning-packets** command. Use the **no** form of this command to reset the number of packets spanned to the default value of 6.

spanning-packets *number*

no spanning-packets

Syntax Description

number	Number of packets spanned for the search of the HTTP Header termination string. Enter a number from 1 to 20.

Usage Guidelines

In some environments, URL, cookie strings, or HTTP header information can span over multiple packets. In these environments, the CSS can parse multiple packets for Layer 5 information before making load-balancing decisions. Through the global configuration mode **spanning-packets** command, the CSS can parse a maximum of 20 packets with a default of 6.

The CSS makes the load-balancing decision as soon as it finds a match and does not require parsing of all of the configured number of spanned packets. Because parsing multiple packets does impose a longer delay in connection, performance can be impacted by longer strings that span mulitple packets.

Command Modes

Global configuration mode

(config) sshd

To control the Secure Shell Host server, use the **sshd** command. The options for this global configuration mode command are:

- **sshd keepalive** - Enables SSHD keepalive
- **sshd port** - Sets the SSHD port
- **sshd server-keybits** - Sets the number of bits in the server key

Note Disable Telnet access when you want to use the Secure Shell Host (SSH) server.

For more information on these options and associated variables, see the following commands.

Related Commands **(config) restrict telnet**

sshd keepalive

To enable SSHD keepalive, use the **sshd keepalive** command. SSHD keepalive is enabled by default. Use the **no** form of this command to disable SSHD keepalive.

sshd keepalive

no sshd keepalive

Command Modes Global configuration mode

sshd port

To set the port number that the server listens to connections from clients, use the **sshd port** command. Use the **no** form of this command to reset the port number to the default of 22.

sshd port *number*

no sshd port

Syntax Description

number	Port number. Enter a number from 22 to 65535. The default is 22.

Command Modes

Global configuration mode

sshd server-keybits

To set the number of bits in the server key, use the **sshd server-keybits** command. Use the **no** form of this command to reset the number of bits to the default of 768.

sshd server-keybits *number*

no sshd server-keybits

Syntax Description

number	Number of bits in the server key. Enter a number from 512 to 1024. The default is 768.

Command Modes

Global configuration mode

Usage Guidelines

The valid range for this command is 512 to 1024. However, to maintain backward compatibility with version 5.00, the CSS allows you to enter a value from 512 to 32768. If you enter a value greater than 1024, the CSS changes the value to the default of 768.

When you reboot the CSS, the following error message appears to remind you of the valid range:

```
NETMAN-3: sshd: Bad server key size <configured value; range 512
to 1024; defaulting to 768
```

(config) ssl-l4-fallback

To disable or reenable the CSS insertion of the Layer 4 hash value, based on the source IP address and destination address pair, into the sticky table, use the **ssl-l4-fallback** command. By default, the CSS inserts the Layer 4 hash value into the sticky table.

ssl-l4-fallback disable|enable

Syntax Description

disable	Disables the CSS from inserting the Layer 4 hash value into the sticky table and continues to look for SSL version 3 session IDs
enable	Resets the CSS to its default behavior of inserting a Layer 4 hash value into the sticky table

Usage Guidelines

Insertion of the Layer 4 hash value into the sticky table occurs when more than three frames are transmitted in either direction (client-to-server, server-to-client) or if SSL version 2 is in use on the network. If either condition occurs, the CSS inserts the Layer 4 hash value into the sticky table, overriding the further use of the SSL version 3 session ID.

The **ssl-l4-fallback** command is only applicable when the **(config-owner-content) advanced-balance ssl** method is specified for a content rule, which forces the content rule to stick to a server based on SSL version 3 session ID.

The use of the **ssl-l4-fallback** command may be necessary in a lab environment when testing SSL with a small number of clients and servers, where some retransmissions might occur. In this case, you would not want to use the Layer 4 hash value because it will skew the test results.

Note Do not use the **ssl-l4-fallback disable** command if SSL version 2 is in use on the network.

Related Commands

(config-owner-content) advanced-balance

(config) ssl associate

To specify an SSL certificate, RSA key or DSA key pair, or Diffie-Hellman parameter association to an imported or generated file, use the **ssl associate** command. Use the **no** form of the command to remove an association.

ssl associate *association_type association_name filename*

no ssl associate *association_type association_name*

Syntax Description

association_type	SSL association type. Enter one of the following: • **cert** - A certificate • **rsakey** - An RSA key pair • **dsakey** - ADSA key pair • **dhparam** - A Diffie-Hellman key exchange parameter file
association_name	Name of the association. Enter a name with a maximum of 31 characters.
filename	Name of the file containing the certificate, key pair, or Diffie-Hellman parameters. Enter a filename with a maximum of 128 characters.

Usage Guidelines

After you import or generate certificate and key pair files, you must distinguish to the CSS whether these files contain certificates, private keys, or Diffie-Hellman parameters. You do this by associating certificate names, private/public key pair names, or Diffie-Hellman parameter names to the particular imported files.

When you associate the entries specified in the various certificate and private key commands to files, CSS stores the bindings in the running configuration. Before you log out or reboot the CSS, you must copy the contents of the running-config file to the startup-config file to save configuration changes and have the CSS use this configuration on subsequent reboots. When you reboot the CSS, the certificate and key associations are automatically loaded.

The **no** form of this command will not function if the association is in use by an active SSL proxy list.

Related Commands

copy ssl
show ssl
(ssl-proxy-list) ssl-server

(config) ssl crl-record

To configure the CSS to obtain a certificate revocation list (CRL) from a certificate authority (CA) and periodically download the CRL through HTTP, use the **ssl crl-record** command. Use the **no** form of the command to remove the CRL record.

ssl crl-record *crl_name url sign_cert hours*

no ssl crl-record *crl_name*

Syntax Description

crl_name	Name for the CRL record. Enter a string with a maximum of 31 characters and no spaces.
url	URL where the CRL is located. Enter a string with a maximum of 168 characters and no spaces (for example, http://www.example.com/crl/clientcrllist.crl).

sign_cert	Name of the CA certificate that signed the CRL. The CA certificate verifies that the CRL is authentic. You must import this certificate on the CSS before configuring the CRL.
hours	Number of hours to wait before retrieving an updated CRL. Enter a value from 0 to 2000. If you enter a value of 0, the CSS will not retrieve or update the CRL.

Usage Guidelines

You can assign only one CRL record to a virtual SSL server. However, you can configure a maximum of 10 CRL records.

Related Commands

show ssl crl-record
(ssl-proxy-list) ssl-server number crl

(config) ssl gencert

To generate and save a temporary certificate to a file on a CSS disk, use the **ssl gencert** command. For purposes of SSL testing, you may want to generate a temporary certificate by generating a CSR and signing it with your own private key.

ssl gencert certkey *certkey* **signkey** *signkey certfile* **"***password***"**

Syntax Description

certkey *certkey*	Name of the RSA or DSA key pair that the certificate is based on. Enter an unquoted string with a maximum of 31 characters.
signkey *signkey*	RSA or DSA key pair to be used to sign the certificate. Enter an unquoted string with a maximum of 31 characters.

certfile	Name of the file used to store the certificate as a file on the CSS disk. Enter an unquoted string with a maximum of 31 characters.
"*password*"	Password used to DES encode the certificate file before it is stored as a file on the CSS disk. Encoding the file prevents unauthorized access to the imported certificate and private key on the disk. Enter the password as a quoted string. The password appears in the CSS running configuration as a DES-encoded string.

Usage Guidelines

Generate keys and certificates on the CSS for purposes of testing. This command produces a valid certificate or key pair (primarily useful for testing purposes). Be aware that most web browsers will flag the certificate as signed by an unrecognized signing authority.

The **ssl gencert** command can sign RSA or DSA certificates with either an RSA key pair or a DSA key pair. You generate the certificate based on:

- The key pair that the certificate is based on (RSA or DSA)
- The key used to sign the certificate

For detailed information on using this command, refer to the *Cisco Content Services Switch SSL Configuration Guide*.

Related Commands

show ssl

(config) ssl gencsr

To generate a Certificate Signing Request (CSR) file for an RSA key pair file and transfer the certificate request to the Certificate Authority (CA), use the **ssl gencsr** command. You must generate a CSR file if you are requesting a new certificate or renewing a certificate. When the CA signs the CSR, using its RSA private key, the CSR becomes the certificate.

ssl gencsr *rsakey*

Syntax Description

rsakey	Key that the RSA certificate is built on. It is the public key that is embedded in the certificate. The RSA key pair must already be loaded on the CSS and you must associate an RSA key pair name to the generated RSA key pair. If the appropriate key pair does not exist, the CSS logs an error message

Usage Guidelines

The **ssl gencsr** command produces a valid certificate or key pair (primarily useful for testing purposes). Be aware that most web browsers will flag the certificate as signed by an unrecognized signing authority.

The **ssl gencsr** command generates a CSR in PKCS10 format.

For detailed information on using this command, refer to the *Cisco Content Services Switch SSL Configuration Guide*.

Related Commands

show ssl

(config) ssl gendh

To generate a Diffie-Hellman key agreement parameter file on the CSS, use the **ssl gendh** command. Diffie-Hellman is a shared key agreement algorithm. Diffie-Hellman key exchange uses a complex algorithm and public and private keys to encrypt and then decrypt packet data. The CSS disk stores the generated parameters as a file.

ssl gendh *filename numbit* **"***password***"**

Syntax Description

filename	Name of the key or key pair file. Enter a name with a maximum of 31 characters. The filename is used only for identification in the CSS.

numbits	Key strength. The number of bits in the file defines the size of the key or key pair used to secure web transactions. Longer keys produce a more secure implementation by increasing the strength of the DSA security policy. Available selections in bits are: • **512** - Least security • **768** - Normal security • **1024** - High security • **2048** - Highest security
"*password*"	Password used to DES encode the certificate file before it is stored as a file on the CSS disk. Encoding the file prevents unauthorized access to the imported certificate and private key on the disk. Enter the password as a quoted string. The password appears in the CSS running configuration as a DES-encoded string.

Usage Guidelines

Generation of a Diffie-Hellman key agreement parameter file can sometimes take a lengthy period of time (perhaps a maximum of 20 minutes) and is a CPU-intensive utility. If you use the **ssl gendh** command, ensure that the CSS is not actively passing traffic at the same time to avoid impacting CSS performance. For detailed information on using this command, refer to the *Cisco Content Services Switch SSL Configuration Guide*.

Related Commands

show ssl

(config) ssl gendsa

To generate a DSA private/public key pair for asymmetric encryption on the CSS, use the **ssl gendsa** command. DSA is the public key exchange cryptographic system developed by the National Institutes of Science and Technology. DSA can only be used for digital signatures (signings) but not for key exchange. The CSS disk stores the generated DSA key pair as a file.

ssl gendsa *filename numbit* "*password*"

Syntax Description

filename	Name of the key or key pair file. Enter a name with a maximum of 31 characters. The filename is used only for identification in the CSS.
numbits	Key strength. The number of bits in the file defines the size of the key or key pair used to secure web transactions. Longer keys produce a more secure implementation by increasing the strength of the DSA security policy. Available selections in bits are: • **512** - Least security • **768** - Normal security • **1024** - High security The **2048** selection, highest security, is not available for use with the **ssl gendsa** command.
"*password*"	Password used to DES encode the certificate file before it is stored as a file on the CSS disk. Encoding the file prevents unauthorized access to the imported certificate and private key on the disk. Enter the password as a quoted string. The password appears in the CSS running configuration as a DES-encoded string.

Usage Guidelines

The **ssl gendsa** command produces a valid certificate or key pair (primarily useful for testing purposes). Be aware that most web browsers will flag the certificate as signed by an unrecognized signing authority.

For detailed information on using this command, refer to the *Cisco Content Services Switch SSL Configuration Guide*.

Related Commands

show ssl

(config) ssl genrsa

To generate an RSA private/public key pair for asymmetric encryption on the CSS, use the **ssl genrsa** command. RSA key pairs are used to sign and encrypt packet data, and are a requirement before another device (client or web server) can exchange an SSL certificate with the CSS. The key pair refers to a public key and its corresponding private (secret) key. The CSS stores the generated RSA key pair as a file.

ssl genrsa *filename numbit* **"***password***"**

Syntax Description

filename	Name of the key or key pair file. Enter a name with a maximum of 31 characters. The filename is used only for identification in the CSS.
numbits	Key strength. The number of bits in the file defines the size of the key or key pair used to secure web transactions. Longer keys produce a more secure implementation by increasing the strength of the DSA security policy. Available selections in bits are: • **512** - Least security • **768** - Normal security • **1024** - High security • **2048** - Highest security
"*password*"	The password used to DES encode the certificate file before it is stored as a file on the CSS disk. Encoding the file prevents unauthorized access to the imported certificate and private key on the disk. Enter the password as a quoted string. The password appears in the CSS running configuration as a DES-encoded string.

Usage Guidelines

The **ssl genrsa** command produces a valid certificate or key pair (primarily useful for testing purposes). Be aware that most Web browsers will flag the certificate as signed by an unrecognized signing authority.

For detailed information on using this command, refer to the *Cisco Content Services Switch SSL Configuration Guide*.

Related Commands

show ssl

(config) ssl verify

To verify a certificate against a key pair, use the **ssl verify** command. A digital certificate is built around a public key, and it can only be used with one key pair. This command compares the public key in the associated certificate with the public key stored with the associated private key, and verify that they are both the same.

ssl verify *certname keyname*

Syntax Description

certname	Association name of the certificate used to verify against the specified key pair
keyname	Association name of the key pair used to verify against the specified certificate

Usage Guidelines

If the certificate does not match the public and private key pair, the CSS logs an error message.

# (config) ssl-proxy-list

To access SSL proxy list configuration mode and configure an SSL proxy configuration list, use the **ssl-proxy-list** command. An SSL proxy configuration list is a group of related virtual SSL servers that are associated with an SSL service. The SSL modules in the CSS use these servers to properly process and terminate SSL communications between the client and the web server.

In global configuration mode, use the **no** form of this command to delete an existing list.

ssl-proxy-list *name*

(config) **no ssl-proxy-list** *name*

Syntax Description

name	Name of a new SSL proxy list you want to create or an existing list you want to modify. Enter an unquoted text string with no spaces and a maximum length of 31 characters. To see a list of existing names, enter: `#(config) ssl-proxy-list ?`

Usage Guidelines

You can access the ssl-proxy-list configuration mode from any configuration mode except for the ACL, boot, group, RMON, or owner configuration modes. When you use the **ssl-proxy-list** command to access this mode, the prompt changes to (ssl-proxy-list [*name*]). For information about commands available in this mode, see the "SSL-Proxy-List Configuration Mode Commands" section.

Note You cannot delete an SSL proxy list if an SSL service is in use and contains the active SSL proxy list. You must first suspend the SSL service to delete a specific list.

(config) tacacs-server

To configure the CSS as a client of a TACACS+ server, authenticates users, and authorizes and accounts for configuration and nonconfiguration commands, use the **tacac-server** command. The options for this command are:

- **tacacs-server** *ip_address port* - Defines a TACACS+ server
- **tacacs-server account** - Enables the the TACACS+ server to receive accounting reports for CSS commands
- **tacacs-server authorize** - Enables the the TACACS+ server to authorize CSS commands
- **tacacs-server frequency** - Sets the global CSS TACACS+ keepalive frequency
- **tacacs-server key** - Defines a global encryption key
- **tacacs-server send-full-command** - Enables the CSS to expand user-executed abbreviated commands to their full command syntax before sending them to the TACACS+ server
- **tacacs-server timeout** - Sets the global CSS TACACS+ timeout period

For information about these commands and any associated arguments, see the **tacac-server** commands in this section.

tacacs-server *ip_address port*

To define a TACACS+ server, use the **tacacs-server** *ip_address port* command. You must provide the IP address and port number for the server. You can define the keepalive frequency, timeout period, and encryption key, and designate the server as the primary server. Use the **no** form of this command to remove the server.

tacacs-server *ip_address port* {*timeout* [**"***cleartext_key***"**|*des_key*]}
{**primary**} {**frequency** *number*}

no tacacs-server *ip_address port*

Syntax Description

ip_address	IP address of the TACACS+ server. Enter the IP address in dotted-decimal format.
port	TCP port of TACACS+ server. The default port is 49. You can enter a port number from 1 to 65535.
timeout	(Optional) Amount of time to wait for a response from the server. Enter a number from 1 to 255. The default is 5 seconds. Defining this option overrides the **tacacs-server timeout** command.
"*cleartext_key*"|*des_key*	Shared secret between the CSS and the server. You must define an encryption key to encrypt TACACS+ packet transactions between the CSS and the TACACS+ server. If you do not define an encryption key, packets are not encrypted. The shared secret value is identical to the one on the TACACS+ server. The shared secret key can be either clear text entered in quotes or the DES encrypted secret entered without quotes. The clear text key is DES encrypted before it is placed in the running configuration. Either key type can have a maximum of 100 characters. Defining this option overrides the **tacacs-server key** command.
primary	(Optional) Assigns the TACACS+ server precedence over the other configured servers. You can specify only one primary server.
frequency *number*	(Optional) Allows you to set the keepalive frequency for the specified TACACS+ server. The default number variable is 5 seconds. The range for the variable is 0 to 255. A setting of 0 disables keepalives. Defining this option overrides the **tacacs-server frequency** command.

Command Modes

Global configuration mode

Usage Guidelines

To change the keepalive frequency, timeout period, or encryption key for a specific TACACS+ server, you must delete the server and then redefine it with the updated parameter.

To apply a global keepalive frequency, timeout period, or encryption key change to a TACACS+ server, you must delete the server and then reconfigure the server.

After configuring the TACACS+ server, enable TACACS+ authentication for console and virtual logins (if the user and password pair is not in the local user database) through the **(config) console authentication** and **(config) virtual authentication** commands.

Note The TACACS+ server must be configured before defining the server on the CSS.

Related Commands

show tacacs-server
(config) console authentication
(config) virtual authentication

tacacs-server account

To enable the TACACS+ server to receive accounting reports for all commands that change or do not change the CSS running configuration, use the **tacacs-server account** command. Use the **no** form of this command to disable accounting.

tacacs-server account config|non-config

no tacacs-server account config|non-config

Syntax Description

config	Enables the TACACS+ server to receive accounting reports for all commands that change the running configuration
non-config	Enables the TACACS+ server to receive accounting reports for all commands that do not change the running configuration

Usage Guidelines

TACACS+ accounting allows the TACACS+ server to receive an accounting report for commands that the user can execute. CSS accounting divides the command set into two categories:

- Configuration commands that change the CSS running configuration.
- Nonconfiguration commands that do not change the running configuration. These commands include, but are not limited to, mode transition commands, show commands, and administrative commands.

By default, the CSS disables accounting. When you enable accounting, you can account for configuration commands, nonconfiguration commands, or both.

Note Failure of the TACACS+ server does not result in the suspension of user activity.

Related Commands

show tacacs-server

tacacs-server authorize

To enable the TACACS+ server to authorize commands that change or do not change the CSS running configuration, use the **tacacs-server authorize** command. Use the **no** form of this command to disable authorization.

tacacs-server authorize config|non-config

no tacacs-server authorize config|non-config

Syntax Description

config	Enables authorization of all commands that change the running configuration
non-config	Enables authorization of all commands that do not change the running configuration

Usage Guidelines

TACACS+ authorization allows the TACACS+ server to control specific CSS commands that the user can execute. CSS authorization divides the command set into two categories:

- Configuration commands that change the CSS running configuration.
- Nonconfiguration commands that do not change the running configuration. These commands include, but are not limited to, mode transition, show, and administrative commands.

By default, authorization is disabled. When authorization is enabled, the TACACS+ server is responsible for granting permission or denying all attempts to execute commands. When you enable authorization, the exchange between the TACACS+ server and the CSS causes a delay in executing the command.

Note Failure of the TACACS+ server results in the failure of all authorization requests and the suspension of user activity unless another server is reachable. To enable users to execute commands in this case, configure a failover authentication method to a local user database. Users will need to log back into the CSS.

Related Commands

show tacacs-server

tacacs-server frequency

To define the global keepalive frequency for use with all configured TACACS+ servers, use the **tacacs-server frequency** command. Use the **no** form of the command to reset the keepalive frequency to its default of 5 seconds.

tacacs-server frequency *seconds*

no tacacs-server frequency

Syntax Description

seconds	Keepalive frequency in seconds. Enter an integer from 0 to 255. The default is 5 seconds. A setting of 0 disables keepalives.

Usage Guidelines

To determine the availability of the TACACS+ servers, the CSS sends periodic TCP keepalive probes to them. If the server does not respond to the probes within the configured timeout period, the CSS considers the server unavailable.

A keepalive frequency defined when specifying a TACACS+ server overrides the global keepalive frequency.

To apply a modified global keepalive frequency to a configured CSS TACACS+ server, remove the server and reconfigure it.

Related Commands

show tacacs-server

tacacs-server key

To specify a global shared secret between the CSS and the server, use the **tacacs-server key** command. Use the **no** form of this command to remove the global key.

tacacs-server key [**“***cleartext_key***”**|*des_key*]

no tacacs-server key

Syntax Description

“*cleartext_key*”|*des_key*	Shared secret between the CSS and the server. You must define an encryption key to encrypt TACACS+ packet transactions between the CSS and the TACACS+ server. If you do not define an encryption key, packets are not encrypted. The shared secret value is identical to the one on the TACACS+ server. The shared secret key can be either clear text entered in quotes or the DES encrypted secret entered without quotes. The clear text key is DES encrypted before it is placed in the running configuration. Either key type can have a maximum of 100 characters.

Command Modes

Global configuration mode

Usage Guidelines

The CSS allows you to define a global encryption key for communications with all configured TACACS+ servers. To encrypt TACACS+ packet transactions between the CSS and the TACACS+ server, you must define an encryption key. If you do not define an encryption key, packets are not encrypted. The key is a shared secret value that is identical to the one on the TACACS+ server. A shared secret defined when specifying a TACACS+ server overrides the global secret. See the **tacacs-server ip_address port** command.

Related Commands

show tacacs-server

tacacs-server send-full-command

To reset the CSS default behavior of expanding user-executed abbreviated commands to their full command syntax before the CSS sends them to the TACACS+ server, use the **tacacs-server send-full-command** command. Use the **no** form of the command to send user-executed commands exactly as entered to the TACACS+ server without expanding abbreviated commands.

tacacs-server send-full-command

no tacacs-server send-full-command

tacacs-server timeout

To define the global timeout period for use with all configured TACACS+ servers, use the **tacacs-server timeout** command. Use the **no** form of the command to reset the timeout period to its default of 5 seconds.

tacacs-server timeout *seconds*

no tacacs-server timeout

Syntax Description

seconds	Amount of time to wait for a response from the server. Enter a number from 1 to 255. The default is 5 seconds.

Usage Guidelines

To determine the availability of the TACACS+ servers, the CSS sends periodic keepalive probes to them. If the server does not respond to the probe within the timeout period, the CSS considers the server unavailable.

If the CSS attempts to contact the server and does not receive a response within the defined timeout value, it will use another server. The next configured server is contacted and the process repeated. If a second (or third) TACACS+ server has been identified, that server is selected as the active server.

If the CSS cannot reach all three TACACS+ servers, users will not be authenticated and cannot log into the CSS unless TACACS+ is used in combination with a RADIUS or local server, as defined through the **(config) console authentication** command or the **(config) virtual authentication** command.

Note The timeout period defined when specifying a TACACS+ server overrides the global timeout period. See the **tacacs-server ip_address port** command.

Related Commands

show tacacs-server

(config) tcp-ip-fragment-enabled

To allow a CSS to flow-process TCP IP fragments, use the **tcp-ip-fragments-enabled** command. When a CSS flow-processes IP fragments, it has the potential to match the fragmented packets to content rules and source groups for intelligent routing and load balancing. This command is disabled by default. Use the **no** form of this command to reset the default behavior of the CSS to forwarding TCP IP fragments.

```
tcp-ip-fragment-enabled

no tcp-ip-fragment-enabled
```

Command Modes

Global configuration mode

Usage Guidelines

This feature performs content rule-based forwarding using the Layer 3 (IP address) and Layer 4 (TCP port) information in the IP header and the TCP header. Layer 5 forwarding decisions for IP fragments, based on the packet payload (data), are not supported. For more information, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

show ip-fragment-stats
zero ip-fragment-stats
(config) ip-fragment max-assembled-size
(config) udp-ip-fragment-enabled

(config) udp-ip-fragment-enabled

To allow a CSS to flow-process UDP IP fragments, use the **ip-udp-fragment-enabled** command. When a CSS flow-processes IP fragments, it has the potential to match the fragmented packets to content rules and source groups for intelligent routing and load balancing. This command is disabled by default. Use the **no** form of this command to reset the default behavior of the CSS to forwarding UDP IP fragments.

udp-ip-fragment-enabled

no udp-ip-fragment-enabled

Command Modes

Global configuration mode

Usage Guidelines

This feature performs content rule-based forwarding using the Layer 3 (IP address) and Layer 4 (UDP port) information in the IP header and the UDP header. Layer 5 forwarding decisions for IP fragments, based on the packet payload (data), are not supported. For more information refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

show ip-fragment-stats
zero ip-fragment-stats
(config) ip-fragment max-assembled-size
(config) tcp-ip-fragment-enabled

(config) urql

To access Uniform Resource Locator qualifier list (URQL) configuration mode and configure a URQL, use the **urql** command. Use the **no** form of this command to an existing URQL.

urql *urql_name*

no urql *existing_urql_name*

Syntax Description

urql_name	Name of a new URQL you want to create or of an existing list. Enter an unquoted text string with no spaces and a maximum length of 31 characters. To see a list of existing URQL names, enter: `urql ?`

Usage Guidelines

A URQL is a collection of URLs for content requests that you can associate to one or more content rules. The CSS uses this list to identify which requests to send to a service.

You cannot configure a URQL with subscribers services.

You can access this mode from any configuration mode except ACL, boot, group, keepalive, and owner configuration modes. The prompt changes to (config-urql [*name*]). You can also use this command from URQL mode to access another URQL. For information about commands available in this mode, see the "URQL Configuration Mode Commands" section.

(config) username

To configure a local username and its password for logging into the CSS, and allow it to access SuperUser mode, use the **username** command. Use the **no** form of this command to delete an existing username.

username *name* [**password** *password* {**superuser**}{**dir-access** *access*}
|**des-password** *password* {**superuser**}{**dir-access** *access*}]

no username *name*

Syntax Description

name	Username you want to assign or change. Enter an unquoted text string with no spaces and a maximum of 16 characters. To see a list of existing usernames, enter: `username ?`
password	Password. Enter an unquoted text string with no spaces and a length of 6 to 16 characters. A DES password can have a length of 6 to 64 characters. When you enter a password with the **des-password** keyword, the CSS encrypts the password. Use the **show running-config** command to view the encrypted password in the running configuration. You must use the encrypted form of the password to log in to the CSS.
superuser	(Optional) Allows this user to access SuperUser mode. If you do not enter this option, the user can only access User mode.
password	Specifies that the password is not encrypted. Use this keyword when you dynamically use the CLI to create new users.
des-password	Specifies that the password is Data Encryption Standard (DES) encrypted. Use this keyword only when you are creating a file for use as a script or a startup configuration file.

dir-access	(Optional) Defines the CSS directory access levels. By default, the CSS assigns users with read and write access to the directories. Changing the access level also affects the use of the CLI commands associated with the directories.
access	(Optional) The access levels for the CSS script, log, root, archive, release root, core, and MIB directories, in this order. Sequentially enter one of the following levels for each of the directories: • **N** - No access to the directory • **B** - Read and write access • **W** - Write access • **R** - Read access For example, to allow no access for the root and release root directories but read and write access for all other directories, enter BBNBNBB. Note that the release root directory contains the configuration files. The root directory contains the installed CSS software.

Usage Guidelines

If the **(config) restrict user-database** command is entered, only a user with administrative or technician privileges can use the **username** command.

The CSS can support a maximum of 32 usernames including the administrator and technician usernames. It ships with a default username of **admin** and password of **system**.

You cannot permanently delete an administrative username and password. If you delete this username by using the **no username** command, it removes it from use until you reboot the CSS. When you reboot the CSS, it restores the username and password from NVRAM.

Related Commands

show running-config
show user-database
(config) restrict

(config) username-offdm

To change the administrative username and password without having to use the Offline DM menu, use the **username-offdm** command. The CSS ships with a default administrative username of **admin** and password of **system**.

username-offdm *name* **password** *password*

Syntax Description

name	Username you want to assign as the administrative username. Enter an unquoted text string with no spaces and a maximum of 16 characters. The CSS does not allow you to set the administrative username to the same name as the technician username.
password	Password. Enter an unquoted text string with no spaces and a length of 6 to 16 characters.

Usage Guidelines

Unlike other usernames and passwords, the CSS saves the administrative username and password in nonvolatile RAM (NVRAM). When you reboot the CSS, it reads the username and password from NVRAM and reinserts them into the user database.

Note You cannot permanently delete an administrative username and password. If you delete the username by using the **no username** command, it removes it from use until you reboot the CSS. When you reboot the CSS, it restores the username and password from NVRAM.

(config) username-technician

Caution This command is for use by technical personnel only. The technician user is created primarily for CSS troubleshooting and should not be used to perform normal CSS administrative purposes.

A technician user has access to all directories in the WebNS directory structure in the CSS. This user can remove or copy valuable system files (including encrypted certificates or keys in an CSS 11503 or 11506 containing an SSL module). The removing of system files could make the CSS unusable.

To set the technician username and password without having to use the Technician Offline DM menu, use the **username-technician** command.

username-technician *name* **password** *password*

Syntax Description

name	Username you want to assign as the technician username. Enter an unquoted text string with no spaces and a maximum of 16 characters. The CSS does not allow you to set the technician username to the same name as the administrative username.
password	Password. Enter an unquoted text string with no spaces and a length of 6 to 16 characters.

(config) virtual authentication

To configure the primary, secondary, or tertiary virtual authentication on the CSS, use the **virtual authentication** command. Use this command to require users to enter a username and password to remotely log in to the CSS.

virtual authentication [**primary**|**secondary**|**tertiary**
[**local**|**radius**|**tacacs**|**disallowed**]]

Syntax Description

primary	Defines the first authentication method that the CSS uses. The default primary virtual authentication method is the local user database.
secondary	Defines the second authentication method that the CSS uses if the first method fails. The default secondary virtual authentication method disallows all user access. If you are configuring a TACACS+ server as the primary authentication method, define a secondary authentication method, such as **local**.
tertiary	Defines the third authentication method that the CSS uses if the second method fails. The default tertiary virtual authentication method disallows all user access.
local	The CSS uses the local user database for authentication.
radius	The CSS uses the configured RADIUS server for authentication.
tacacs	The CSS uses the configured TACACS+ server for authentication.
disallowed	The CSS does not allow access by all remote users. Entering this option does not terminate existing connections. To remove users currently logged into the CSS, use the **disconnect** command.

Usage Guidelines

Virtual authentication allows remote users to log into the CSS through FTP or Telnet with or without requiring a username and password. The CSS can also deny access to all remote users.

You can configure the CSS to authenticate users by using the local database, RADIUS server, or TACACS+ server. By default, the CSS uses the local database as the primary method to authenticate users and disallows user access for the secondary and tertiary method.

Before you can use RADIUS or TACACS+ as the virtual authentication method, you must enable communication with the RADIUS or TACACS+ security server. Use either the **(config) radius-server** command or the **(config) tacacs-server** command.

Related Commands

show user-database
(config) console authentication
(config) radius-server
(config) restrict
(config) tacacs-server

(config) vrrp-backup-timer

To specify the time interval in seconds that the backup CSS waits to assume mastership when the master CSS goes down, use the **vrrp-backup-timer** command. Use the **no** form of this command to reset the timer to the default value of 3 seconds.

vrrp-backup-timer *wait_time*

no vrrp-backup-timer

Syntax Description

wait_time	Interval in seconds. Enter an integer from 3 to 120 seconds. The default is 3 seconds.

Usage Guidelines

Timer values greater than the 3-second default cause longer failover times. Use the **vrrp-backup-timer** command only in environments where the CPU utilization on the CSS is close to 100 percent.

After you set the timer value, you need to reenter the **(config-circuit-ip) redundancy-protocol** command on the redundant circuit between the CSSs for the new timer value to take effect.

Note If you intend to use the commit_redundancy script to synchronize your redundant configuration, be sure to specify the **-a** argument in the **script play** command to ensure that the script copies the timer configuration setting from the master CSS to the backup CSS.

Related Commands

script play
(config-circuit-ip) redundancy-protocol

(config) web-mgmt state

To allow or deny client access to the XML HTTP server running on the CSS, use the **web-mgmt state** command.

web-mgmt state [**disable**|**enable**]

Syntax Description

disable	Denies client access to the HTTP server on the CSS. Performs the same function as the **restrict xml** command.
enable	Allows client access to the HTTP server on the CSS. Performs the same function as the **no restrict xml** command.

Usage Guidelines

The **web-mgmt state** command performs the same function as the **(config) restrict xml** command and its **no** form of the command. Note that when you use this command, it does not appear in the configuration file. Instead, the **(config) restrict** or its **no** form of the command appears in the configuration file.

When XML is enabled, the CSS listens for XML connections on port 80.

Related Commands

(config) restrict

(config) zero flow-state-counters

To reset all the hit counters in the flow state table to zero, use the **zero flow-state-counters** command. The flow state table contains hit counters that total the number of hits for each port entry in the table.

zero flow-state-counters

Related Commands

(config) flow-state
show flow-state-table

ACL Configuration Mode Commands

ACL configuration mode allows you to configure an access control list (ACL) on the CSS. ACLs provide a basic level of security for accessing your network. Through ACL clauses that you define, the CSS determines how to handle each packet it processes. When the CSS examines each packet, it either forwards or blocks the packet based on whether the packet matches a clause in the ACL.

To access ACL mode, use the **acl** command from any configuration mode, except boot, and RMON alarm, event, and history modes. The prompt changes to (config-acl [*index*]). You can use this command from ACL mode to access another ACL. For information about commands available in this mode, see the following commands.

Use the **no** form of this command to delete an ACL.

acl *index*

no acl *index*

Syntax Description

index	Number you want to assign to a new ACL or the number for an existing ACL. Enter a number from 1 to 99.

Usage Guidelines

If you do not configure ACLs on the CSS, all packets passing through the CSS could be allowed onto the entire network. For example, you may want to permit all e-mail traffic, but block Telnet traffic. You can also use ACLs to allow one client to access a part of the network and prevent another client from accessing the same area.

ACLs function as a firewall security feature. When you enable ACLs, all traffic not configured in an ACL permit clause *will be denied*. It is extremely important that you first configure an ACL to permit traffic *before you enable ACLs*. If you do not permit any traffic, you will lose network connectivity. Note that the console port is not affected.

We recommend that you configure either a permit all or a deny all clause depending on your ACL configuration. For example, you could first configure a permit all clause and then configure deny clauses for only the traffic you wish to deny. You could also use the default deny all clause and configure permit clauses only for the traffic you wish to permit.

(config-acl) apply

To assign an ACL to an individual circuit, all circuits without ACLs or DNS queries, use the **apply** command.

apply [**all**|**circuit-(***circuit_name***)**|**dns**]

Syntax Description

all	Applies this ACL to all existing circuits without ACLs or reapply the ACL to circuits that currently have the same ACL applied. If a circuit has a different ACL applied, this keyword bypasses the circuit.
circuit-(*circuit_name***)**	Applies this ACL to an individual circuit. Enter the name of the circuit. To see a list of existing circuits, enter: `apply ?`
dns	Adds this ACL to DNS queries.

Usage Guidelines

To add a new clause to an existing and applied ACL, reapply the ACL to the circuit with the **apply circuit** command.

To apply any changes to an existing clause on an existing and applied ACL, you must remove the ACL from the circuit with the **(config-acl) remove** command, and then reapply the ACL to the circuit.

To remove a clause currently in use, you must remove its applied ACL from the circuit, delete the clause, and then reapply the ACL to the circuit.

Note You cannot apply an ACL that has no clauses.

Note If you configure a CSS with the **dns-server** command, and the CSS receives a DNS query for a domain name that you configured on the CSS using the **host** command, the DNS query *will not* match on an ACL that is configured with the **apply dns** command.

However, if you configure a domain name on a content rule on a CSS using the **add dns** *domain_ name* command, a DNS query for that domain name *will* match on an ACL that is configured with the **apply dns** command.

Related Commands

(config-acl) remove

(config-acl) clause

To enter clauses in a specific ACL to control incoming traffic on a circuit and to control logging on the clause, use the **clause** command. Use the **no** form of this command to delete a clause.

clause *number* [**log** [**enable**|**disable**]]|[**bypass**|**deny**|**permit**] *protocol* [*source_info* {*source_port*}] **destination** [*dest_info* {*dest_port*}] {**sourcegroup** *name*} {**prefer** *name*}]

no clause number

Syntax Description

log disable	Disables ACL logging.
log enable	Enables ACL logging.
bypass	Sends traffic directly to its destination, bypassing the content rule.
deny	Denies traffic on a circuit.
permit	Permits traffic on a circuit.
number	Number you want to assign to the clause. Enter a number from 1 to 254.

protocol	Protocol for the type of traffic. Enter **TCP**, **UDP**, **ICMP**, **IGP**, **IGMP**, **OSPF**, **any** for any protocol, or the number associated with the protocol.
source_info	Source of the traffic. Enter one of the following: • **any** for any combination of source IP address and host name information. • *host_name* for the source host name. Enter a host name in mnemonic host-name format (for example, myhost.mydomain.com). • *ip_address* {*mask_ip_address*} for the source IP address and the optional mask IP address. Enter an IP address in dotted decimal notation (for example, 192.168.11.1). • **nql** *nql* for an existing NQL consisting of a list of IP addresses. Enter the name of the NQL. To see a list of NQLs, enter: `show nql`
source_port	(Optional) Source port for the traffic. Enter either: • [**eq**|**lt**|**gt**|**neq**] *number* where: – **eq** is equal to the port number. – **lt** is less than the port number. – **gt** is greater the port number. – **neq** is not equal to the port number. – *number* is the source port number. Enter a number from 1 to 65535. • **range** *low high* for a range of port numbers, inclusive. Enter numbers from a range of 1 to 65535. Separate the *low* and *high* number with a space. If you do not designate a source port, this clause allows traffic from any port number.

dest_info

Destination information for the traffic. Enter one of the following:

- **any** for any combination of destination information.
- **content** *owner_name/rule_name* for an owner's content rule. Separate the owner and rule name with a / character. To see a list of owners and content rules, enter:

  ```
  content ?
  ```

- *host_name* for the destination host name. Enter a host name in mnemonic host-name format (for example, myhost.mydomain.com).
- *ip_address* {*mask_ip_address*} for the destination IP address and the optional mask IP address. Enter an IP address in dotted decimal notation (for example, 192.168.11.1).
- **nql** *nql* for an existing NQL consisting of host IP addresses. Enter the name of the NQL. To see a list of NQLs, enter:

  ```
  show nql
  ```

dest_port

(Optional) Destination port. Enter one of the following:

- [**eq**|**lt**|**gt**|**neq**] *number* where:

  eq is equal to the port number.

  lt is less than the port number.

  gt is greater the port number.

  neq is not equal to the port number.

  number is the destination port number. Enter a number from 1 to 65535.

- **range** *low high* for a range of port numbers, inclusive. Enter numbers from a range of 1 to 65535. Separate the *low* and *high* number with a space.
- *destport-enum* where you enter one of the following ports: **ftp-data**, **ftp**, **telnet**, **smtp**, **domain**, **gopher**, **http**, **pop**, **nntp, ntp**, **bgp**, **ldap**, **https**.

If you do not designate a destination port, this clause allows traffic to any port number.

sourcegroup *name*

(Optional) Defines a source group based on matching this ACL clause. Enter the group name. To see a list of source groups, enter:

```
show group ?
```

prefer *name*

(Optional) Defines a preferred service or source group based on matching this ACL clause. Enter the service or source group name. To see a list of services, enter:

```
show service summary
```

To see a list of source groups, enter:

```
show group ?
```

You can define two preferred services. Separate each service with a comma (,).

Usage Guidelines

When implementing an ACL, the number assigned to each clause is very important. The CSS looks at the ACL starting from clause 1 and sequentially progresses through the rest of the clauses. Assign the lowest clause numbers to clauses with the most specific matches. Then, assign higher clause numbers to clauses with less specific matches.

You do not need to enter the clauses sequentially. The CSS automatically inserts the clause in the appropriate order in the ACL. When you can enter clauses 10 and 24, and then clause 15, the CSS inserts the clauses in the right sequence.

Note To add a new clause to an existing and applied ACL, reapply the ACL to the circuit with the **apply circuit** command.

To apply any changes to an existing clause on an existing and applied ACL, you must remove the ACL from the circuit with the **(config-acl) remove** command, and then reapply the ACL to the circuit.

To remove a clause currently in use, you must remove its applied ACL from the circuit, delete the clause, and then reapply the ACL to the circuit.

If you did not enable global ACL logging, the **enable** option does not work. To enable global ACL logging, use the **(config) logging subsystem acl level debug-7** command.

The **bypass** option bypasses traffic only on a content rule, thus does not cause NATing to occur. Do not use the **bypass** option in an ACL clause with a source group. Since this option does not bypass traffic that does not match a rule, it does not effect NATing on a source group in an ACL clause.

Related Commands

show acl
show running-config acl
(config-acl) apply

(config-acl) no

To negate a command or set it to its default in ACL mode, use the **no** command. Not all commands have a **no** form. For information on general **no** commands you can use in this mode, see the general **no** command.

Syntax Description

no acl *number*	Deletes an ACL
no clause *number*	Deletes a clause

(config-acl) remove

To remove the ACL from an individual circuit, all circuits, or DNS queries, use the **remove** command.

remove [**all|circuit-(***circuit_name***)|dns**]

Syntax Description

all	Removes this ACL from all circuits.
circuit-(*circuit_name***)**	Removes this ACL from the circuit. Enter the name of the circuit for the ACL. To see a list of circuits, use the r**emove ?** command.
dns	Removes this ACL from DNS queries.

Related Commands

(config-acl) apply

(config-acl) zero counts

To set the content and DNS hit counters in the **show acl** command screen to zero for this ACL, use the **zero counts** command.

zero counts

Related Commands

show acl

Boot Configuration Mode Commands

Boot configuration mode contains all commands necessary to manage booting the CSS and to maintain the software revision. To access this mode, use the **boot** command from global configuration mode.

(config) **boot**

The prompt changes to (config-boot). For information about commands available in this mode, see the following commands.

(config-boot) gateway address

To configure a management port default gateway to load a boot file on a CSS across different subnets, use the **gateway address** command. To change the IP address, reenter this command. Use the **no** form of this command to disable the default gateway address by setting the IP address to 0.0.0.0.

gateway address *ip_or_host*

no gateway address

Syntax Description

ip_or_host	IP address for the management port gateway. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1) or mnemonic host-name format (for example, myhost.mydomain.com).

Usage Guidelines

If you have a second SCM installed in a CSS 11800, use the **passive gateway address** command to configure the Management Port gateway address on the passive SCM boot-config.

The **gateway address** command has an effect only in an Offline DM boot operation and not in the running-config.

A gateway address of 0.0.0.0 for the Ethernet management port does not appear in the **show boot-config** command output for the CSS boot configuration.

Related Commands

show boot-config
(config-boot) passive

(config-boot) ip address

To configure the system boot IP address, use the **ip address** command. To change the boot IP address, reenter this command.

ip address *ip_or_host*

Syntax Description

ip_or_host	IP address used upon boot. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1) or mnemonic host-name format (for example, myhost.mydomain.com). Do not enter an all zero IP address.

Related Commands

(config-boot) subnet mask

(config-boot) no

To negate a command or set it to its default, use the **no** command. Not all commands have a **no** form. For information on general **no** commands you can use in this mode, see the general **no** command.

Syntax Description

no gateway address	Disables the default gateway address by setting the IP address to 0.0.0.0
no passive primary boot-file	Removes the primary boot file from the passive SCM
no passive primary boot-type	Removes the primary boot type from the passive SCM
no passive secondary boot-file	Removes the secondary boot file from the passive SCM

no passive secondary boot-type	Removes the secondary boot type from the passive SCM
no primary boot-file	Removes the primary boot file
no primary boot-type	Removes the primary boot type
no primary config-path	Removes the primary network configuration path
no secondary boot-file	Removes the secondary boot file
no secondary boot-type	Removes the secondary boot type
no secondary config-path	Removes the secondary network configuration path

(config-boot) passive

To configure the boot configuration record for the current passive SCM, use the **passive** command. The boot configuration record consists of the IP address, subnet mask, boot method, and boot file.

The options for this boot mode command are:

- **passive gateway address** - Configures a management port default gateway to load a boot file on a CSS across different subnets for the passive SCM.
- **passive ip address** - Configures the system boot IP address for the passive SCM.
- **passive primary boot-file** - Specifies the primary boot file for the passive SCM.
- **passive primary boot-type** - Specifies the primary boot method, local disk, FTP, or network-mounted file system via FTP, for the passive SCM.
- **passive primary config-path** - Specifies the primary alternate path to a network CSS configuration for the passive SCM.
- **passive secondary boot-file** - Specifies the secondary boot file for the passive SCM.
- **passive secondary boot-type** - Specifies the secondary boot method, local disk, FTP, or network-mounted file system via FTP, for the passive SCM.

- **passive secondary config-path** - Specifies the secondary alternate path to a network CSS configuration for the passive SCM.
- **passive subnet mask** - Configures the system boot subnet mask for the passive SCM.
- **passive sync** - Copies the boot configuration record from the active SCM to the passive SCM. For the CSS 11506, the **passive sync** command also copies the start configuration and the clock time from the active SCM to the passive SCM.

Usage Guidelines

The **passive** command also allows you to configure the individual components of the boot configuration record on the passive SCM. For example, you can configure a boot record on the passive SCM that has a software version that differs from the active SCM. This allows you to run a new software version on the active SCM with the security of having an older software version on the passive SCM.

You can also configure a different IP address on the passive SCM to track an active-to-passive state transition between the SCMs. You can accomplish this through a management station where you can receive SNMP host traps.

Note The **passive** command and its options only affect the current passive SCM. When you configure the passive SCM, the set values are loaded into its nonvolatile RAM. If the passive SCM transitions to the active state, it continues to retain these values but is no longer affected by these commands; **boot** commands are not saved in the running-config.

For more information on the **passive** command options and associated variables, see the following commands.

passive gateway address

To configure a management port default gateway to load a boot file on a CSS across different subnets for the passive SCM, use the **passive gateway address** command. To change the IP address, reenter this command.

passive gateway address *ip_or_host*

Syntax Description

ip_or_host	IP address for the management port gateway. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1) or mnemonic host-name format (for example, myhost.mydomain.com). Do not enter an all zero IP address.

Related Commands

(config-boot) gateway address

passive ip address

To configure the system boot IP address for the passive SCM, use the **passive ip address** command. To change the boot IP address, reenter this command.

passive ip address *ip_or_host*

Syntax Description

ip_or_host	IP address for the passive SCM used upon boot. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1) or mnemonic host-name format (for example, myhost.mydomain.com). Do not enter an all zero IP address.

Command Modes

Boot

passive primary boot-file

To specify the primary boot image for the passive SCM, use the **passive primary boot-file** command. Use the **no** form of this command to remove the primary boot file from the passive SCM.

passive primary boot-file *filename*

no passive primary boot-file

Syntax Description

filename	Filename of the primary boot image for the passive SCM. Enter an unquoted text string with no spaces and a maximum length of 64 characters. To see a list of boot filenames, enter: `passive primary boot-file ?`

Command Modes

Boot

passive primary boot-type

To specify the primary boot method for the passive SCM, use the **passive primary boot-type** command. The method is from either the CSS software on the CSS disk or a network-mounted file system, or to install the CSS software from an FTP server onto the CSS disk and then boot the CSS from the drive. Use the **no** form of this command to remove the primary boot type from the passive SCM.

passive primary boot-type [**boot-via-disk**|**boot-via-ftp** *ftp_record*|
boot-via-network *ftp_record*]

no passive primary boot-type

Syntax Description

boot-via-disk	Boots the CSS from its disk.
boot-via-ftp	Installs the CSS software on the CSS disk and boots the CSS. The CSS accesses an .ADI or GZIP file containing the CSS software from an FTP server, copies it to its disk, and unpacks it. Then the CSS boots from the disk.
ftp_record	Name of the FTP record file that contains the IP address, username, and password for the FTP server. Enter an unquoted text string with no spaces.
boot-via-network	Boots the system from a network-mounted file system via FTP. Instead of the CSS disk, the network file system contains the CSS software. The CSS boots from this file system and loads the configuration into memory.

Command Modes

Boot

Usage Guidelines

Be aware of the following network boot restrictions:

- A network boot is not supported on UNIX workstations.
- The War-FTP daemon is not supported for network-booting the system software.

A network boot requires that the CSS contains an operational disk.

passive primary config-path

To specify the alternate path to a network configuration for the network boot method for the passive SCM, use the **passive primary config-path** command. An alternate configuration path allows multiple CSSs to use the same boot image while keeping their configuration information in separate directories. Use the **no** form of this command to remove the primary network configuration path.

passive primary config-path *path*

no passive primary config-path

Syntax Description

path	Path to use for network configuration. Enter an unquoted text string with no spaces and a maximum length of 64 characters.

Command Modes

Boot

Usage Guidelines

When using an alternate configuration path, make sure that the path leads to a directory containing the script, log and info subdirectories, and the startup-config file. These subdirectories must contain the files in the corresponding subdirectories in the unZipped boot image. Create these subdirectories. Then copy the files from the boot image.

Note The CSS must be able to access the configuration path through an FTP server as defined through the FTP record for the network boot method.

passive secondary boot-file

To specify the secondary boot image for the passive SCM, use the **passive secondary boot-file** command. Use the **no** form of this command to remove the secondary boot file from the passive SCM.

passive secondary boot-file *filename*

no passive secondary boot-file

Syntax Description

filename	Filename of the primary boot image. Enter an unquoted text string with no spaces and a maximum length of 64 characters. To see a list of boot filenames, enter: `passive primary boot-file ?`

Command Modes

Boot

passive secondary boot-type

To specify the secondary boot method for the passive SCM, use the **passive secondary boot-type** command. The method is from either the CSS software on the CSS disk or a network-mounted file system, or to install the CSS software from an FTP server onto the CSS disk and then boot the CSS from the drive. Use the **no** form of this command to remove the secondary boot type from the passive SCM.

passive secondary boot-type [**boot-via-disk**|**boot-via-ftp** *ftp_record*|**boot-via-network** *ftp_record*]

no passive secondary boot-type

Syntax Description

boot-via-disk	Boots the CSS from its disk.
boot-via-ftp	Installs the CSS software on the CSS disk and boots the CSS. The CSS accesses an .ADI or GZIP file containing the CSS software from an FTP server, copies it to its disk, and unpacks it. Then the CSS boots from the disk.
ftp_record	Name of the FTP record file that contains the IP address, username, and password for the FTP server. Enter an unquoted text string with no spaces.
boot-via-network	Boots the system from a network-mounted file system via FTP. Instead of the CSS disk, the network file system contains the CSS software. The CSS boots from this file system and loads the configuration into memory.

Command Modes

Boot

Usage Guidelines

Be aware of the following network boot restrictions:

- A network boot is not supported on UNIX workstations.
- The War-FTP daemon is not supported for network-booting the system software.

A network boot requires that the CSS contains an operational disk.

passive secondary config-path

To specify the secondary alternate path to a network configuration for the network boot method for the passive SCM, use the **passive secondary config-path** command. Use the **no** form of this command to remove the secondary network configuration path.

passive secondary config-path *path*

no passive secondary config-path

Syntax Description

path	Path to use for network configuration. Enter an unquoted text string with no spaces and a maximum length of 64 characters.

Command Modes

Boot

Usage Guidelines

An alternate configuration path allows multiple CSSs to use the same boot image while keeping their configuration information in separate directories.

Note The CSS must be able to access the configuration path through an FTP server as defined through the FTP record for the network boot method.

When using an alternate configuration path, make sure that the path leads to a directory containing the script, log and info subdirectories, and the startup-config file. These subdirectories must contain the files in the corresponding subdirectories in the unZipped boot image. Create these subdirectories. Then copy the files from the boot image.

passive subnet mask

To configure the system boot subnet mask for the passive SCM, use the **passive subnet mask** command.

passive subnet mask *mask*

Syntax Description

mask	Subnet mask used at boot. Enter the mask in dotted-decimal notation (for example, 255.255.255.0).

Command Modes

Boot

passive sync

To copy the primary and secondary boot configuration record from the nonvolatile RAM (NVRAM) of the active Switch Control Module (SCM) to its passive SCM backup, use the **passive sync** command. For the CSS 11506, the **passive sync** command also copies the boot configuration, boot image, startup configuration, or the clock time from the active SCM to the passive SCM.

passive sync {**boot-config**|**image**|**startup-config**|**time**}

Syntax Description

boot-config	Copies the boot configuration record from the active SCM to the passive SCM (CSS 11506 only).
image	Copies the boot image and local startup configuration file from the active SCM to the passive SCM (CSS 11506 only).
startup-config	Copies the startup configuration file and archive directory from the active SCM to the passive SCM (CSS 11506 only).
time	Synchronizes the clock time of the passive SCM with the active SCM (CSS 11506 only).

Command Modes

Boot

Related Commands

show chassis

(config-boot) primary

To specify the primary boot configuration, use the **primary** command. The options for this boot mode command are:

- **primary boot-file** - Specifies the primary boot file
- **primary boot-type** - Specifies the primary boot method, local disk, via FTP, or a network-mounted file system via FTP
- **primary config-path** - Specifies the alternate path to a network CSS configuration

For more information on these options and associated variables, see the following commands.

Related Commands

(config) ftp-record
(config-boot) secondary

primary boot-file

To specify the primary boot image, use the **primary boot-file** command. Use the **no** form of this command to remove the primary boot file.

primary boot-file *filename*

no primary boot-file

Syntax Description

filename	Filename of the primary boot image. Enter an unquoted text string with no spaces and a maximum length of 64 characters. To see a list of boot filenames, enter: `primary boot-file ?`

Command Modes

Boot

primary boot-type

To specify the primary boot method, use the **primary boot-type** command. The method is from either the CSS software on the CSS disk or a network-mounted file system, or to install the CSS software from an FTP server onto the CSS disk and then boot the CSS from the drive. Use the **no** form of this command to remove the primary boot type.

primary boot-type [**boot-via-disk**|**boot-via-ftp** *ftp_record*|
boot-via-network *ftp_record*]

no primary boot-type

Syntax Description

boot-via-disk	Boots the CSS from its disk.
boot-via-ftp	Installs the CSS software on the CSS disk and boots the CSS. The CSS accesses an .ADI or GZIP file containing the CSS software from an FTP server, copies it to its disk, and unpacks it. Then the CSS boots from the disk.
ftp_record	Name of the FTP record file that contains the IP address, username, and password for the FTP server. Enter an unquoted text string with no spaces.
boot-via-network	Boots the system from a network-mounted file system via FTP. Instead of the CSS disk, the network file system contains the CSS software. The CSS boots from this file system and loads the configuration into memory.

Command Modes

Boot

Usage Guidelines

Be aware of the following network boot restrictions:

- A network boot is not supported on UNIX workstations.
- The War-FTP daemon is not supported for network-booting the system software.

A network boot requires that the CSS contains an operational disk.

primary config-path

To specify the alternate path to a network configuration for the network boot method, use the **primary config-path** command. Use the **no** form of this command to remove the primary network configuration path.

primary config-path *path*

no primary config-path

Syntax Description

path	Path to use for network configuration. Enter an unquoted text string with no spaces and a maximum length of 64 characters.

Command Modes

Boot

Usage Guidelines

An alternate configuration path allows multiple CSSs to use the same boot image while keeping their configuration information in separate directories.

Note The CSS must be able to access the configuration path through an FTP server as defined through the FTP record for the network boot method.

When using an alternate configuration path, make sure that the path leads to a directory containing the script, log and info subdirectories, and the startup-config file. These subdirectories must contain the files in the corresponding subdirectories in the unZipped boot image. Create these subdirectories. Then copy the files from the boot image.

(config-boot) reboot

To reboot the CSS, use the **reboot** command.

reboot

Usage Guidelines

Before you enter the **reboot** command, save an existing running-config file prior to rebooting the CSS by using the **copy running-config startup-config** command from SuperUser mode. If you are not in expert mode, the CSS displays the prompts to save profile and configuration changes before it reboots.

The CSS displays a prompt to verify that you want to reboot it:

```
Are you sure you want to reboot the system, [y/n]
```

Enter **y** to reboot the CSS.

The CSS has a reboot alias that allows you to reboot it from any mode except User mode. When you issue the reboot alias, the CSS changes the current mode to Boot mode and then executes the **reboot** command.

You must enter the entire reboot alias name to execute it. The CSS does not automatically complete the reboot alias when you enter only part of its name. For example, if you enter **reb** in global configuration mode, the CSS displays an invalid command message.

(config-boot) remove

To remove an ArrowPoint Distribution Image (ADI) file from the CSS or a version of CSS software that is currently not running on the CSS, use the **remove** command.

remove {*disk_slot*} *software*

Syntax Description

disk_slot	(Optional) Slot location of the disk in a CSS. The valid entries are: • **0** for the disk in slot 0 • **1** for the disk in slot 1
software	Filename of the ADI or the version of software installed on the CSS. Enter an unquoted text string with a maximum length of 32 characters. To see a list of CSS software versions and ADI files on the CSS, enter: `remove ?`

Related Commands

(config-boot) unpack

(config-boot) secondary

To specify the secondary boot configuration, use the **secondary** command. The secondary boot configuration is used when the primary configuration fails. The options for this boot mode command are:

- **secondary boot-file** - Specifies the secondary boot file
- **secondary boot-type** - Specifies the boot method, local disk or FTP
- **secondary config-path** - Specifies the path to a network configuration via FTP

For more information on these options and associated variables, see the following commands.

Related Commands

(config) ftp-record
(config-boot) primary

secondary boot-file

To specify the secondary boot image, use the **secondary boot-file** command. Use the **no** form of this command to remove the secondary boot file.

secondary boot-file *filename*

no secondary boot-file

Syntax Description

filename	Filename of the primary boot image. Enter an unquoted text string with no spaces and a maximum length of 64 characters. To see a list of boot filenames, enter: `secondary boot-file ?`

Command Modes

Boot

secondary boot-type

To specify the secondary boot method, use the **secondary boot-type** command. The method is either from the CSS software on the CSS disk or a network-mounted file system, or to install the CSS software from an FTP server onto the CSS disk and then boot the CSS from the drive. Use the **no** form of this command to remove the secondary boot type.

secondary boot-type [**boot-via-disk**|**boot-via-ftp** *ftp_record* |**boot-via-network** *ftp_record*]

no secondary boot-type

Syntax Description

boot-via-disk	Boots the CSS from its disk.
boot-via-ftp	Installs the CSS software on the CSS disk and boots the CSS. The CSS accesses an .ADI or GZIP file containing the CSS software from an FTP server, copies it to its disk, and unpacks it. Then the CSS boots from the disk.
ftp_record	Name of the FTP record file that contains the IP address, username, and password for the FTP server. Enter an unquoted text string with no spaces.
boot-via-network	Boots the CSS from a network-mounted file system on via FTP. Instead of the CSS disk, the network file system contains the CSS software. The CSS boots from this file system and loads the configuration into memory.

Command Modes

Boot

Usage Guidelines

Be aware of the following network boot restrictions:

- A network boot is not supported on UNIX workstations.
- The War-FTP daemon is not supported for network-booting the system software.

A network boot requires that the CSS contains an operational disk.

secondary config-path

To specify the alternate path to a network configuration for the network boot method, use the **secondary config-path** command. Use the **no** form of this command to remove the secondary network configuration path.

secondary config-path *path*

no secondary config-path

Syntax Description

path	Path to use for network configuration. Enter an unquoted text string with no spaces and a maximum length of 64 characters.

Command Modes

Boot

Usage Guidelines

An alternate configuration path allows multiple CSSs to use the same boot image while keeping their configuration information in separate directories.

Note The CSS must be able to access the configuration path through an FTP server as defined through the FTP record for the network boot method.

When using an alternate configuration path, make sure that the path leads to a directory containing the script, log and info subdirectories, and the startup-config file. Create these subdirectories. These subdirectories must contain the files in the corresponding subdirectories in the unZipped boot image. Copy the files from the boot image.

(config-boot) shutdown

To shut down the CSS, use the **shutdown** command.

shutdown

Usage Guidelines

The CSS displays a prompt to verify that you want to shut it down:

```
Are you sure you want to shutdown the system, [y/n]:
```

Enter **y** to shut down the CSS.

The CSS has a shutdown alias that allows you to shut it down from any mode except User mode. When you issue the shutdown alias, the CSS changes the current mode to Boot mode and then executes the **shutdown** command.

You must enter the entire shutdown alias name to execute it. The CSS does not automatically complete the shutdown alias when you enter only part of its name. For example, if you enter **shutd** in global configuration mode, the CSS displays an invalid command message.

(config-boot) subnet mask

To configure the system boot subnet mask, use the **subnet mask** command.

subnet mask *mask*

Syntax Description

mask	Subnet mask used at boot. Enter the mask in dotted-decimal notation (for example, 255.255.255.0).

Related Commands

(config-boot) ip address

(config-boot) unpack

To unpack the ArrowPoint Distribution Image (ADI), use the **unpack** command.

unpack *install_filename*

Syntax Description

install_filename	Filename of the ADI. Enter an unquoted text string with a maximum length of 32 characters.

Related Commands

(config-boot) remove

Circuit Configuration Mode Commands

Circuit configuration mode allows you to configure a circuit on the CSS. A circuit on the CSS is a logical entity that maps IP interfaces to a logical port or group of logical ports.

To access circuit configuration mode, use the **circuit** command from global, IP, interface, and service. The prompt changes to (config-circuit [*circuit_name*]). You can also use this command from circuit mode to access another circuit. For information about commands available in this mode, see the following commands.

circuit *circuit_name*

Syntax Description

circuit_name	Name of the circuit you want to configure. To see a list of available circuits, enter: `circuit ?`

(config-circuit) description

To specify the description for the circuit, use the **description** command. Use the **no** form of this command to delete the circuit description.

description "*circuit_description***"**

no description

Syntax Description

"*circuit_description*"	Description for the circuit. Enter a quoted text string with a maximum length of 32 characters.

Related Commands **show circuits**

(config-circuit) dhcp relay-to

To specify the DHCP relay destination address to the DHCP server, use the **dhcp relay-to** command. Use the **no** form of this command to remove the relay destination address.

dhcp relay-to *ip_address*

no dhcp relay-to *ip_address*

Syntax Description

ip_address	IP address for the DHCP relay destination. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1).

Usage Guidelines

You can configure a maximum of five DHCP relay destination addresses per circuit.

Do not configure a relay destination on a circuit when the relay destination is directly connected to or reachable from one of the ports on the same circuit. In this case, the DHCP packets reach the relay destination through normal broadcast and a relay agent is not required.

Related Commands

show dhcp-relay-agent global
(config-circuit) dhcp-relay-agent

(config-circuit) dhcp-relay-agent

To enable DHCP relay agent on the circuit, use the **dhcp-relay-agent** command. Use the **no** form of this command to disable the DHCP relay agent on the circuit.

dhcp-relay-agent

no dhcp-relay-agent

Related Commands

show dhcp-relay-agent global
(config) dhcp-agent max-hops
(config-circuit) dhcp relay-to

(config-circuit) ip

To enter IP configuration mode and assign a local IP interface address to this circuit, use the **ip** command. Use the **no** form of this command to delete a local IP address from this circuit.

ip address *ip_or_host ip_mask*

no ip address *ip_or_host*

Syntax Description

ip_or_host	IP address or host name you want to assign to the circuit. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or a host name in mnemonic form (for example, myhost.mydomain.com).
ip_mask	IP mask. Enter the mask as either: • A prefix length in CIDR bitcount notation (for example, /24). The valid prefix length range is from 8 to 31. Do not enter a space to separate the IP address from the prefix length. • A subnet mask in dotted-decimal notation (for example, 255.255.255.0).

Usage Guidelines

When you use the **ip** command to access IP configuration mode, the prompt changes to (config-circuit-ip [*circuit_name*-*ipaddress*]). For information about commands available in this mode, see the "IP Configuration Mode Commands" section.

Related Commands

show ip interfaces

(config-circuit) no

To negate a command or set it to its default, use the **no** command. For information on general **no** commands you can use in this mode, see the general **no** command. The following options are available in circuit mode.

Syntax Description

no acl *index*	Deletes an ACL
no description	Deletes the circuit description
no dhcp relay-to *ip_address*	Removes the DHCP relay destination address from the circuit
no dhcp-relay-agent	Disables the DHCP relay agent on the circuit
no ip address *ip_or_host*	Removes a local IP address from the circuit
no keepalive *name*	Deletes an existing keepalive
no owner *existing_owner_name*	Deletes an existing owner
no redundancy	Removes this circuit from the redundancy configuration
no router-discovery lifetime	Resets the maximum time for the hosts to remember the router advertisements to the default of 3 x *the maximum advertisement value*
no router-discovery limited-broadcast	Transmits router discovery packets using the default of 224.0.0.1
no router-discovery max-advertisement-interval	Resets the maximum router advertisement interval to the default of 600

no router-discovery min-advertisement-interval	Resets the minimum router advertisement interval to the default of 0.75 x *the maximum advertisement value*

(config-circuit) redundancy

To configure the circuit as a redundant circuit, use the **redundancy** command. Use the **no** form of this command to remove a circuit.

redundancy

no redundancy

Related Commands

(config) ip redundancy
(config-circuit-ip) redundancy-protocol

(config-circuit) router-discovery

To configure router discovery advertisements, use the **router-discovery** command. The options for this circuit mode command are:

- **router-discovery lifetime** - Sets the maximum amount of time for the hosts to remember router advertisements
- **router-discovery limited-broadcast** - Transmits router advertisements to 255.255.255.255
- **router-discovery max-advertisement-interval** - Configures the maximum router advertisement interval
- **router-discovery min-advertisement-interval** - Configures the minimum router advertisement interval

For more information on these options and associated variables, see the following commands.

Related Commands

(config-circuit-ip) router-discovery

router-discovery lifetime

To set the maximum amount of time for the hosts to remember router advertisements, use the **router-discovery lifetime** command. Use the **no** form of this command to set the time to the default of three times *the maximum advertisement value*.

router-discovery lifetime *time*

no router-discovery lifetime

Syntax Description

time	Time in seconds. Enter an integer from 0 to 9000. The default is three times *the maximum advertisement value*. Use the **router-discovery max-advertisement-interval** command to set the maximum advertisement value.

Command Modes

Circuit

router-discovery limited-broadcast

To transmit router advertisements to 255.255.255.255, use the **router-discovery limited-broadcast** command. Use the **no** form of this command to transmit router advertisements to the default of 224.0.0.1.

router-discovery limited-broadcast

no router-discovery limited-broadcast

Command Modes

Circuit

router-discovery max-advertisement-interval

To configure the maximum router advertisement interval, use the **router-discovery max-advertisement-interval** command. Use the **no** form of this command to reset the maximum router advertisement interval to the default of 600.

router-discovery max-advertisement-interval *max_value*

no router-discovery max-advertisement-interval

Syntax Description

max_value	Maximum interval between advertisements in seconds. Enter an integer from 4 to 1800. The default is 600 (10 minutes).

Command Modes

Circuit

router-discovery min-advertisement-interval

To configure the minimum router advertisement interval, use the **router-discovery min-advertisement-interval** command. Use the **no** form of this command to reset the minimum router advertisement interval to the default of 0.75 x *the maximum advertisement value*.

router-discovery min-advertisement-interval *min_value*

no router-discovery min-advertisement-interval

Syntax Description

min_value	Minimum interval between advertisements in seconds. Enter an integer from 0 to 1800. The default is 0.75 x *the maximum advertisement value*. If this argument is greater than 0, it must be less than the maximum advertisement value. Use the **router-discovery max-advertisement-interval** command to set the maximum advertisement value.

Command Modes Circuit

IP Configuration Mode Commands

IP configuration mode allows you to assign a local IP interface address to this circuit and configure it. To access IP configuration mode, use the **ip** command from circuit configuration mode. The prompt changes to (config-circuit-ip [*circuit_name-ipaddress*]). You can also use this command in IP mode to configure another IP address for this circuit. For information about commands available in this mode, see the following commands.

Use the **no** form of this command to delete a local IP address from the circuit.

(config-circuit) **ip address** *ip_or_host ip_mask*

no ip address *ip_or_host*

Syntax Description

ip_or_host	IP address or host name you want to assign to the circuit. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or a host name in mnemonic form (for example, myhost.mydomain.com).
ip_mask	IP mask. Enter the mask as either: • A prefix length in CIDR bitcount notation (for example, /24). The valid prefix length range is from 8 to 31. Do not enter a space to separate the IP address from the prefix length. • A subnet mask in dotted-decimal notation (for example, 255.255.255.0).

(config-circuit-ip) broadcast

To change the broadcast address, use the **broadcast** command. The default broadcast address is an all-ones host address (for example, an IP address 192.168.1.1/24 has a broadcast address of 192.168.1.255).

Use the **no** form of this command to reset the broadcast IP address to the default all-ones host address.

broadcast *ip_address*

no broadcast

Syntax Description

ip_address	Broadcast IP address associated with the entry. If left at zero, the all-ones host is used for numbered interfaces. 255.255.255.255 is always used for unnumbered interfaces.

(config-circuit-ip) enable

To enable the IP interface on this circuit, use the **enable** command. This is the default state. Use the **no** form of this command to disable the interface.

enable

no enable

Related Commands

show ip interfaces

(config-circuit-ip) ip

To configure VIP and virtual interface redundancy, use the **ip** command and options. The options for this IP mode command are:

- **ip critical-reporter** - Associates a reporter with a virtual router
- **ip critical-service** - Associates a service with a virtual router
- **ip redundant-interface** - Configures a virtual redundant interface and associate it with a virtual router
- **ip redundant-vip** - Configures a redundant VIP and associates it with a virtual router
- **ip virtual-router** - Configures a virtual router on a CSS

For more information on these options and associated variables, see the following commands.

ip critical-reporter

To associate a reporter with a virtual router, use the **ip critical-reporter** command. Use the **no** form of this command to remove a critical reporter from a virtual router.

ip critical-reporter *vrid reporter_name*

no ip critical-reporter *vrid reporter_name*

Syntax Description

vrid	ID for an existing virtual router.
reporter_name	Name of the reporter. To see a list of reporters, enter: `ip critical-reporter vrid ?`

Command Modes

Circuit-IP

Usage Guidelines

There are three types of critical reporters that you can configure:

- A scripted service, as defined by the **(config-service) keepalive type named** or **(config-service) keepalive type script** command, that is constantly scanning for service and network availability. The keepalive sets the service to a down state whenever network or service availability is a problem. The virtual router goes down if *any* associated scripted service goes down.
- A redundancy uplink critical service, as defined by the **(config-service) type redundancy-up** command. The virtual router goes down when all associated redundancy uplink services go down regardless of any configured keepalive type.

  Note You cannot add redundant uplink services to a content rule.

- Local critical services for any service other than scripted or redundancy uplink, such as a web service. The virtual router goes down when *all* associated local critical services go down.

Note The **show service** command displays the current service type only. It does, however, display the keepalive type, so you can determine from it the behavior of a configured critical service. To display critical service-specific information, use the **show critical-services** command.

Note SNMP values returned for services show the current service type only. To determine the critical service behavior of a particular service, you need to consult the service keepalive type.

Related Commands

show critical-services
(config-circuit-ip) ip virtual-router

ip critical-service

To associate a service to a virtual router, use the **ip critical-service** command. Use the **no** form of this command to remove a critical service from a virtual router.

ip critical-service *vrid service_name*

no ip critical-service *vrid service_name*

Syntax Description

vrid	ID for an existing virtual router.
service_name	Name of the service. To see a list of services, enter: `ip critical-service vrid ?`

Command Modes

Circuit-IP

Usage Guidelines

There are three types of critical services that you can configure:

- A scripted service, as defined by the **(config-service) keepalive type named** or **(config-service) keepalive type script** command, that is constantly scanning for service and network availability. The keepalive sets the service to a down state whenever network or service availability is a problem. The virtual router goes down if *any* associated scripted service goes down.
- A redundancy uplink critical service, as defined by the **(config-service) type redundancy-up** command. The virtual router goes down when all associated redundancy uplink services go down regardless of any configured keepalive type.

Note You cannot add redundant uplink services to a content rule.

- Local critical services for any service other than scripted or redundancy uplink, such as a web service. The virtual router goes down when *all* associated local critical services go down.

Note The **show service** command displays the current service type only. It does, however, display the keepalive type, so you can determine from it the behavior of a configured critical service. To display critical service-specific information, use the **show critical-services** command.

Note SNMP values returned for services show the current service type only. To determine the critical service behavior of a particular service, you need to consult the service keepalive type.

Related Commands

show critical-services
(config-circuit-ip) ip virtual-router

ip redundant-interface

To configure a redundant virtual interface address used for a backend server's default route, use the **ip redundant-interface** command. Use the **no** form of this command to remove an interface from a virtual router.

ip redundant-interface *vrid ip_address*

no ip redundant-interface *vrid ip_address*

Syntax Description

vrid	ID for an existing virtual router.
ip_address	Address for the redundant interface. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1). You cannot use an IP address that already exists for a VIP, redundant VIP, source group, service, log host, or IP interface address on a circuit. If you do, the following error message appears: `Address conflicts with local I/F, VIP, service, or sourcegroup.`

Command Modes

Circuit-IP

Usage Guidelines

Servers use the IP address of the virtual interface as a default route to guarantee packets will be sent to the CSS containing the master virtual router. A redundant interface should be matched with the same virtual router of a VIP that has a rule that references the server. This ensures that the master for a VIP is also the CSS is master for the redundant virtual interface.

Related Commands

show redundant-interfaces
(config-circuit-ip) ip virtual-router

ip redundant-vip

To associate an existing VIP to a virtual router, use the **ip redundant-vip** command. Use the **no** form of this command to remove a VIP from a virtual router.

ip redundant-vip *vrid vip_address* {**range** *number*} {**shared**}

no ip redundant-vip *vrid vip_address*

Syntax Description

vrid	ID for an existing virtual router.
vip_address	Address for the redundant VIP. This address must be already configured in a content rule. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1).
range *number*	(Optional) Defines the IP address range specified in the content rule. You cannot specify a range that differs from the content rule. Also, you cannot specify address ranges to overlap. Enter a number from 0 to 65535.
shared	(Optional) Enables shared VIP redundancy. When you use this option, the master and backup virtual routers share the processing of traffic directed to the VIP, so the backup does not forward packets to the master. Each VIP should be configured identically on each CSS.

Command Modes

Circuit-IP

Usage Guidelines

Before you use the **ip redundant-vip** command, the VIP must be configured in at least one active content rule or source group.

Related Commands

show redundant-vips
(config-circuit-ip) ip virtual-router

ip virtual-router

To create a virtual router on a CSS and configure its identifier and priority used when negotiating control of associated VIPs, use the **ip virtual-router** command. Use the **no** form of this command to remove the virtual router from the CSS.

ip virtual-router *vrid* {**priority** *number*} {**preempt**}

no ip virtual-router *vrid*

Syntax Description

vrid	Virtual router identifier (VRID). Enter an integer between 1 and 255. You can configure 255 virtual routers per VLAN. Virtual routers are considered peers when they have the same VRID and are on the same VLAN.

priority *number*	(Optional) Sets the priority for the virtual router with its peer. The default priority value is 100. Enter an integer between 1 and 255. When the virtual router is the master, it handles the traffic directed to its associated VIPs. To set the virtual router as the master when it becomes alive, set its priority to 255 and configure it with the **preempt** option. You can configure only one virtual router as the master.
preempt	(Optional) Allows a backup virtual router to assert mastership over a lower-priority router. By default, if you create a virtual router, the router does not assert itself as the master even though the current master has a lower priority. For example, if a CSS with a virtual router that has a low priority boots before other CSSs, that router becomes the master. When another CSS with a virtual router that has a higher priority boots, it will not take the mastership from the first router unless you specify the **preempt** option.

Command Modes

Circuit-IP

Usage Guidelines

You must configure the virtual router before you can configure redundant VIPs. A virtual router's role as a master or backup is determined during negotiations between all virtual routers with the same ID and on the same VLAN.

⚠ **Caution** Never configure the **preempt** option on the same virtual router on both CSSs. Such a configuration may result in both CSSs becoming master, which will cause network problems.

Related Commands

show virtual-routers

(config-circuit-ip) no

To negate a command or set it to its default, use the **no** command. For information on general **no** commands you can use in this mode, see the general **no** command. The following options are available in IP mode.

Syntax Description

no acl *number*	Deletes an ACL
no broadcast	Resets the broadcast IP address to the default all-ones host address
no enable	Disables the interface
no ip address *ip_or_host*	Removes a local IP address
no ip critical-service *vrid service_name*	Removes a critical service from a virtual router
no ip redundant-interface *vrid ip_address*	Removes a virtual interface
no ip redundant-vip *vrid vip_address*	Removes a VIP from a virtual router
no ip virtual-router *vrid*	Removes the virtual router from the CSS
no keepalive *name*	Deletes an existing keepalive
no ospf area	Resets this interface to the default area of 0.0.0.0
no ospf cost	Resets the packet cost to its default value
no ospf dead	Resets the dead router interval to its default of 40 seconds
no ospf enable	Disables OSPF on this interface
no ospf hello	Resets the hello interval to its default value of 10 seconds
no ospf password	Removes the OSPF password from this interface
no ospf poll	Resets the poll interval to its default value of 120 seconds
no ospf priority	Resets the router priority to its default value of 1

no ospf retransmit	Resets the retransmit interval to its default value of 5 seconds
no ospf transit-delay	Resets the transit delay to its default value of 1 second
no owner *existing_owner_name*	Deletes an existing owner
no redirects	Disables the transmission of ICMP redirect messages
no redundancy-protocol	Stops running the redundancy protocol on this interface
no rip	Stops running RIP on the interface
no rip advertise *ip_address ip_mask*	Stops advertising a route through RIP on the interface
no rip default-route	Does not advertise a default route
no rip log [**rx**|**tx**]	Disables the logging of received or transmitted RIP packets
no router-discovery	Disables router discovery
no router-discovery preference	Resets the router discovery preference value to the default of 0
no unreachables	Disables the transmission of ICMP “destination unreachable” messages

(config-circuit-ip) ospf

To run OSPF on an IP interface and configure the OSPF parameters, use the **ospf** command. The syntax and options for this IP configuration mode command are:

- **ospf** - Configures this IP interface as an OSPF interface
- **ospf area** - Configures an OSPF area to the IP interface
- **ospf cost** - Configures the cost for sending a data packet on the IP interface
- **ospf dead** - Sets the interval for determining that a neighbor router is dead
- **ospf enable** - Enables OSPF on the IP interface
- **ospf hello** - Sets the interval between the hello packets that the CSS sends on the interface
- **ospf password** - Sets the password for the interface
- **ospf poll** - Sets the interval between the hello packets that the CSS sends to a dead neighbor router
- **ospf priority** - Sets the CSS priority to elect the designated router
- **ospf retransmit** - Sets the interval between link-state advertisement retransmissions for adjacencies belonging to the interface
- **ospf transit-delay** - Sets the interval to transmit a link-state update packet over the interface

For more information on these options and associated variables, see the following commands.

Related Commands

show ospf
(config) ospf

ospf

To configure the IP interface as an OSPF interface, use the **ospf** command. You must enter this command before the **(config-circuit-ip) ospf enable** command can take effect.

ospf

Command Modes

Circuit-IP

ospf area

To assign the interface to an OSPF area that you globally configured to the CSS, use the **ospf area** command. Use the **no** form of this command to reset the interface to the default area.

ospf area *area_id*

no ospf area

Syntax Description

area_id	ID for the area that was globally configured to the CSS. Enter the ID in dotted-decimal notation (for example, 0.0.0.1). An area ID of 0.0.0.0 is the default and is reserved for the OSPF backbone.

Command Modes

Circuit-IP

Related Commands

(config) ospf area

ospf cost

To set the cost for sending a data packet on the interface, use the **ospf cost** command. Use the **no** form of this command to reset the packet cost for the interface to its default value.

ospf cost *cost*

no ospf cost

Syntax Description

cost	Cost for the interface. Enter a number from 0 to 65535. The default value for a given type of circuit is 10^8 / interface_speed. For a Gigabit Ethernet interface, the value is 1. For a 10/100-Mbps Ethernet interface, the value is 10.

Command Modes

Circuit-IP

ospf dead

To set the dead router interval for the interface, use the **ospf dead** command. The interface declares that a neighbor router is dead if the interface does not receive hello packets from the router before the interval expires. Use the **no** form of this command to reset the dead router interval to its default of 40 seconds.

ospf dead *interval*
no ospf dead

Syntax Description

interval	Dead router interval in seconds. This value must be a multiple of the hello interval, and it must be the same for all routers attached to a common network. Enter a number from 1 to 2147483647. The default is 40.

Command Modes

Circuit-IP

ospf enable

To enable OSPF on the IP interface, use the **ospf enable** command. By default, OSPF is disabled on an IP interface. Do not enable OSPF until you have finished configuring its interface attributes. Use the **no** form of this command to disable OSPF on the interface.

ospf enable

no ospf enable

Command Modes

Circuit-IP

ospf hello

To set the hello interval for the interface, use the **ospf hello** command. This interval is the length of time between hello packets that the interface sends to its neighbor routers. Use the **no** form of this command to reset the hello interval to its default value of 10 seconds.

ospf hello *interval*

no ospf hello

Syntax Description

interval	Hello interval in seconds. This value must be the same for all routers attached to a common network. Enter a number from 1 to 65535. The default is 10 seconds.

Command Modes

Circuit-IP

ospf password

To set the password for the interface, use the **ospf password** command. The OSPF password is used for authentication of all OSPF protocol exchanges. Use the **no** form of this command to remove the OSPF password from the interface.

ospf password "*password***"**

no ospf password

Syntax Description

"*password*"	OSPF password. This password must be the same for all routers attached to a common network. Enter a quoted text string with a maximum of eight characters.

Command Modes

Circuit-IP

ospf poll

To set the poll interval for the interface, use the **ospf poll** command. This interval is the length of time between hello packets that the CSS sends to an assumed inactive neighbor router in a nonbroadcast, multi-access network. Use the **no** form of this command to reset the poll interval to its default value of 120 seconds.

ospf poll *interval*

no ospf poll

Syntax Description

interval	Poll interval in seconds. The interval should be larger than the hello time interval. Enter a number from 1 to 2147483647. The default is 120 seconds.

Command Modes

Circuit-IP

Usage Guidelines

The **ospf poll** command has no effect when you operate the CSS over a broadcast LAN (an Ethernet network).

ospf priority

To set the router priority for the interface, use the **ospf priority** command. The priority determines which router is the designated router. The router with the highest priority becomes the designated router. In case of a tie, routers use their router ID as a tie breaker. Use the **no** form of this command to reset the router priority to its default value of 1.

ospf priority *priority*

no ospf priority

Syntax Description

priority	Priority of the interface. Enter an integer from 0 to 255. The default is 1. The value of 0 signifies that the CSS is not eligible to become the designated router on a particular network.

Usage Guidelines

If a designated router exists on the network, it remains the designated router regardless of its router priority.

Command Modes

Circuit-IP

ospf retransmit

To set the retransmission interval for the interface, use the **ospf retransmit** command. The retransmission interval is the number of seconds between link-state advertisement retransmissions for adjacencies belonging to the interface. OSPF creates adjacencies between neighboring routers for the purpose of exchanging routing information. The CSS also uses this interval when retransmitting database descriptions and link-state request packets.

Use the **no** form of this command to reset the retransmit interval to its default value of 5 seconds.

ospf retransmit *interval*

no ospf retransmit

Syntax Description

interval	Retransmit interval in seconds. Enter a number from 1 to 3600 (1 hour). The default is 5 seconds.

Command Modes

Circuit-IP

ospf transit-delay

To set the transit delay for the interface, use the **ospf transit-delay** command. Transit delay is the estimated number of seconds to transmit a link-state update packet over the interface. Use the **no** form of this command to reset the transit delay to its default value of 1 second.

ospf transit-delay *delay*

no ospf transit-delay

Syntax Description

delay	Delay in seconds. Enter a number from 0 to 3600 (1 hour). The default is 1 second.

Command Modes Circuit-IP

(config-circuit-ip) redirects

To enable the transmission of Internet Control Message Protocol (ICMP) redirect messages, use the **redirects** command. This is the default state. Use the **no** form of this command to disable the transmission of ICMP redirect messages.

redirects

no redirects

Related Commands **show ip interfaces**

(config-circuit-ip) redundancy-protocol

To run the router redundancy protocol on the interface, use the **redundancy-protocol** command. Use the **no** form of this command to stop running the redundancy protocol on the interface.

redundancy-protocol

no redundancy-protocol

Related Commands **(config) ip redundancy**
(config) vrrp-backup-timer
(config-circuit) redundancy

(config-circuit-ip) rip

To configure Routing Information Protocol (RIP) parameters and run RIP on the interface, use the **rip** command. The default mode is to send RIP version 2 (v2) and receive either version. The options for this IP mode command are:

- **rip** - Starts RIP on the interface
- **rip advertise** - Advertises a route through RIP on this interface
- **rip default-route** - Advertises a default route on this interface
- **rip log** - Enables the logging of transmitted or received RIP packets on the interface
- **rip receive** - Specifies the RIP version packets that the interface receives
- **rip send** - Specifies the RIP version packets that the interface sends

For information on these options and associated variables, see the following commands.

rip

To start RIP on the interface, use the **rip** command. Use the **no** form of this command to stop RIP on the interface.

rip

no rip

Command Modes

Circuit-IP

rip advertise

To advertise a route through RIP on this interface, use the **rip advertise** command. Use the **no** form of this command to stop advertising a route through RIP on the interface.

rip advertise *ip_address ip_mask_prefix* {*metric*}

no rip advertise *ip_address ip_mask*

Syntax Description

ip_address	IP address for the route prefix. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1).
ip_mask_prefix	IP mask. Enter the mask as either: • A prefix length in CIDR bitcount notation (for example, /24). Do not enter a space to separate the IP address from the prefix length. • A subnet mask in dotted-decimal notation (for example, 255.255.255.0).
metric	(Optional) Metric to use when advertising this route. Enter a number from 1 to 15. The default is 1.

Usage Guidelines

You can use the **rip advertise** command in global configuration mode. When you do, it applies to all interfaces.

Command Modes

Circuit-IP

Related Commands

show rip

rip default-route

To advertise a default route on the interface, use the **rip default-route** command. Use the **no** form of this command to stop advertising the default route.

rip default-route {*metric*}

no rip default-route

Syntax Description

metric	(Optional) Metric to use when advertising the route. Enter a number from 0 to 15. The default is 1. A value of zero indicates that no default route originates from the interface. In this case, a default route through another router may be propagated.

Command Modes

Circuit-IP

Related Commands

show rip

rip log

To enable the logging of received or transmitted RIP packets on the interface, use the **rip log** command. Use the **no** form of this command to disable logging, the default setting.

rip log [**rx**|**tx**]

no rip log [**rx**|**tx**]

Syntax Description

rx	Logs the received RIP packets
tx	Logs the transmitted RIP packets

Command Modes Circuit-IP

rip receive

To specify the type of RIP packets that the interface can receive, use the **rip receive** command.

rip receive [**both|none|v1|v2**]

Syntax Description

both	Receives both version 1 and version 2 (default)
none	Receives no RIP packets
v1	Receives RIP version 1 packets only
v2	Receives RIP version 2 packets only

Command Modes Circuit-IP

Related Commands **show rip**

rip send

To specify the type of RIP packets that the interface can send, use the **rip send** command.

rip send [**none|v1|v2**]

Syntax Description

none	Does not send RIP packets
v1	Sends RIP version 1 packets only
v2	Sends RIP version 2 packets only (default)

Command Modes Circuit-IP

Related Commands

show rip

(config-circuit-ip) router-discovery

To enable router discovery and configure the router discovery preference value, use the **router-discovery** command. The syntax and option for this IP mode command are:

- **router-discovery** - Enables router discovery
- **router-discovery preference** - Configures the router discovery preference value

router-discovery

To enable router discovery, use the **router-discovery** command. The default setting disables router discovery. Use the **no** form of this command to disable router discovery.

router-discovery

no router-discovery

Command Modes

Circuit-IP

Related Commands

show ip interfaces
(config-circuit) router-discovery

router-discovery preference

To configure the router discovery preference value, use the **router-discovery preference** command. Use the **no** form of this command to reset the router discovery preference value to the default of 0.

router-discovery preference *value*

no router-discovery preference

Syntax Description

value	Preference value to advertise. Enter an integer from 0 (default) to 4294967295.

Command Modes

Circuit-IP

(config-circuit-ip) unreachables

To enable the transmission of ICMP “destination unreachable” messages, use the **unreachables** command. This is the default state. Use the **no** form of this command to disable the transmission of ICMP “destination unreachable” messages.

unreachables

no unreachables

Related Commands

show ip interfaces

DQL Configuration Mode Commands

DQL configuration mode allows you to configure a domain qualifier list (DQL). A DQL is a collection of domain names which you can assign to a content rule, instead of creating a rule for each domain.

To access DQL configuration mode, use the **dql** command from any configuration mode except boot, group, header-field-group, RMON alarm, RMON event, and RMON history configuration modes. The prompt changes to (config-dql [*name*]). You can also use this command from DQL mode to access another DQL. For information about commands available in this mode, see the following commands.

In global configuration mode, use the **no** form of this command to remove an existing DQL.

dql *dql_name*

(config) no dql *existing_dql_name*

Syntax Description

dql_name	Name of a new DQL you want to create or of an existing list. Enter an unquoted text string with no spaces and a maximum length of 31 characters. To see a list of existing DQL names, enter: `dql ?`

Usage Guidelines

When you have a requirement for a content rule to match on multiple domain names, you can associate a DQL to the rule. A DQL is a list of domain names that you configure and assign to a content rule, instead of creating a content rule for each domain. Assigning multiple domain names to a DQL enables you to have many domain names match on one content rule.

You can use a DQL on a rule to specify that content requests for each domain in the list will match on the rule. You can determine the order that the domain names are listed in the DQL. You can arrange the names in a DQL by assigning an index number as you add the name to the list.

Note You cannot use wildcards in DQL entries.

Note The CSS supports a maximum of 512 DQLs, with a maximum of 2,500 DQL domain name entries. This means that a single DQL can have up to 2500 entries, or five DQLs can have up to 500 entries for each DQL.

DQLs exist independently of any range mapping. You can use them as a matching criteria to balance across servers that do not have VIP or port ranges. If you want to use range mapping when using range services, you need to consider the index of any domain name in the DQL. If you are not using service ranges with DQLs, you do not need to configure any index and the default index is 1.

Related Commands

show dql
(config-owner-content) url

(config-dql) description

To provide a description for the domain qualifier list (DQL), use the **description** command.

description "*text*"

Syntax Description

"*text*"	DQL description. Enter a quoted text string with a maximum length of 63 characters including spaces.

(config-dql) domain

To add a domain to the list of domains supported by this DQL, use the **domain** command. Use the **no** form of this command to remove a domain from this DQL.

domain *name* **index** *number* {**"***description***"**}

no domain *name*

Syntax Description

name	Name of the domain. Enter an unquoted text string with a maximum length of 63 characters (for example, www.point.com). Normally, port 80 traffic does not use a port number in the domain name. To specify a port other than port 80, enter the domain name with the port number exactly. Separate the domain name and the port number with a colon. For example, enter: `(config-dql[pet_domains])# domain www.dogs.com:8080 index 4`
number	Index number for the domain. Enter a number from 1 to 10000. If a domain has more than one domain name, you can assign the same index number to its different names.
"*description*"	(Optional) Description for the domain. Enter a quoted text string with a maximum length of 63 characters.

(config-dql) no

To negate a command or set it to its default, use the **no** command. For information on general **no** commands you can use in this mode, see the general **no** command. The following options are available in DQL mode.

Syntax Description

no acl *index*	Deletes an ACL
no domain *name*	Removes the specified domain from the DQL
no keepalive *existing_keepalive_name*	Deletes an existing keepalive
no nql *existing_nql_name*	Deletes an existing Network Qualifier List
no owner *existing_owner_name*	Deletes an existing owner

EQL Configuration Mode Commands

EQL configuration mode allows you to configure an extension qualifier list (EQL). This list is a collection of file extensions for content requests joined together through content rules. The CSS uses this list to identify which requests to send to a service.

To access EQL configuration mode, use the **eql** command from any configuration mode except ACL, boot, DQL, group, header-field-group, NQL, and owner configuration modes. The prompt changes to (config-eql [*name*]). You can also use this command from EQL mode to access another EQL. For information about commands available in this mode, see the following commands.

Use the **no** form of this command to delete an existing extension list.

eql *eql_name*

no eql *existing_eql_name*

Syntax Description

eql_name	Name of a new extension list you want to create or of an existing list. Enter an unquoted text string with no spaces and a maximum length of 31 characters. To see a list of existing EQL names, enter: `eql ?`

Related Commands

show eql
(config-owner-content) url

(config-eql) description

To provide a description for an extension qualifier list (EQL), use the **description** command.

description "*text***"**

Syntax Description

“*text*”	Description for the EQL. Enter a quoted text string with a maximum length of 64 characters.

(config-eql) extension

To include the extension of content requests you want as part of this EQL, and optionally provide a description, use the **extension** command. Use the **no** form of this command to remove an extension from an EQL.

extension *name* **“***description***”**

no extension *name*

Syntax Description

name	Extension that appears on the content request. Enter a text string from 1 to 7 characters. Make sure you enter an extension for static content, such as avi, gif, and jpg. Do not enter extensions for dynamic content, such as html, asp, and java.
“*description***”**	Description about the extension. Enter a quoted text string with a maximum length of 64 characters.

(config-eql) no

To negate a command or set it to its default, use the **no** command. For information on general **no** commands you can use in this mode, see the general **no** command. The following options are available in EQL mode.

Syntax Description

no acl *index*	Deletes an ACL
no description	Removes a description for the EQL
no extension *extension_name*	Deletes the specified extension from the EQL
no owner *existing_owner_name*	Deletes an existing owner

Group Configuration Mode Commands

Group configuration mode allows you to configure a group. A group is a collection of local servers that initiate flows from within the local web farm. For example, after processing a group of real audio transmitters, they all appear on the same source IP address. The CSS lets you treat a group as a virtual server with its own source IP address.

To access group configuration mode, use the **group** command from any mode except ACL, boot, and header-field-group configuration modes. The prompt changes to (config-group [*name*]). You can also use this command from group mode to access another group. For information about commands available in this mode, see the following commands.

Use the **no** form of this command to delete an existing group.

group *group_name*

no group *existing_group_name*

Syntax Description

group_name	Name of a new group you want to create or of an existing group. Enter an unquoted text string with no spaces and a maximum length of 31 characters. To see a list of existing group names, enter: `group ?`

(config-group) active

To activate the specified group, use the **active** command.

active

Related Commands

(config-group) suspend

(config-group) add destination service

To add a destination service to a source group, use the **add destination** command.

add destination service *service_name*

Syntax Description

service_name	Name of the service to add to the group. Enter an unquoted text string. To see a list of services, enter: `show service ?`

Usage Guidelines

You can configure a maximum of 64 services per source group.

You cannot use a service with the same name in other source groups or the source service list within the same source group. You can use services with duplicate addresses among destination services since the actual service is chosen through content rule selection.

If the group is active and the same service is hit through a content rule, ACL preferred service, or sorry service, the source group is used to NAT the source address.

The service must be active and added to a content rule to perform destination address NATing for the source group.

Note Adding a destination service to a group will not allow that specific service flows to be NATed by the group when initiated flows are from the service. The destination service applies group membership based on rule and service match. To ensure service-initiated connections are NATed, you must additionally configure an ACL match criteria or additional service names with duplicate addresses, and then add those services to a source group. The source group used could be the current group with the destination service or any other group.

If your topology consists of a CSS 11800 using ECMP to the servers and server port NAT configured on the services, to ensure the correct processing of packets either:

- Enable Service Remapping with the **persistence reset remap** command.
- Create source groups for the services in the content rule with the **add destination service** command.

Related Commands

show group
show service
(config-group) remove destination service

(config-group) add service

To add a source service to a source group, use the **add service** command.

add service *service_name*

Syntax Description

service_name	Name of the service to add to the group. Enter an unquoted text string. To see a list of services, enter: `show service ?`

Usage Guidelines

You can configure a maximum of 64 services per source group.

You cannot use a service with:

- The same name in other source groups or the destination service list within the same source group
- The same address as a source service on another source group

If the service matches the client, the source group is used.

Before you can add a service, you must suspend the group.

The services configured under a source group must be active to perform NATing through the group.

Related Commands

show group
show service
(config-group) remove service

(config-group) flow-timeout-multiplier

To specify the number of seconds for which an idle flow can exist before the CSS tears it down, use the **flow-timeout-multiplier** command. Use the **no** form of this command to restore the default timeout for the port type.

flow-timeout-multiplier *timeout-multiplier*

no flow-timeout-multiplier

Syntax Description

timeout-multiplier	Value that the CSS multiplies by 16 to calculate the flow timeout in seconds. Enter an integer from 0 to 65533. The default value depends on the port type (see the **show flow-timeout default** command). This default value applies only to flows that are created under the specified source group. A value of zero (no timeout) instructs the CSS to never tear down the flow, resulting in a permanent flow and lost resources. This is equivalent to entering the global configuration **flow permanent port** command.

Usage Guidelines

We do not recommend that you set the **flow-timeout multiplier** command to 0 for UDP flows on Layer 3 and Layer 4 content rules. If the value is set to 0, the CSS does not clean up the resources for the UDP flows.

Use the **flow-timeout-multiplier** command to configure flow inactivity timeout values for TCP and UDP flows on a per-rule and per-source group basis. Note that this timeout value is *not* the frequency with which a CSS reclaims flow resources, but the time period that must elapse for an idle flow before the CSS cleans up the flow.

If you configure a source group with destination services for client source NATing, you need to configure the **flow-timeout multiplier** command only on the content rule. The CSS sets the same flow timeout value for flows in both directions. If you configure different timeout values on the content rule and on the source group, the CSS uses the timeout value configured on the content rule for both flows.

To set up and keep track of flows, a CSS uses data structures called flow control blocks (FCBs). For optimal performance, the CSS reuses FCBs that are no longer needed by flows. Flow resource reclamation involves removing FCBs from the TCP and UDP lists.

Normally, flow cleanup occurs at a rate that is directly related to the overall number of flows that are currently active on a CSS. The fewer the number of active flows there are on a CSS, the less frequently the CSS reclaims FCBs. A CSS also cleans up long-lived TCP flows that have received a FIN or a RST, or whose timeout values have been met.

The CSS uses the following precedence when reclaiming flow resources:

1. If a flow matches on a content rule, the CSS checks for a user-configured timeout value and uses that value if one exists.
2. If the flow matches on a source group, the CSS checks for a user-configured timeout and uses that value if one exists.
3. If you have configured a permanent port using the global configuration **flow permanent port** command, the CSS sets the flow timeout value to 0, which means that the flow should never time out.
4. If none of the previous conditions are met, then the CSS uses the default timeout value for the protocol type.

Related Commands

show flow-timeout
(config) flow permanent

(config-group) ip address

To specify the source IP address for the group, use the **ip address** command. This address is substituted for the source address in flows originating from one of the group's sources. This command's function is identical to the **(config-group) vip address** command.

ip address *ip_address*

Syntax Description

ip_address	IP address for the group. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1).

Related Commands

show group

(config-group) no

To negate a command or set it to its default, use the **no** command. For information on general **no** commands you can use in this mode, see the general **no** command. The following options are available in group mode.

Syntax Description

no acl *index*	Deletes an ACL
no flow-timeout-multiplier	Restores the default flow timeout for the port type
no portmap base-port	Resets the starting SFP port number to its default value
no portmap number-of-ports	Resets the number of ports per SFP to its default value
no redundancy-l4-stateless	Disables stateless redundancy failover
no redundant-index	Disables redundancy on the source group

(config-group) portmap

To enable or disable the NATing of source IP addresses and source ports for a configured source group, or define the source port translation of flows from the services configured in a source group, use the **portmap** command. Use the **no** form of this command to reset the starting SFP port number to its default value of 2016 or number of ports to its default value of 63488.

portmap [**base-port** *base_number*|**disable**|**enable**|**number-of-ports** *number*|**vip-address-range** *number*]

no portmap [**base-port**|**number-of-ports**|**vip-address-range**]

Syntax Description

base-port *base_number*	Defines the base port (starting port number) for the CSS. Enter a base number from 2016 to 63456. The default is 2016.

disable	Instructs the CSS to perform Network Address Translation (NAT) only on the source IP addresses and not on the source ports of UDP traffic hitting a particular source group. This option does not affect TCP flows. For applications with high-numbered assigned ports (for example, SIP and WAP), we recommend that you preserve those port numbers by configuring destination services in source groups. Destination services cause the CSS to NAT the client source ports, but not the destination ports. **Note** If you disable flows for a UDP port using the flow-state table and configure the **portmap disable** command in a source group, traffic for that port that matches on the source group does not successfully traverse the CSS. The CSS maintains but ignores any **base-port** or **number-of ports** (see the options above) values configured in the source group. If you later reenable port mapping for that source group, any configured **base-port** or **number-of ports** values will take effect. The default behavior for a configured source group is to NAT both the source IP address and the source port for port numbers greater than 1023.
enable	Restores the default CSS behavior of NATing source IP addresses and source ports for a configured source group.

number-of-ports *number*	Defines the total number of ports in the portmap range for the entire CSS. The CSS allocates the total number of configured ports proportionally among all the session processors in the CSS chassis. The allocation is based on the session processor relative weight value. To display the relative weight value of a session processor, enter the **show chassis session-processors** command as described in the *Cisco Content Services Switch Administration Guide*. The more modules you add to the CSS chassis, the fewer session processing each module performs and the fewer ports the CSS assigns to each module. To display the number of ports that the CSS allocates to each module, enter the **show group portmap** command. Enter a number from 2048 to 63488. The default is 63488. This default value should be fine for most applications. If you enter a value that is not a multiple of 32, the CSS rounds up the value to the next possible multiple of 32.

vip-address-range *number*	Specifies a VIP address range for port mapping. Use this option to increase the number of available ports for port mapping. For each additional VIP address that you configure, the CSS creates a new port mapper to manage the available ports for that VIP. When the CSS performs PAT, the source group roundrobins among all the configured port mappers and the selected port mapper chooses the next eligible port for a given VIP. The *number* variable indicates a range of VIP addresses starting with the address specified by the group configuration mode **vip address** command. Enter an integer from 1 to 255. The default is 1. With a VIP range of 255, the maximum number of eligible ports on an SCM in a fully populated CSS 11506 chassis is 63240. For other SPs or chassis configurations, the number of ports is greater. If you observe no-portmap errors, increase the *number* variable to make additional source ports available for port mapping. Note that configuring a VIP address range for port mapping is different from a Virtual Web Hosting (VWH) configuration where you configure a VIP address range on a source group, not the port mapper. In a VWH configuration, there is only one port mapper available. For complete details, refer to the *Cisco Content Services Switch Content Load-Balancing Guide*.

Usage Guidelines

Before you can change the port mapping, you must suspend the group.

The services configured under the source group must be active to perform source address NATing through the group.

(config-group) redundancy-l4-stateless

To enable the Stateless Redundancy Failover feature for a source group on a redundant CSS, use the **redundancy-l4-stateless** command. The CSS can set up a connection for a mid-stream TCP flow, allowing TCP traffic to continue when a failure occurs at the load-balancing CSS. By default, the CSS rejects TCP sessions that do not begin with a TCP/SYN frame. Use the **no** form of this command to reset the default behavior of the CSS.

redundancy-l4-stateless

no redundancy-l4-stateless

Command Modes

Group configuration mode

Usage Guidelines

The Stateless Redundancy Failover feature has specific environment and configuration requirements. The environment requirements are as follows:

- Layer 3 and Layer 4 content rules with a VIP address. This feature is not supported in Layer 5 configurations.
- Source IP address load balance method only.
- CSS-to-CSS identical server and content rule configuration including:
  - Content VIP address.
  - Content balance method.
  - Failover method.
  - Service IP address, number, and order. The CSS orders services alphabetically. Apply identical service names on the master and backup CSSs.
- Visibility of identical servers to keepalive traffic from CSS to CSS. This ensures that the redistribution of the balance method does not occur in a failover event.

Redundant routes in a high availability topology surrounding the CSS are supported. However, the topology must not balance packets in a TCP/IP socket connection across more than one Ethernet port on the CSS.

IP and VIP redundant configurations are supported. The configuration requirement for each server farm is synchronization across all CSSs of:

- Membership and IP addresses of the server farms.
- Content rule VIP address. Each CSS must share the content VIP address that is used as a balance point for the server farm.
- Source group VIP address. Define each CSS with a source group VIP address as the content VIP address to NAT source addresses for packets returning from the server. In case of a failover, the source group handles connection setups for TCP/IP retransmissions that arrive at the CSS from a server. All servers on the farm must be a member of the source group.

  Do not configure source groups for outbound traffic from the servers because the backup CSS does not know which ports were mapped by the source group on the master CSS. This restriction also applies to active FTP because the server initiates the data connection.

For more detailed information on Stateless Redundancy Failover, refer to the *Cisco Content Services Switch Redundancy Configuration Guide*.

Related Commands

show redundancy
(config) ip redundancy
(config) group
(config) interface
(config) service
(config-owner) content
(config-owner-content) redundancy-l4-stateless

(config-group) redundant-index

To configure the global content index for a redundant source group, use the **redundant-index** command. A CSS uses the global content index to keep track of redundant content rules and associated flow state information. Use the **no** form of this command to disable redundancy on the source group.

redundant-index *number*

no redundant-index

Syntax Description

number	Redundant index for the source group. Enter a unique integer from 0 to 32767, where a value of 0 disables ASR for a source group. The default is 0, but it does not appear in the running-config even if you configure it explicitly.

Usage Guidelines

If you enter the **no redundant-index** command on an active redundant source group on live redundancy peers, the command automatically suspends the source group. Flows already mapped by a CSS are not affected. However, if a failover occurs during the life of an active flow that matches on such a suspended source group, the backup CSS cannot map the flow because it cannot find the source group with the same global index as that on the original master.

Note For implicit or explicit Layer 5 rules, where there is delayed binding, binding is not complete until the CSS processes the SYN/ACK from the server. This means that, if a failover occurs in the middle of a spanned content request, the master CSS will not receive the SYN/ACK from the server and the flow will not be replicated on the backup CSS. No data is lost and users can simply refresh their browsers to restart the connection.

For information on redundant indexes and configuring Adaptive Session Redundancy (ASR) on Cisco 11500 series CSS peers, including requirements and restrictions that apply to both CSS peers in an ASR configuration, refer to the *Cisco Content Services Switch Redundancy Configuration Guide*.

Related Commands

(config-group) vip address
(config-owner-content) redundant-index
(config-service) redundant-index

(config-group) remove destination service

To remove a previously configured destination service from a source group, use the **removedestination service** command.

remove destination service *service_name*

Syntax Description

service_name	Name of an existing service you want to remove from the group. Enter a case-sensitive unquoted text string. To see a list of services for this group, enter: `show group`

Related Commands

show group
show service
(config-group) add destination service

(config-group) remove service

To remove a previously configure a source service from a source group, use the **remove service** command.

remove service *service_name*

Syntax Description

service_name	Name of an existing service you want to remove from the group. Enter a case-sensitive unquoted text string. To see a list of services for this group, enter: `show group`

Usage Guidelines

Before you can remove a service, you must suspend the group.

Related Commands

show group
show service
(config-group) add service

(config-group) suspend

To suspend the specified group, use the **suspend** command. The group and its attributes remain the same but it no longer has an effect on flow creation.

suspend

Usage Guidelines

To reactivate the group, use the **(config-group) active** command.

Related Commands

show group
(config-group) active

(config-group) vip address

To specify the source virtual IP address or a range of IP addresses for the group, use the **vip address** command. The address is substituted for the source address in flows originating from one of the group's sources. This command's function is identical to the **(config-group) ip address** command. Use the **no** form of this command to remove the VIP address for the group.

vip address *ip_or_host* {**range** *number*}

no vip address

Syntax Description

ip_or_host	IP address or name for the group. Enter the address in either dotted-decimal IP notation (for example, 192.168.11.1) or mnemonic host-name format (for example, myhost.mydomain.com).
range *number*	(Optional) Defines the range of IP addresses for the group. Enter a *number* from 1 to 65353. The default is 1. The *ip_or_host* variable is the first address in the range.

Usage Guidelines

Before you can change the address to 0 or use the **no vip address** command, you must suspend the group.

Related Commands

show group

(config-group) zero all

To set the statistics displayed by the **show group** command to zero, use the **zero all** command.

zero all

Related Commands

show group

Header-Field Group Configuration Mode Commands

Header-field group configuration mode allows you to configure a request header-field group. A request header-field group contains a list of defined header-field entries used by the content rule lookup process. Each header-field group is given a unique name so different content rules can use them. A group can contain several header-field entries.

To access header-field-group configuration mode, use the **header-field-group** command from configuration modes except boot and RMON modes. The prompt changes to (config-header-field-group [group_name]). You can also use this command in header-field-group mode to access another group. For information about commands available in this mode, see the following commands.

Use the **no** form of this command to delete an existing header-field group.

header-field-group *group_name*

no header-field-group *group_name*

Syntax Description

group_name	The header-field group that you want to configure. You must define a unique name for each header-field group so different content rules can use the groups. Enter a text string with a maximum of 32 characters. To see an existing list of header-field groups, enter: `header-field-group ?`

Usage Guidelines

The CSS supports a maximum number of 1024 header field groups, with a maximum of 4096 header field entries.

When there is more than one header field entry in a group, each header field entry must be successfully matched before the CSS uses the associated content rule.

Related Commands

show header-field-group
(config-owner-content) header-field-rule

(config-header-field-group) description

To provide a description for a header-field group, use the **description** command. Use the **no** form of this command to delete a description for a header-field group.

description "*text***"**

no description

Syntax Description

text	A description for the header-field group. Enter a quoted text string with a maximum length of 64 characters.

Related Commands

show header-field-group

(config-header-field-group) header-field

To define a header-field entry in a header-field group, use the **header-field** command. A header-field entry contains a header-field name, field type to be used, an operation to be performed, the header-string to be searched for, and an optional search length.

Use the **no** form of this command to delete a header-field entry for a header-field group.

header-field *name field_type operator*

no header-field *name*

Syntax Description

name	The name uniquely identifies the header-field entry. Enter the name as a string from 1 to 31 characters. You must define a header-field entry name because the CSS is able to use the same field type multiple times in a header-field group.
field_type	The field type includes a request line and all the commonly used header fields in an HTTP request header. For more information, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*. Enter one of the following: • **accept** • **cache-control** • **charset** • **connection** • **cookies** • **custom** • **encoding** • **host** • **language** • **msisdn** • **pragma** • **referer** • **request-line** • **user-agent**

operator Enter one of the following operators:

- **exist|not-exist**. Use the **exist** and **not-exist** operators to check whether a specified header field exists in a content request header.
- **equal |not-equal** {**"***header_string***"**}. Use the **equal** and **not-equal** operators to match a defined *header_string* to the contents of the specified header field, and determine whether it is equal to the header string. Enter the *header_string* as a quoted text string with a maximum of 31 characters including spaces.
- **contain |not-contain** {**"***header_string***"** {*search_length*}}. Use the **contain** and **not-contain** operators to match the configured *header_string* to a substring in the contents of the specified field type, and determine whether its contents contain the *header_string*. Enter the *header_string* as a quoted text string with a maximum of 31 characters including spaces.

  You may include an optional *search_length* to define the header field portion to be used for the operation. If you do not define a search length, the CSS uses the entire header field (delimited by a CR and LF) for the operation. To define the search length, enter a number from 0 to 1024.

Usage Guidelines

If a header-field group contains multiple header-field entries, a content request must match each entry for the rule to be used.

Related Commands

show header-field-group

(config-header-field-group) no

To negate a command or set it to its default, use the **no** command. For information on general **no** commands you can use in this mode, see the general **no** command. The following options are available in header-field-group mode:

Syntax Description

no acl *index*	Deletes an ACL
no description	Removes a description for a header-field group
no header-field *name*	Removes a header-field entry
no header-field-group *name*	Removes a header-field group

Interface Configuration Mode Commands

Interface configuration mode allows you to configure an interface in the CSS. To access interface configuration mode, use the **interface** command from global, circuit, IP, and keepalive configuration modes. The prompt changes to (config-if [interface_name]). You can also use this command in interface mode to access another interface.

interface *interface_name*

Syntax Description

interface_name	CSS interface that you want to configure. For a CSS 11501, enter the interface name in *interface-port* format (for example, e2). For a CSS 11503 or 11506, enter the interface name in *slot/port* format (for example, 3/1). To see a list of valid interfaces for this CSS, enter: `interface ?`

(config-if) admin-shutdown

To shut down the current interface, use the **admin-shutdown** command. Use the **no** form of this command to restart the interface.

admin-shutdown

no admin-shutdown

Usage Guidelines

To shut down all interfaces in the CSS, use the **admin-shutdown** command in SuperUser mode.

Related Commands

admin-shutdown
show interface

(config-if) bridge

To configure bridge parameters, use the **bridge** command. The options for this interface mode command are:

- **bridge pathcost** - Sets the bridge interface path cost
- **bridge port-fast** - Enables Port Fast forwarding for a non-trunked CSS interface (port)
- **bridge port-priority** - Sets the bridge port priority
- **bridge state** - Enables or disables the bridge interface
- **bridge vlan** - Sets the bridge interface virtual LAN number

For more information on these options and associated variables, see the following commands.

Note Before you can configure trunking and multiple VLANs on an Ethernet interface, the **(config-if) bridge** command options must be at their default states. You can turn on trunking through the **(config-if) trunk** command, and assign the VLAN and access VLAN mode through the **(config-if) vlan** command.

Related Commands

(config) interface

bridge pathcost

To set the bridge interface path cost, use the **bridge pathcost** command. Use the **no** form of this command to restore the default path cost which the CSS sets automatically based on the port speed.

bridge pathcost *cost*

no bridge pathcost

Syntax Description

cost	Contribution of the port to the path cost of paths towards the spanning tree root. Enter an integer from 1 to 65535. The CSS sets the default pathcost automatically based on the port speed.

Command Modes

Interface

bridge port-fast

To enable PortFast forwarding for a nontrunked CSS port, use the **bridge port-fast** command. By default, PortFast forwarding is disabled.

bridge port-fast [**enable**|**disable**]

Syntax Description

enable	Enables PortFast forwarding
disable	Disables PortFast forwarding (default)

Command Modes

Interface configuration mode

Usage Guidelines

You cannot configure PortFast on a trunked port.

PortFast forwarding mode skips spanning-tree intermediate states (such as listening and learning) when a port moves from blocking to forwarding state, thereby providing access to the network without delay.

Related Commands

show bridge
(config-if) bridge bpdu-guard

bridge port-priority

To set the bridge priority for the port, use the **bridge port-priority** command. Use the **no** form of this command to restore the default priority of 128.

bridge port-priority *priority*

no bridge port-priority

Syntax Description

priority	Value of the bridge priority for the port. Enter an integer from 0 to 255. The default is 128.

Command Modes

Interface

bridge state

To enable or disable the bridge interface, use the **bridge state** command.

bridge state [**disable**|**enable**]

Syntax Description

disable	Disables the bridge interface. This is the default state.
enable	Enables the bridge interface.

Command Modes

Interface

bridge vlan

To set the bridge interface virtual LAN identifier, use the **bridge vlan** command. Use the **no** form of this command to restore the default virtual LAN identifier of 1.

bridge vlan *number*

no bridge vlan

Syntax Description

number	Virtual LAN identifier to associate with this port. Enter an integer from 1 to 4094. The default is 1.

Command Modes

Interface

Usage Guidelines

The following list defines the maximum number of VLANs supported by the specific CSS models:

- CSS 11501 and 11503 - A maximum of 256 VLANs
- CSS 11506 - A maximum of 512 VLANs

(config-if) description

To specify the description for the interface, use the **description** command. Use the **no** form of this command to delete the interface description.

description "*text_string*"

no description

Syntax Description

"*text_string*"	Description for the interface. Enter a quoted text string with a maximum length of 255 characters.

Related Commands

show running-config interface

(config-if) fcb-lowwater

To configure the low-water mark of flow control blocks (FCBs) on the interface, use the **fcb-lowwater** command. The low-water mark is the percentage of the total number of FCBs available. If the number of FCBs available on a port goes below the low-water mark, then aggressive flow recovery occurs.

Use the **no** form of this command to reset the percentage of available FCBs to its default of 25.

fcb-lowwater *percentage*

no fcb-lowwater

Syntax Description

percentage	Percentage of the total number of available FCBs. Enter a number from 1 to 100. The default is 25.

(config-if) isc-port-one

To enable Inter-Switch Communications (ISC) on the first port between two CSSs in an ASR configuration, use the **isc-port-one** command. Use the **no** form of the command to disable ISC on the first port.

isc-port-one

no isc-port-one

Usage Guidelines

ISC allows 11500 series CSS peers to exchange flow state information in an ASR configuration. If the master CSS fails, the backup CSS already has the flow state information necessary to continue the current flows without interruption. Using ISC, CSSs exchange state information:

- For existing flows at boot-up time and at VIP redundancy failover
- For new flows in real time (after the CSS receives a SYN/ACK from the server)

You can configure a maximum of two ISC ports on a CSS. Multiple ports must reside on the same module in the CSS 11503 or 11506 or on the same CSS 11501. Also, the ports must be of the same type (Gigabit Ethernet or Fast Ethernet) in both CSSs. The CSS 11501 does not support redundant GE Inter-Switch Communications links for ASR because the switch includes only a single GBIC port.

If you configure any ISC ports on an SCM, you can have only one SCM installed in the CSS 11506. Be sure that the ISC ports are not configured in any VLANs. If necessary, remove the designated ports from all VLANs before configuring ISC. Ensure that you connect the ISC ports between the two CSSs directly.

(config-if) isc-port-two

To enable Inter-Switch Communications (ISC) on a second port between two 11500 series CSSs in an ASR configuration, use the **isc-port-two** command. ISC allows two redundant CSSs to exchange flow state information. If a failover occurs, the backup CSS has enough flow state information to continue current flows without interruption. Use the **no** form of this command to disable ISC on the second port.

isc-port-two

no isc-port-two

Usage Guidelines

For the CSS 11503 or 11506, the second port must be on the same module as the first port. Also, the ports must be of the same type (Gigabit Ethernet or Fast Ethernet) in both CSSs. The CSS 11501 does not support redundant GE Inter-Switch Communications links for ASR because the switch includes only a single GBIC port.

If you configure any ISC ports on an SCM, you can have only one SCM installed in the CSS 11506. Be sure that the ISC ports are not configured in any VLANs. If necessary, remove the designated ports from all VLANs before configuring ISC. Ensure that you connect the ISC ports between the two CSSs directly.

(config-if) max-idle

To set the maximum idle time for the interface, use the **max-idle** command. Use the **no** form of this command to reset the idle time for this interface to its default value of 0.

max-idle *seconds*

no max-idle

Syntax Description

seconds	Idle time in seconds. Enter a number from 15 to 65535. The default is 0, which disables the idle timer.

Usage Guidelines

Use the **max-idle** as a troubleshooting tool to verify an interface's ability to receive traffic. If the interface does not receive traffic within the maximum time configured, the CSS reinitializes it automatically.

Set the idle time to a value greater than the interval over which the interface is not receiving traffic. For example, if the interface receives traffic every 90 seconds, set the idle time to a value greater than 90 seconds. If you set the idle time to less than 90 seconds in this situation, the CSS would continuously reinitialize the interface before the interface was able to receive traffic.

(config-if) no

To negate a command or set it to its default, use the **no** command. For information on general **no** commands you can use in this mode, see the general **no** command. The following options are available in interface mode.

Syntax Description

no acl *index*	Deletes an ACL
no admin-shutdown	Restarts the interface
no bridge pathcost	Restores the default path cost which the CSS sets automatically based on the port speed

no bridge port-priority	Restores the default port priority of 128
no bridge vlan	Restores the default virtual LAN number of 1
no description	Clears the description for the interface
no fcb-lowwater	Resets the percentage of available FCBs to its default of 25
no isc-port-one	Disables ISC on the first port in the CSS
no isc-port-two	Disables ISC on the second port in the CSS
no keepalive *name*	Deletes an existing keepalive
no max-idle	Resets the maximum idle time for this interface to the default of 0 (disabled)
no owner *existing_owner_name*	Deletes an existing owner
no redundancy-phy *interface_name*	Deletes an interface from the physical link configuration list
no shut	Restarts the interface
no trunk	Disables trunking on the Ethernet interface and removes all associated VLANs
no vlan *number*	Deletes the VLAN from a trunked Ethernet interface

(config-if) phy

To configure the speed or flow control (pause) method and duplex for a CSS Fast Ethernet or Gigabit Ethernet interface (port), use the **phy** command.

phy [**auto-negotiate** [**enable**|**disable**]|**10Mbits-**[**FD**|**HD**]
|**100Mbits-**[**FD**|**HD**]|**1Gbits-FD-**[**asym**|**no pause**|**sym**|**sym-asym**]]

Syntax Description

auto-negotiate	Resets the Fast Ethernet or Gigabit Ethernet port to automatically negotiate speed or pause method and duplex (default). **Note** The CSS 1000BASE-T Gigabit Ethernet port supports 1000 Mbps full-duplex operation only and does not support auto-negotiation.
enable|disable	Disables or enables the Gigabit Ethernet interface autonegotiation. By default, autonegotiation is enabled for all Gigabit Ethernet ports. **Note** The CSS 1000BASE-T Gigabit Ethernet port supports 1000 Mbps full-duplex operation only and does not support auto-negotiation. Autonegotiation remains enabled when a pause mode command is entered in order for the Gigabit Ethernet interface ports to act upon the link partner's flow control capability. If it is necessary to disable autonegotiation for the Gigabit Ethernet port when using a pause mode, use the **phy auto-negotiate disable** command.
10Mbits-FD	Sets the Fast Ethernet port to 10 Mbps and full duplex.
10Mbits-HD	Sets the Fast Ethernet port to 10 Mbps and half duplex.
100Mbits-FD	Sets the Fast Ethernet port to 100 Mbps and full duplex.
100Mbits-HD	Sets the Fast Ethernet port to 100 Mbps and half duplex.
1Gbits-FD-asym	Sets the Gigabit Ethernet port to full-duplex mode with asymmetric pause toward the link partner.
1Gbits-FD-no pause	Sets the Gigabit Ethernet port to full-duplex mode with no pause.
1Gbits-FD-sym	Sets the Gigabit Ethernet port to full-duplex mode with symmetric pause.
1Gbits-FD-sym-asym	Sets the Gigabit Ethernet port to full-duplex mode with asymmetric and symmetric pause toward the local device.

Usage Guidelines

By default, the CSS Fast Ethernet and Gigabit Ethernet interfaces are configured to auto-negotiate, which enables the CSS ports to automatically detect the network line speed (Fast Ethernet only) and duplex of incoming signals, and to synchronize those parameters during data transfer. Autonegotiation enables the CSS and the other devices on the link to achieve the maximum common level of operation.

Note The CSS 1000BASE-T Gigabit Ethernet port supports 1000 Mbps full-duplex opration only and does not support auto-negotiation.

If you configure the **redundancy-phy** command on an interface of the master CSS and then make any change to the port settings of that interface using the **phy** command (for example, changing **auto-negotiate** to **100Mbits-FD**), the master CSS fails over to the backup CSS. To prevent the failover from occurring, enter the **no redundancy-phy** command on the interface first, change the port settings, then reenter the **redundancy-phy** command.

For the Fast Ethernet ports, when older equipment cannot transmit the duplex and speed with its signals, you can manually configure the speed (10 Mbps, 100 Mbps) and duplex (half or full duplex) of the CSS port to match the transmitting equipment.

For the Gigabit Ethernet ports, if the link does not come up (perhaps due to traffic congestion), you may need to force the CSS and its link partner into a specific mode. The CSS allows you to manually select a full duplex and flow control (pause frame) mode. Flow control allows the CSS to control traffic during congestion by notifying the other port to stop transmitting until the congestion clears. When the other device receives the pause frame, it temporarily stops transmitting data packets. When the CSS detects local congestion and becomes overwhelmed with data, the Gigabit Ethernet ports transmit a pause frame. Both the CSS Gigabit Ethernet and its link partner must be configured with the same pause method (asymmetric, symmetric, or both). By default, all Gigabit Ethernet ports are configured to full-duplex mode with symmetric pause (pause frames transmitted and received by the CSS).

(config-if) redundancy-phy

To add the interface to the physical link configuration list, use the **redundancy-phy** command. If any physical link in the configuration list goes down, the CSS fails over to the backup CSS. Use the **no** form of this command to delete the interface from the physical link configuration list.

redundancy-phy

no redundancy-phy

Usage Guidelines

You cannot use the **redundancy-phy** command if you used the **(config) ip redundancy master** command to configure the master CSS. Before you can use the **redundancy-phy** command, you must enter the **(config) no ip redundancy master** command.

You can configure a maximum number of 32 interfaces in the physical link configuration list. The physical link configuration information is saved to the running configuration.

When you use the redundancy-phy command and both CSSs are connected to a Layer 2 switch, be sure to monitor physical link failure only on the critical physical links and not on the redundant link between the two CSSs. This will avoid the detection of a physical link down and possible thrashing when one of the CSSs is rebooting or transitioning between master and backup states.

If you configure the **redundancy-phy** command on an interface of the master CSS and then make any change to the port settings of that interface using the **phy** command (for example, changing **auto-negotiate** to **100Mbits-FD**), the master CSS fails over to the backup CSS. To prevent the failover from occurring, enter the **no redundancy-phy** command on the interface first, change the port settings, then reenter the **redundancy-phy** command.

If you configure the **redundancy-phy** command on an interface and then disable the interface using the **admin-shutdown** command, the master CSS fails over to the backup CSS. To prevent the CSS from failing over when you administratively disable the interface, remove the **redundancy-phy** command by entering **no redundancy-phy** before you enter the **admin-shutdown** command on that interface.

Related Commands

show redundancy
(config) no ip redundancy master

(config-if) shut

To shut down the current interface, use the **shut** command. Use the **no** form of this command to restart the interface.

shut

no shut

Usage Guidelines

The **shut** command performs the same function as the Interface mode **admin-shutdown** command. When you use the **shut** command, the CSS changes this command to the **admin-shutdown** command in the running configuration.

To shut down all interfaces in the CSS, use the **admin-shutdown** command in SuperUser mode.

Related Commands

admin-shutdown
show interface

(config-if) trunk

To enable VLAN trunking for an Ethernet interface, use the **trunk** command. After you enable trunking, you can add a VLAN to the interface and enter VLAN mode to configure it. Use the **no** form of this command to disable trunking on the interface and remove its associated VLANs.

trunk

no trunk

Usage Guidelines

If you configured nondefault values for the bridge VLAN, path cost, state, and path cost on the interface, the CSS prompts that you cannot use the **trunk** command. Use the **no** form of the **(config-if) bridge** command to set the bridge default attributes before executing the **trunk** command.

Related Commands

show trunk
(config-if) vlan

(config-if) vlan

To add a VLAN on a trunked Ethernet interface and access VLAN mode to configure it, use the **vlan** command. For more information on VLAN mode and its commands, see the "VLAN Configuration Mode Commands" section. Use the **no** form of this command to delete the VLAN from the interface.

vlan *number*

no vlan *number*

Syntax Description

number	Virtual LAN identifier to associate with the interface. Enter an integer from 1 to 4094. The default is 1.

Usage Guidelines

Before you can use the **vlan** command, you must enable trunking through the **(config-if) trunk** command. You can add multiple VLANs to a trunked interface.

The following list defines the maximum number of VLANs supported by the specific CSS models:

- CSS 11501 and 11503 - A maximum of 256 VLANs
- CSS 11506 - A maximum of 512 VLANs

Command Modes

Interface

VLAN Configuration Mode Commands

VLAN configuration mode allows you to configure VLANs on a trunked Ethernet interface in the CSS. The following list defines the maximum number of VLANs supported by the specific CSS models:

- CSS 11501 and 11503 - A maximum of 256 VLANs
- CSS 11506 - A maximum of 512 VLANs

To access VLAN configuration mode, use the **vlan** command from the interface or reporter configuration mode. The prompt changes to (config-if-vlan [number]). You can also use this command in VLAN mode to access a circuit, service, interface, or another VLAN. For information about commands available in this mode, see the following commands.

(config-if [interface_name]) # **vlan** *number*

Syntax Description

number	Virtual LAN identifier to associate with this port. Enter an integer from 1 to 4094.

(config-if-vlan) bridge

To configure spanning-tree parameters for the VLAN on the interface, use the **bridge** command. The options for this VLAN mode command are:

- **bridge pathcost** - Sets the spanning-tree port path cost
- **bridge port-priority** - Sets the spanning-tree port priority
- **bridge state** - Enables or disables the spanning-tree port

For more information on these options and associated variables, see the following commands.

Related Commands

(config) interface

bridge pathcost

To set the spanning-tree port path cost for the VLAN on the trunked interface, use the **bridge pathcost** command. Use the **no** form of this command to restore the default path cost which the CSS sets automatically based on the port speed.

bridge pathcost *cost*

no bridge pathcost

Syntax Description

cost	Contribution of the port to the path cost of paths toward the spanning-tree root. Enter an integer from 1 to 65535. The CSS sets the default pathcost automatically based on the port speed.

Command Modes

Interface-vlan

bridge port-priority

To set the spanning-tree port priority for the VLAN on the trunked interface, use the **bridge port-priority** command. Use the **no** form of this command to restore the default priority of 128.

bridge port-priority *priority*

no bridge port-priority

Syntax Description

priority	Value of the spanning-tree port priority. Enter an integer from 0 to 255. The default is 128.

Command Modes

Interface-vlan

bridge state

To enable or disable the spanning-tree port on the VLAN on the trunked interface, use the **bridge state** command.

bridge state [**disable**|**enable**]

Syntax Description

disable	Disables the spanning-tree port on the VLAN.
enable	Enables the spanning-tree port on the VLAN. This is the default state.

Command Modes

Interface-vlan

(config-if-vlan) default-vlan

To define the VLAN as the default VLAN, use the **default-vlan** command. The default VLAN receives and processes all inbound untagged frames on the interface. The VLAN also transmits all outbound frames as untagged. Use the **no** form of this command to unassign the VLAN as the default VLAN.

default-vlan

no default-vlan

Usage Guidelines

You can define only one VLAN on each interface as the default VLAN. Before you can assign another VLAN as the default VLAN, use the **no default-vlan** command to unassign the current default VLAN.

If no VLAN on the interface is the default VLAN, the interface discards all untagged frames.

Command Modes

Interface-vlan

(config-if-vlan) no

To negate a command or set it to its default, use the **no** command. For information on general **no** commands you can use in this mode, see the general **no** command. The following options are available in VLAN mode.

Syntax Description

no bridge pathcost	Restores the default path cost which the CSS sets automatically based on the port speed
no bridge port-priority	Restores the default priority of 128
no default-vlan	Unassigns the VLAN as the default VLAN

Keepalive Configuration Mode Commands

Keepalive configuration mode allows you to configure keepalive properties and apply them to any service. Global keepalives reduce the amount of configuration required for each service. You can apply the keepalive configuration to multiple services. Global keepalives are independent of service mode.

Note You can configure keepalive message parameters for a service in service configuration mode. However, if you assign a keepalive you created in keepalive mode to a service, it supersedes the keepalive parameters configured in service mode.

The CSS divides the keepalive types into two categories, Class A and Class B keepalives. The CSS supports a maximum of 2048 Class A keepalives. The CSS supports a maximum of 512 Class B keepalives. Table 2-1 lists the keepalive types in each class, the maximum number of each type, and the maximum number of each keepalive type that can execute concurrently.

Table 2-1 Keepalive Class, Types, and Limitations

Class	Type	CSS Maximum	Concurrent Maximum
A (The CSS limits 2048 keepalives per Class A.)	ICMP	2048	2048
	HTTP-HEAD non-persistent	2048	2048
	SSL (Hello)	2048	2048
	TCP	2048	2048
B (The CSS limits 512 keepalives per Class B.)	FTP	256	32
	HTTP-GET persistent and non-persistent	256	32
	HTTP-HEAD persistent	256	32
	Script	256	16

Caution For an 11500 series CSS, do not configure more than 2048 total keepalives, including a total of 512 Class B keepalives. Any services assigned to keepalives over the supported total number will not be eligible for content rule selection.

Regardless of the number of services you assign to a global keepalive through the **(config-service) keepalive type named** command, the CSS always counts it as one keepalive.

To access keepalive configuration mode, use the **keepalive** command from circuit, global, header-field-group, interface, and IP configuration modes. The prompt changes to (config-keepalive [*name*]). You can also use this command from keepalive mode to access another keepalive. For information about commands available in this mode, see the following commands.

Use the **no** form of this command to delete an existing keepalive.

keepalive *name*

no keepalive *existing_keepalive_name*

Syntax Description

name	Name of a new keepalive you want to create or of an existing keepalive. Enter an unquoted text string with no spaces and a maximum length of 31 characters. To see a list of existing keepalive names, enter: `keepalive ?`

Related Commands

show keepalive
(config-service) keepalive type named

(config-keepalive) active

To activate the keepalive you are configuring, use the **active** command. Activating a keepalive starts the sending of messages to the keepalive IP address.

active

Related Commands

show keepalive
(config-keepalive) ip address
(config-keepalive) suspend

(config-keepalive) description

To specify the description for the keepalive, use the **description** command. Use the **no** form of this command to delete the description.

description "*keepalive_description***"**

no description

Syntax Description

"*keepalive_description*"	The description for the keepalive. Enter a quoted text string with a maximum length of 64 characters including spaces.

Related Commands

show keepalive

(config-keepalive) frequency

To specify the frequency to send keepalive messages to the IP address, use the **frequency** command. Use the **no** form of this command to reset the frequency to its default value of 5.

frequency *frequency*

no frequency

Syntax Description

frequency	Time in seconds between sending keepalive messages to the IP address. Enter an integer from 2 to 255. The default is 5.

Usage Guidelines

For script keepalives, configure a higher frequency time value. A time interval of over 10 seconds ensures that the script keepalive has enough time to finish. Otherwise, state transitions may occur more often than usual.

If you configure more than 16 keepalives, the CSS automatically adjusts the keepalive frequency time to a value that best fits the resource usage. Note that this adjustment also affects the keepalive retry period value by adjusting that value to a number that is one-half the adjusted frequency time. If this occurs, you may observe in the running-configuration that your previously set keepalive frequency and retry-period times change to a different value, as determined by the CSS.

The timeout for a keepalive is related to the configured keepalive frequency. In WebNS 5.1 and earlier versions, the timeout is equivalent to the keepalive frequency. In version 5.2, the timeout is one second less than the keepalive frequency.

Related Commands

show keepalive

(config-keepalive) hash

To specify the MD5 hash for the keepalive, use the **hash** command. The keepalive process compares the hash with the computed hash of all HTTP GET responses. A successful comparison results in the keepalive maintaining an ALIVE state. Use the **no** form of this command to clear the hash value.

hash “*object*”

no hash

Syntax Description

“*object*”	Object containing the MD5 hash in hexadecimal value for the keepalive. To determine the value for the hash, use the **show keepalive** command after you configure the keepalive without the hash option. Enter a quoted text string up to 32 characters.

Related Commands

show keepalive

(config-keepalive) http-rspcode

To specify the response code expected from the HTTP daemon when a CSS issues a HEAD request, use the **http-rspcode** command. This command could be helpful for checking a redirect by specifying the 302 response code, or by triggering another non-200 HTTP response code. Use the **no** form of the command to reset the response code to its default value of 200.

http-rspcode *value*

no http-rspcode

Syntax Description

value	Response code expected from the HTTP daemon. Enter the response code as an integer from 100 to 999. The default is 200.

Related Commands **(config-service) keepalive http-rspcode**

(config-keepalive) ip address

To specify the IP address where the keepalive messages are sent, use the **ip address** command.

ip address *ip_address*

Syntax Description

ip_address	IP address for the keepalive. Enter this address in dotted-decimal notation (for example, 192.168.11.1).

Related Commands **(config-keepalive) port**

(config-keepalive) logging

To specify where to either capture the output from a script keepalive or turn off script keepalive logging, use the **logging** command.

logging [*log_filename*|**none**]

Syntax Description

log_filename	Name of the log file where you want to capture the script output. This file is saved in the log directory on the CSS disk. Enter an unquoted text string with a maximum of 32 characters.
none	Turns off script keepalive logging.

Related Commands **(config-keepalive) type**

(config-keepalive) maxfailure

To specify how many times the IP address can fail to respond to a keepalive message before being considered dead, use the **maxfailure** command. Use the **no** form of this command to reset the maximum failure number to its default value of 3.

maxfailure *number*

no maxfailure

Syntax Description

number	Maximum failure number. Enter an integer from 1 to 10. The default is 3.

(config-keepalive) method

To specify the HTTP keepalive method assigned to the keepalive, use the **method** command.

method [**get**|**head**]

Syntax Description

get	Specifies the get method. The CSS issues a HTTP GET method to the service, computes a hash value on the page, and stores the hash value as a reference hash. Subsequent GETs require a 200 OK status (HTTP command completed OK response) and the hash value to equal the reference hash value. If the 200 OK status is not returned, or if the 200 OK status is returned but the hash value is different from the reference hash value, the CSS considers the service down. When you specify the content information of an HTTP Uniform Resource Identifier (URI) for an HTTP keepalive, the CSS calculates a hash value for the content. If the content information changes, the hash value no longer matches the original hash value and the CSS assumes that the service is down. To prevent the CSS from assuming that a service is down due to a hash value mismatch, specify the **method** as **head**.

head	Specifies the head method (default). The CSS issues a HTTP HEAD method to the service and a 200 OK status is required. The CSS does not compute a reference hash value for this type of keepalive. If the 200 OK status is not returned, the CSS considers the service down.

Usage Guidelines

If you change the keepalive method on an active service, suspend and reactivate the service for the change to take effect.

(config-keepalive) no

To negate a command or set it to its default, use the **no** command. For information on general **no** commands you can use in this mode, see the general **no** command. The following options are available in keepalive mode.

Syntax Description

no acl *index*	Deletes an existing ACL
no description	Clears the keepalive description
no frequency	Resets the keepalive frequency to its default of 5 seconds
no hash	Clears the MD5 hash object value
no http-rspcode	Resets the response code to its default value of 200
no keepalive *name*	Deletes an existing keepalive
no maxfailure	Resets the keepalive maximum number of failures to its default setting of 3
no owner *name*	Deletes an existing owner
no port	Resets the keepalive port number to its default setting based on the configured keepalive type
no retryperiod	Resets the keepalive retry period to its default of 5 seconds
no uri	Clears the keepalive content information of the URI

(config-keepalive) port

To specify the port number for the keepalive, use the **port** command. Use the **no** form of this command to reset the port to the default based on the configured keepalive type.

port *number*

no port

Syntax Description

number	Port number associated with the keepalive. Enter the number as an integer from 0 to 65535. The default is based on the keepalive type. If the keepalive type is: • Not configured, the default port number is 0 • HTTP or TCP, the default port number is 80 • FTP, the default port number is 21

Related Commands

(config-keepalive) ip address

(config-keepalive) retryperiod

To specify the retry period to send messages to the keepalive IP address, use the **retryperiod** command. Use the **no** form of this command to reset the retry period to its default value of 5.

retryperiod *period*

no retryperiod

Syntax Description

period	Time in seconds between sending retry messages to the keepalive IP address. Enter an integer from 2 to 255. The default is 5.

Usage Guidelines

When a service has failed to respond to a given keepalive message (the service has transitioned to the dying state), the retry period specifies how frequently the CSS tests the service to see if it is functional.

(config-keepalive) suspend

To deactivate the keepalive, use the **suspend** command.

suspend

Related Commands

show keepalive
(config-keepalive) active

(config-keepalive) tcp-close

To specify the keepalive to close a TCP socket with a FIN or a RST, use the **tcp-close** command.

tcp-close [**fin**|**rst**]

Syntax Description

fin	Specifies that the keepalive closes the TCP socket with a FIN rather than a RST.
rst	Specifies that the keepalive closes the TCP socket with a RST (default).

Usage Guidelines

By default and in compliance with RFC 1122, the CSS sends a reset (RST) to close the socket on a server port for TCP keepalives. A RST is faster than a FIN, because a RST requires only one packet, while a FIN can take up to four packets. If your servers require a graceful closing of a socket using a FIN, use the **tcp-close fin** command.

The **tcp-close fin** and service mode **keepalive tcp-close** fin commands may be applied to a total of 100 TCP keepalives.

Related Commands

(config-keepalive) type

(config-keepalive) type

To specify the type of keepalive message assigned to the keepalive, use the **type** command.

type [**ftp** *ftp_record*|**http** {**non-persistent**}|**icmp**|**script** *script_name* {"*arguments*"} {**use-output**}|**ssl**|**tcp**]

Syntax Description

ftp *ftp_record*	The keepalive method by which the CSS logs in to an FTP server as defined in the FTP record file. Provide the name of an existing FTP record for the FTP server. Enter an unquoted text string with no spaces. To create an FTP record, use the **(config) ftp-record** command.
http {**non-persistent**}	An HTTP index page request. By default, HTTP keepalives attempt to use persistent connections. To disable this behavior, include the **non-persistent** keyword.
icmp	An ICMP echo message (default).
script *script_name*	The script keepalive to be used by the service. The script is played every time the keepalive is entered. Enter the name of the script keepalive. To view a list of scripts, enter: `type script ?`
"*arguments*"	Arguments to pass into the keepalive script. Enter a quoted text string with a maximum of 128 characters including spaces.
use-output	(Optional) Allows the script to parse the output for each executed command. This keyword allows the use **grep** and file direction within a script. By default, the script does not parse the output. You can configure only 16 keepalives that use script output.
ssl	SSL HELLO keepalives for this service. Use this keepalive for all backend services supporting SSL. The CSS sends a client HELLO to connect the SSL server. After the CSS receives a HELLO from the server, the CSS closes the connection with a TCP RST. When the CSS is using an SSL module, use the keepalive type of **none**. The SSL module is an integrated device in the CSS and does not require the use of keepalive messages for the service.
tcp	TCP connection handshake request.

Usage Guidelines

To enable the HTTP-HEAD optimization, use the **type http non-persistent** command.

The CSS divides the keepalive types into two categories, Class A and Class B keepalives. The CSS supports a maximum of 2048 Class A keepalives. The CSS supports a maximum of 512 Class B keepalives. Table 2-1 lists the keepalive types in each class, the maximum number of each type, and the maximum number of each keepalive type that can execute concurrently.

Table 2-2 Keepalive Class, Types, and Limitations

Class	Type	CSS Maximum	Concurrent Maximum
A	ICMP	2048	2048
(The CSS limits 2048 keepalives per Class A.)	HTTP-HEAD non-persistent	2048	2048
	SSL (Hello)	2048	2048
	TCP	2048	2048
B	FTP	256	32
(The CSS limits 512 keepalives per Class B.)	HTTP-GET persistent and non-persistent	256	32
	HTTP-HEAD persistent	256	32
	Script	256	16

Caution For an 11500 series CSS, do not configure more than 2048 total keepalives, including a total of 512 Class B keepalives. Any services assigned to keepalives over the supported total number will not be eligible for content rule selection.

When the CSS is using an SSL module, use the keepalive type of **none**. The SSL module is an integrated device in the CSS and does not require the use of keepalive messages for the service.

The **tcp-close fin** and service mode **keepalive tcp-close** fin commands may be applied to a total of 100 TCP keepalives.

(config-keepalive) uri

To specify the content information for an HTTP global keepalive, use the **uri** command. Use the **no** form of this command to clear the URI assigned to the keepalive.

uri "*uri*"

no uri

Syntax Description

"*uri*"	Content information for the HTTP keepalive URI. Enter the content information for a URI as a quoted text string with a maximum length of 64 characters. Do not include the host information in the string. The CSS derives the host information from the service IP address and the keepalive port number.

Usage Guidelines

When you specify the content information for an HTTP keepalive, the CSS calculates a hash value for the content. If the content information changes, the hash value no longer matches the original hash value and the CSS assumes that the service is down. To prevent the CSS from assuming that a service is down due to a hash value mismatch, specify the **keepalive method** as **head**. If you specify a Web page with changeable content and do not specify the keepalive method as **head**, you must suspend and reactivate the service each time the content information changes.

NQL Configuration Mode Commands

NQL configuration mode allows you to configure a network qualifier list (NQL). An NQL is a collection of subnet and host IP addresses that you can assign to an ACL clause, instead of creating a clause for each address. You can configure a maximum of 512 networks to an NQL and a maximum of 512 NQLs on the CSS.

To access NQL configuration mode, use the **nql** command from any configuration mode except boot, group, header-field-group, RMON alarm, RMON event, and RMON history configuration modes. The prompt changes to (config-nql [*name*]). You can also use this command from NQL mode to access another NQL. For information about commands available in this mode, see the following commands.

In global configuration mode, use the **no** form of this command to delete an existing NQL.

nql *nql_name*

(config) no nql *existing_nql_name*

Syntax Description

nql_name	Name of a new NQL you want to create or of an existing list. Enter an unquoted text string with no spaces and a maximum length of 31 characters. To see a list of existing NQL names, enter: `nql ?`

Related Commands

show nql
(config-acl) clause

(config-nql) description

To provide a description for the network qualifier list (NQL), use the **description** command.

description "*text***"**

Syntax Description

“*text*”	Description for the NQL. Enter a quoted text string with a maximum length of 63 characters.

(config-nql) ip address

To add an IP address to the list of networks supported by the NQL, use the **ip address** command. You can configure a maximum of 512 networks to an NQL. Use the **no** form of this command to remove an IP address from the NQL.

ip address *ip_address*[**/***subnet_prefix***|** *subnet_address*] {**“***description***”**} {**log**}

no ip address *ip_address*[**/***subnet_prefix***|** *subnet_address*]

Syntax Description

ip_address	Destination network prefix. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
subnet_prefix	IP subnet mask prefix length in CIDR bit count notation (for example, /24). The valid prefix length range is from 8 to 32.
subnet_address	IP subnet mask IP address in dotted-decimal notation (for example, 255.255.255.0).
“*description***”**	(Optional) Description for the IP address. Enter a quoted text string with a maximum length of 63 characters.
log	(Optional) Logs an event involving an NQL. You must also enable global NQL logging by using the **(config) logging subsystem nql level debug-7** command. If you do not enter this option, the event is not logged.

Related Commands **show nql**

Owner Configuration Mode Commands

Owner configuration mode allows you to configure an owner. An owner is an entity that owns web content and uses the CSS to manage access to that content through content rules. Up to 255 owners can use a single CSS and each owner has a configurable profile.

To access owner configuration mode, use the **owner** command from any mode except ACL, boot, group, and RMON alarm, event, and history configuration modes. The prompt changes to (config-owner [*owner_name*]). You can also use this command in owner mode to access another owner. For information about commands available in this mode, see the following commands.

Use the **no** form of this command to delete an existing owner.

owner *owner_name*

no owner *existing_owner_name*

Syntax Description

owner_name	Name of a new owner you want to create or the name of an existing owner. Enter an unquoted text string with no spaces and a maximum length of 31 characters. To see a list of existing owner names, enter: `owner ?`

(config-owner) address

To enter the address for the owner of the web hosting service, use the **address** command. Use the **no** form of this command to delete an address for the owner.

address "*address*"
no address

Syntax Description

"*address*"	Street address for the owner. Enter a quoted text string with a maximum length of 128 characters.

(config-owner) billing-info

To enter billing information about the owner providing the web hosting service, use the **billing-info** command. Use the **no** form of this command to delete the billing information.

billing-info “*information*”

no billing-info

Syntax Description

“*information*”	Billing information about the owner. Enter a quoted text string with a maximum length of 128 characters.

(config-owner) case

To define whether the matching of content requests to the owner’s rules is case-sensitive, use the **case** command.

case insensitive|sensitive

Syntax Description

insensitive	Matching of the owner’s rules is not case-sensitive. Uppercase and lowercase characters in content requests are ignored.
sensitive	Matching of the owner’s rules is case-sensitive. Uppercase and lowercase characters in content requests are used as part of the matching criteria.

(config-owner) content

To access content configuration mode and configure a content rule, use the **content** command. Use the **no** form of this command to an existing content rule.

content *content_rule_name*

no content *content_rule_name*

Syntax Description

content_rule_name	Name of a new content rule you want to create or an existing rule you want to modify. Enter an unquoted text string with no spaces and a maximum length of 31 characters. Enter an existing name exactly. To see a list of existing rules, enter: **`content ?`**

Usage Guidelines

When you use the **content** command to access this mode, the prompt changes to (config-owner-content [*owner-rule*]). For information about commands available in this mode, see the commands in the "Content Configuration Mode Commands" section.

Related Commands

show rule
(config) service

(config-owner) dns

To set the peer DNS exchange policy for the owner, use the **dns** command. The default DNS exchange policy for the owner is none; the owner is hidden from the CSS peer. Use the **no** form of this command to reset the DNS exchange policy for the owner to its default setting of none.

dns [**accept**|**push**|**both**]

no dns

Syntax Description

accept	Accepts all content rules proposed by the CSS peer
push	Advertises the owner and pushes all content rules onto the CSS peer
both	Advertises the owner and pushes all content rules onto the CSS peer, and accept all content rules proposed by the CSS peer

Related Commands

(config) dns
(config) dns-server
(config-owner-content) add

(config-owner) dnsbalance

To determine where to resolve a request for a domain name into an IP address, use the **dnsbalance** command. Use the **no** form of this command to reset the DNS load-balancing method to its default setting of **roundrobin**.

dnsbalance leastloaded|preferlocal|roundrobin

no dnsbalance

Syntax Description

leastloaded	Resolves the request to the least-loaded local or remote domain site. The CSS first compares load numbers. If the load number between domain sites is within 50, the CSS compares their response times. The site with the faster response time is considered the least-loaded site. For the **leastloaded** option to work properly, all domain sites must be running a minimum of CSS software version 3.02.

preferlocal	Resolves the request to a local VIP address. If all local systems exceed their load threshold, the CSS chooses the least-loaded remote system VIP address as the resolved address for the domain name.
roundrobin	Resolves the request by evenly distributing the load to resolve domain names among content domain sites, local and remote. The CSS does not include sites that exceed their local load threshold.

Usage Guidelines

The DNS load-balancing method configured for the owner applies to all of its content rules. To set a different method to a specific content rule, use the **(config-owner-content) dnsbalance** command.

Related Commands

(config-owner-content) dnsbalance

(config-owner) email-address

To enter an email address for the owner providing the Web hosting service, use the **email-address** command. Use the **no** form of this command to delete the e-mail address for the owner.

email-address "*information***"**
no email-address

Syntax Description

"*information***"**	E-mail address for the owner. Enter a quoted text string with a maximum length of 64 characters.

(config-owner) no

To negate a command or set it to its default, use the **no** command. For information on general **no** commands you can use in this mode, see the general **no** command. The following options are available in owner mode.

Syntax Description

no acl *index*	Deletes an ACL
no address	Deletes the address for the owner
no billing-info	Deletes the billing information for the owner
no content *content_rule_name*	Deletes an existing content rule
no dns	Resets the DNS exchange policy for the owner to its default setting of none
no dnsbalance	Resets the DNS load-balancing method for the owner to its default setting of round robin
no email-address	Deletes the e-mail address for the owner
no owner *owner_name*	Deletes an existing owner

(config-owner) show owner

To display owner configuration information and statistics for the current owner, use the **show owner** command. An owner is an entity that owns web content and is using the CSS to manage access to that content.

show owner {**statistics**}

Syntax Description

statistics	(Optional) Displays the statistics for the current owner

Usage Guidelines

The **show owner** command without an option displays configuration information only.

Examples

To display configuration information for the owner, enter:

```
#(config-owner (test.com) show owner
```

To display statistics for the owner, enter:

```
#(config-owner (test.com) show owner statistics
```

For output descriptions of the **show owner** command, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config-owner) address
(config-owner) billing-info
(config-owner) case
(config-owner) dns
(config-owner) email-address

(config-owner) zero

To set the content rule counters to zero, use the **zero** command.

zero all

Related Commands

show rule

Content Configuration Mode Commands

Content configuration mode allows you to configure a content rule. In the CSS, content refers to web content that exists as an object or set of objects. Content rules:

- Describe the content available at services
- Tell the CSS where the content physically resides, whether local or remote
- Specify how to treat requests for the content

Content rules are hierarchical. If a request for content matches more than one rule, the characteristics of the most specific rule apply to the flow.

To access content mode, use the **content** command from owner mode. The prompt changes to (config-owner-content [*owner-rule*]). You can also use this command in content mode to access another content rule. For information about commands available in this mode, see the following commands.

Use the **no** form of this command to delete an existing content rule.

(config-owner) content *name*

no content *content_rule_name*

Syntax Description

name	Name of a new content rule you want to create or an existing rule you want to modify. Enter an unquoted text string with no spaces and a maximum length of 31 characters. Enter an existing name exactly. To see a list of existing rules, enter: `content ?`

(config-owner-content) active

To activate the content rule you are configuring, use the **active** command. Activating a content rule includes it in CSS content rule matching and load-balancing decisions.

active

Usage Guidelines

Once a content rule is activated, the following commands cannot be changed for the active content rule: **port**, **protocol**, **balance**, **dnsbalance**, **header-field-rule**, and **url**. In addition, you cannot remove the last remaining service from the content rule. If you need to make modifications to an active content rule, you must first suspend it.

Related Commands

show rule
show running-config
(config-owner-content) suspend

(config-owner-content) add

To add an existing service to the content rule or to specify a DNS name that maps to the content rule, use the **add** command. The options for this command are:

- **add dns** - Specifies a DNS name that maps to the content rule
- **add location-service** - Adds a service to a content rule as a location service
- **add service** - Adds an existing service to the content rule

For more information on these options, see the following commands.

add dns

To specify a DNS name that maps to the content rule, use the **add dns** command.

add dns *dns_name* {*ttl_value*}

Syntax Description

dns_name	DNS name mapped to the content rule. Enter the name as a lower-case unquoted text string with no spaces and a maximum length of 63 characters.
ttl_value	(Optional) Time-to-Live (TTL) value in seconds. This value sets how long the DNS client remembers the IP address response to the query. Enter a value of 0 to 255. The default is 0.

Command Modes

Owner-Content

Usage Guidelines

To add a TTL value to an existing DNS name, remove the name and then readd it with the TTL value.

Use the **remove dns** command to remove a DNS name mapped to the content rule.

Related Commands

show rule
(config) dns
(config) dns-server
(config-owner-content) add
(config-owner) dns
(config-owner-content) remove

add location service

To add a destination service or a redirect service to a content rule that a CSS uses to locate the CSS where the client was originally stuck, use the **add location-service** command.

add location-service *service_name*

remove location-service *service_name*

Syntax Description

service_name	Name of an existing destination service or redirect service that you want to use as a location service. Enter the name as a lowercase, unquoted text string with no spaces and a maximum of 31 characters.

Command Modes

Owner-Content

Usage Guidelines

Use the **add location-service** command with the **location-cookie** and **cookie-domain** commands to ensure that a client returns to the original server after a DNS re-resolution sends the client to a new server.

You can configure a maximum of 10 location services; either destination services or redirect services. These services do not count toward the 64-service maximum per content rule and do not participate in the load-balancing algorithm of the content rule. For more information on the location cookie feature, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config-owner-content) add
(config-owner-content) remove
(config-owner-content) no
(config-owner-content) cookie-domain

add service

To add an existing service to the content rule, use the **add service** command. Adding a service includes it in the resource pool that the CSS uses for load-balancing requests for the content governed by the rule.

add service *service_name* **weight** *number*

Syntax Description

service_name	Name of the existing service. Enter the name as a case-sensitive unquoted text string with no spaces.
weight	Allows you to assign a weight to the service used when you configure weighted roundrobin load balancing on the content rule. When you assign a higher weight, the CSS redirects more requests to the service. To configure load balancing, see the **(config-owner-content) balance** command.
number	Weight for the service. Enter a number from 1 to 10. The default is the weight configured for the service through the **(config-service) weight** command. By default, all services have a weight of 1.

Command Modes

Owner-Content

Usage Guidelines

Use the **remove service** command to remove a service.

To perform a graceful shutdown of an overloaded service or to take a service offline gracefully for maintenance, when you specify a weight of 0 no new connections, except the connections for existing sticky sessions, will be directed to the service. Over time, as existing sticky sessions complete, the load on the service begins to diminish. Changing the weight to a value between 1 and 10 causes the service to be brought back into rotation for all load-balancing methods.

Note the following guidelines for the **weight** option when configuring the CSS for graceful shutdown:

- If you do not have a weighted roundrobin load-balancing method specified for the content rule command in service mode. Using the **add service** command in content mode has no affect on the service weights and cannot be used to gracefully shut down the service.
- Weight is not configurable on content rule basis for primary or secondary sorry servers. Sorry servers can be gracefully shut down only by setting the weight to 0 in service mode.
- Cisco Systems recommends that you use the **sticky-inact-timeout** command to specify an inactivity timeout period if you use advanced load-balancing methods such as **sticky-srcip** or **sticky-srcip-dstport** in conjunction with graceful shutdown. Once the sticky entries timeout as a result of inactivity, the connection count to the shutdown service decreases.

Related Commands

show rule
(config) service
(config-owner-content) balance
(config-owner-content) remove
(config-service) weight

(config-owner-content) advanced-balance

To specify an advanced load-balancing method for the content rule, including stickiness, use the **advanced-balance** command. A content rule is "sticky" when additional sessions from the same user or client are sent to the same service as the first connection, overriding normal load balancing. By default, the advanced balancing method is disabled. Use the **no** form of this command to disable the advanced balancing method.

advanced-balance arrowpoint-cookie|cookies|cookieurl|none |sip-call-id|sticky-srcip|sticky-srcip-dstport|ssl|url|wap-msisdn

no advanced-balance

Syntax Description

arrowpoint-cookie	Enables the content rule to stick the client to the server based on the unique service identifier information of the selected server in the ArrowPoint-generated cookie. Configure the service identifier by using the **(config-service) string** command. You do not need to configure string match criteria. For information on configuring the ArrowPoint-generated cookie, see the **(config-owner-content) arrowpoint-cookie** command. You can use this option with any Layer 5 content rule.

cookies

Enables the content rule to stick the client to the server based on the configured string found in the HTTP cookie header. You must specify a port in the content rule to use this keyword. The CSS will then spoof the connection. A content rule with a sticky configuration set to **advanced-balance cookies** requires all clients to enable cookies on their browser.

When a client makes an initial request, the client does not have a cookie. But once the client goes to a server that is capable of setting cookies, the client receives the cookie from the server. Each subsequent request contains the cookie until the cookie expires. A string in a cookie can be used to stick a client to a server. The service mode **string** command enables you to specify where the CSS should locate the string within the cookie.

The CSS processes the cookie using:

- An exact match that you set up when you configure the services
- Data for a hash algorithm

cookieurl	Same as **advanced-balance cookies**, but if the CSS cannot find the cookie header in the HTTP packet, this type of failover looks up the URL extensions (that is, the portion after the "?" in the URL) based on the same string criteria. You can use this option with any Layer 5 HTTP content rule. This option is useful if a Microsoft IIS web server is used with Cookie Munger, that dynamically places the session state information in the cookie header or URL extension depending on whether the client can accept cookies. Some client applications do not accept cookies. When a site depends upon the information in the cookie, administrators sometimes modify the server application so that it appends the cookie data to the parameters section of the URL. The parameters typically follow a "?" at the end of the main data section of the URL. Advanced-balanced **cookieurl** sticks a client to a server based on locating the configured string: • In the cookie, if a cookie exists • In the parameters section of the URL if no cookie exists The string can either be an exact match or be hashed.
none	Disables the advanced-balancing method for the rule (default).
sip-call-id	Enables the content rule to stick a client to a server based on the Session Initiation Protocol (SIP) call ID. The application type must be **sip** for the content rule, and the protocol must be UDP. For more information, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.
sticky-srcip	Enables the content rule to stick a client to a server based on the client IP address, also known as Layer 3 stickiness. You can use this keyword with Layer 3, 4, or 5 content rules.

sticky-srcip-dstport	Enables the content rule to stick a client to a server based on both the client IP address and the server destination port number, also known as Layer 4 stickiness. You can use this keyword with Layer 4 or 5 content rules.
ssl	Enables the content rule to stick the client to the server based on the Secure Sockets Layer (SSL) version 3 session ID assigned by the server. The application type must be SSL for the content rule. You must specify a port in the content rule to use this keyword. The CSS will then spoof the connection. Sites where encryption is required for security purposes often use SSL. SSL contains session IDs. The CSS can use these session IDs to stick the client to a server. In order for the CSS to successfully provide SSL stickiness, the application must be using SSL version 3 session IDs. Sticky SSL uses the sticky table. If you are concerned about the number of concurrent sessions, and not concerned about security, you should consider using **cookies**, **cookieurl**, or **url**. In addition, you may need to enter the **ssl-l4-fallback disable** command when you want to disable the CSS from inserting the Layer 4 hash value, based on the source IP address and destination address pair, into the sticky table. This may be necessary in a lab environment when testing SSL with a small number of clients and servers, where some retransmissions might occur. In this case, you would not want to use the Layer 4 hash value because it will skew the test results. Do not enter the **(config) ssl-l4-fallback disable** if SSL version 2 is in use on the network.

url

Enables the content rule to stick a client to a server based on a configured string found in the URL of the HTTP request. You must specify a port in the content rule to use this option. The CSS will then spoof the connection. Similar to advanced-balanced **cookie**, advanced-balanced **url** may use either an exact match method or a hash algorithm. The string can exist anywhere in the URL.

To use stickiness based on SSL version 3 session ID, configure an SSL Layer 5 rule for the service:

- Set the port to 443 with the **(config-owner-content) port** command.
- (Optional) Set the URL to /* with the **(config-owner-content) url** command.
- Enable the content rule to be sticky based on SSL with the **(config-owner-content) advanced-balance ssl** command.
- Specify the SSL application type with the **(config-owner-content) application** command.

You cannot configure both **url urql** and **application sip** or **url urql** and **application ssl** on the same content rule.

wap-msisdn	Enables a Layer 5 content rule to stick a client to a server based on the MSISDN header of the HTTP request. MSISDN is the header field for wireless clients using the Wireless Application Protocol (WAP). If the CSS finds the MSISDN header in an HTTP request, the CSS generates a key based on the value in the header field. The CSS uses the key to look up an entry in the sticky table. If the entry exists, the CSS sends the client to the sticky server indicated by the table entry. If the entry does not exist, the CSS creates a new sticky entry, hashes the MSISDN value into a key, and saves the key in the entry. If the CSS does not find the MSISDN header, the CSS load balances the client request based on the balance method configured through the **(config-owner-content) balance** command. You can use the **advanced-balance wap-msisdn** command alone or with the MSISDN header field type. See the **(config-header-field-group) header-field** command.

Command Modes

Owner-Content

Related Commands

show rule
(config) ssl-l4-fallback
(config-owner-content) sticky-mask
(config-owner-content) string range

(config-owner-content) application

To specify the application type associated with the content rule, use the **application** command. The application type enables the CSS to correctly interpret the data stream matching the content rule and parse them. Otherwise, the data stream packets are rejected. Use the **no** form of this command to reset the application type to its default setting of HTTP.

application *type*

no application

Syntax Description

type	Application type. Enter one of the following: • **bypass** - Bypasses the matching of the content rule and send the request directly to the origin server • **http** (default) - Processes HTTP data streams • **ftp-control** - Processes FTP data streams • **realaudio-control** - Processes RealAudio Control data streams • **sip** - Processes Session Initiation Protocol (SIP) data streams • **ssl** - Processes Secure Sockets Layer (SSL) protocol data streams

Usage Guidelines

You cannot configure both **url urql** and **application ssl** for the same content rule.

Define an application type for nonstandard ports.

When configuring Layer 5 content rules for an application other than HTTP, enter the appropriate **application** type to enable the Layer 5 rule to function.

A Layer 5 content rule supports the HTTP CONNECT, GET, HEAD, POST, PUSH, and PUT methods. The CSS recognizes and forwards these HTTP methods directly to the destination server in a transparent caching environment.

The CSS does not load balance these HTTP methods: RFC-2068: OPTIONS, TRACE; RFC-2518: PROPFIND, PROPPATCH, MKCOL, MOVE, LOCK, UNLOCK, COPY, DELETE.

(config-owner-content) arrowpoint-cookie

To configure the ArrowPoint cookie path and expiration, use the **arrowpoint-cookie** command.

- **arrowpoint-cookie browser-expire** - Allows the browser to expire the cookie
- **arrowpoint-cookie expiration** - Sets an expiration time which the CSS compares with the time associated with the cookie
- **arrowpoint-cookie expire-services** - Expires the service information when the cookie expires
- **arrowpoint-cookie name** - Configures a unique 31-character cookie identifier
- **arrowpoint-cookie path** - Sets the cookie path to a configured path

For more information about these options, see the following commands.

Usage Guidelines

The CSS transparently generates the ArrowPoint cookie for the client, the client stores it and returns it in subsequent requests, and the CSS later uses it to maintain the client-server stickiness. The cookie contains the sticky information itself and does not refer to a sticky table.

If you configure the arrowpoint-cookie method in the content rule, the CSS always checks for the existence of the ArrowPoint cookie when it receives a client request. If this cookie does not exist, the CSS performs a server load balance and generates an ArrowPoint cookie. When the CSS finds the cookie in the client request, it unscrambles the cookie data and then validates it. Then, the CSS checks the cookie expiration time. If the cookie has expired, the CSS sends a new cookie the information about the server where the client was stuck. This will allow for the appearance of an uninterrupted connection.

If the cookie format is valid, the CSS ensures the consistency between the cookie and the CSS configuration. When all the validations are passed, the CSS forwards the client request to the server indicated by the server identifier. Otherwise, the CSS treats the request as an initial request.

If the cookie is valid but the sticky server is not available, the CSS uses the sticky-serverdown-failover configuration to handle the request. If the configured sticky-serverdown-failover type is **balance**, then the CSS treats the client request as an initial client request without the ArrowPoint cookie, runs through the load balance algorithm to choose a server, and then redirects with a generated ArrowPoint cookie. If the sticky-serverdown-failover type is **redirect**, the CSS redirects the request to the specified URL.

Related Commands

show rule
(config-owner-content) advanced-balance

arrowpoint-cookie browser-expire

To allow the browser to expire the ArrowPoint cookie based on the expiration time, use the **arrowpoint-cookie browser-expire** command. To configure the expiration time, see the **arrowpoint-cookie expiration** command. Use the **no** form of this command to allow the CSS to expire the cookie.

arrowpoint-cookie browser-expire

no arrowpoint-cookie browser-expire

Command Modes

Owner-Content

Usage Guidelines

When the cookie expires, all sticky information is lost.

Related Commands

arrowpoint-cookie expiration

arrowpoint-cookie expiration

To set the cookie duration time which the CSS compares with the time associated with the ArrowPoint cookie, use the **arrowpoint-cookie expiration** command. When the cookie time exceeds the duration time, the CSS expires the cookie. To allow the browser to expire the cookie, use the **arrowpoint-cookie browser-expire** command. Use the **no** form of this command to expire the cookie when you close the browser.

arrowpoint-cookie expiration *dd***:***hh***:***mm***:***ss*

no arrowpoint-cookie expiration

Syntax Description

dd	Number of days. Valid numbers are from 00 to 99.
hh	Number of hours. Valid numbers are from 00 to 99.
mm	Number of minutes. Valid numbers are from 00 to 99.
ss	Number of seconds. Valid numbers are from 00 to 99.

Command Modes

Owner-Content

Usage Guidelines

If the cookie has expired, the CSS sends a new cookie that includes the server where the client was stuck. This will allow for the appearance of an uninterrupted connection.

Examples

For example, to set an expiration time of 2 days, 3 hours, 21 minutes and 0 seconds, enter:

```
arrowpoint-cookie expiration 02:03:21:00
```

Related Commands

arrowpoint-cookie browser-expire

arrowpoint-cookie expire-services

To expire service information when the cookie expires before sending a new cookie, use the **arrowpoint-cookie expire-services** command. By default, when the cookie expires, the CSS sends a new cookie with the server information from the expired cookie. Use the **no** form of this command to reset the default behavior.

arrowpoint-cookie expire-services

no arrowpoint-cookie expire-services

Command Modes

Owner-Content

arrowpoint-cookie name

To configure a unique ArrowPoint cookie identifier, use the **arrowpoint-cookie name** command. Use the **no** form of this command to reset the cookie name to ARPT.

arrowpoint-cookie name *name*

no arrowpoint-cookie name

Syntax Description

name	Unique identifier for the ArrowPoint cookie. Enter an unquoted text string with a maximum of 31 alphanumeric characters. The default is ARPT.

Command Modes

Owner-Content

Usage Guidelines

When you configure a new cookie name on a content rule, the CSS no longer recognizes any pre-existing cookie name configured on that rule. Therefore, any existing stickiness is lost.

Related Commands

(config-owner-content) advanced-balance arrowpoint-cookie

arrowpoint-cookie path

To set the ArrowPoint cookie path to a configured path, use the **arrowpoint-cookie path** command. Otherwise, the CSS sets the default path attribute of the cookie to "/". Use the **no** form of this command to reset the cookie path to its default of "/".

arrowpoint-cookie path "*path_name***"**

no arrowpoint-cookie path

Syntax Description

path_name	Pathname where you want to send the cookie. Enter a quoted text string with a maximum of 99 characters. The default path of the cookie is "/".

Command Modes

Owner-Content

Related Commands

(config-owner-content) advanced-balance arrowpoint-cookie

(config-owner-content) balance

To specify the load-balancing algorithm for the content rule, use the **balance** command. Use the **no** form of this command to reset the load-balancing algorithm to its default setting of roundrobin.

balance aca|destip|domain|domainhash|leastconn|roundrobin|srcip|url |urlhash|weightedrr

no balance

Syntax Description

aca	ArrowPoint Content Awareness algorithm. The CSS correlates content request frequency with the server's cache sizes to improve cache hit rates for that server.
destip	Destination IP address division. The CSS directs all client requests with the same destination IP address to the same service.
domain	Domain name division. The CSS uses the domain name in the request URI to direct the client request to the appropriate service.
domainhash	Internal CSS hash algorithm based on the domain string. The CSS uses the algorithm to hash the entire domain string. Then, the CSS uses the hash result to choose the server.
leastconn	Least connections. The CSS chooses a running service that has the least number of connections. We do not recommend that you use UDP content rules with the leastconn load-balancing algorithm. The service connection counters do not increment and remain at 0 because UDP is a connectionless protocol. Because the counters remain at 0, the CSS will give inconsistent results.
roundrobin	Roundrobin algorithm (default).
srcip	Source IP address division. The CSS directs all client requests with the same source IP address to the same service.
url	URL division. The CSS uses the URL (omitting the leading slash) in the redirect URL to direct the client requests to the appropriate service.

urlhash	Internal CSS hash algorithm based on the URL string. The CSS uses the algorithm to hash the entire URL string. Then, the CSS uses the hash result to choose the server.
weightedrr	Weighted roundrobin algorithm. The CSS uses the roundrobin algorithm but weighs some services more heavily than others. You can configure the weight of a service when you add it to the rule.

Usage Guidelines

Before you can change the balance method, you must suspend the rule.

Related Commands

show rule
(config-owner-content) add service
(config-owner-content) advanced-balance
(config-owner-content) string operation

(config-owner-content) change service

To modify the weight of a service without removing the service from the content rule and adding it back again, use the **change service** command. Use the **no** form of this command to restore the weight to the default of 1.

change service *service_name* **weight** *number*

no change service *service_name*

Syntax Description

service_name	Name of the existing service. Enter the name as a case-sensitive unquoted text string with no spaces.
weight	Allows you to assign a weight to the service used when you configure weighted roundrobin load balancing on the content rule. When you assign a higher weight, the CSS redirects more requests to the service. To configure load balancing, see the **(config-owner-content) balance** command.

number	Weight for the service. Enter a number from 0 (graceful shutdown) to 10. The default is the weight configured for the service through the **(config-service) weight** command. By default, all services have a weight of 1.

Command Modes

Owner-Content

Usage Guidelines

Use the **remove service** command to remove a service.

To perform a graceful shutdown of an overloaded service or to take a service offline gracefully for maintenance, when you specify a weight of 0 no new connections, except the connections for existing sticky sessions, will be directed to the service. Over time, as existing sticky sessions complete, the load on the service begins to diminish. Changing the weight to a value between 1 and 10 causes the service to be brought back into rotation for all load-balancing methods.

Note the following guidelines for the **change service weight** command when configuring the CSS for graceful shutdown:

- If you do not have a weighted roundrobin load-balancing method specified for the content rule or do not have DFP specified for server load-balancing, use only the **weight** command in service mode. Using the **change service weight** command in content mode has no affect on the service weights and cannot be used to gracefully shut down the service.
- Weight is not configurable on a content rule basis for primary or secondary sorry servers. Sorry servers can be gracefully shut down only by setting the weight to 0 in service mode.
- Cisco Systems recommends that you use the **sticky-inact-timeout** command to specify an inactivity timeout period if you use advanced load-balancing methods such as **sticky-srcip** or **sticky-srcip-dstport** in conjunction with graceful shutdown. This action avoids decreasing the connection count to the shutdown service over time because the sticky entry remains in the table.

Related Commands

show rule
(config) service
(config-owner-content) add

(config-owner-content) balance
(config-owner-content) remove
(config-service) weight

(config-owner-content) cookie-domain

To configure a domain name for a location cookie, use the **cookie-domain** command. Use the **no** form of this command to remove the cookie domain.

cookie-domain *name*

no cookie-domain

Syntax Description

name	Name of the domain for the location cookie. Enter a quoted text string from 1 to 64 characters.

Usage Guidelines

The cookie domain name allows your browser to send the location cookie back to any site that ends with the domain name that you specify. For example, if you specify a cookie domain name of .xyz.com, the browser will send back the location cookie to all sites that end with .xyz.com, including site1.xyz.com, site2.xyz.com, and site3.xyz.com. For more information, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config-owner-content) no

(config-owner-content) dns-disable-local

To disable DNS on the content rule, use the **dns-disable-local** command. The CSS informs other CSSs through APP that the services related to the content rule are not available for DNS activities. However, the services remain active for other activities.

Use the **no** form of this command to enable DNS on the content rule.

dns-disable-local

no dns-disable-local

(config-owner-content) dnsbalance

To determine where to resolve a request for a domain name into an IP address, use the **dnsbalance** command. By default, the content rule will use the DNS load-balancing method assigned to the owner. Use the **no** form of this command to reset the DNS load-balancing method to its default setting of using the method assigned to the owner.

dnsbalance leastloaded|preferlocal|roundrobin|useownerdnsbalance

no dnsbalance

Syntax Description

leastloaded	Resolves the request to the least-loaded local or remote domain site. The CSS first compares load numbers. If the load number between domain sites is within 50, then the CSS compares their response times. The site with the faster response time is considered the least-loaded site. For the **leastloaded** option to work properly, all domain sites must be running a minimum of CSS software version 3.02.
preferlocal	Resolves the request to a local VIP address. If all local systems exceed their load threshold, the CSS chooses the least-loaded remote system VIP address as the resolved address for the domain name.
roundrobin	Resolves the request by evenly distributing the load to resolve domain names among content domain sites, local and remote. The CSS does not include sites that exceed their local-load threshold.
useownerdnsbalance	Resolves the request by using the DNS load-balancing method assigned to the owner. This is the default method for the content rule. If you do not implicitly set an owner method, the CSS uses the default owner DNS load-balancing method of round robin.

Usage Guidelines

Before you can change the DNS balance method, you must suspend the rule.

Related Commands

(config-owner) dnsbalance

(config-owner-content) failover

To define what will happen to content requests when a service fails or is suspended, use the **failover** command. For the CSS to use this setting, you must configure keepalive for each service. Use the **no** form of this command to reset the failover for the content rule to its default setting of linear. The linear failover method distributes the content requests to the failed service evenly between the remaining services.

failover bypass|next

no failover

Syntax Description

bypass	Bypasses all services and sends the content request directly to the origin service.
next	Sends the content requests to the service next to the failed service. The CSS selects which service is next to the failed one by referring to the order in which the services were configured.

Usage Guidelines

If you remove a service, the CSS rebalances the remaining services. The CSS does not use the **failover** command setting.

Before you can change the failover method, you must suspend the rule.

Related Commands

(config-owner-content) balance
(config-service) keepalive

(config-owner-content) flow-reset-reject

To enable the CSS flow manager subsystem to send a TCP RST (reset) frame when a flow for requested content is mapped to a destination IP address that is no longer reachable, use the **flow-reset-reject** command.

Use the **no** form of this command to reset the CSS back to the default state of not sending a TCP RST frame.

flow-reset-reject

no flow-reset-reject

Usage Guidelines

The **flow-reset-reject** command prevents a CSS client from hanging up and retransmitting when the request can never be serviced. For UDP flows, the command allows the CSS to purge the flow cache of the UDP flow so that another request gets remapped to a different IP address, if necessary, without attempting to use the previously mapped IP address. The **flow-reset-reject** command is applied on a per-content rule basis.

Related Commands

show rule

(config-owner-content) flow-timeout-multiplier

To specify the number of seconds for which an idle flow can exist before the CSS tears it down, use the **flow-timeout-multiplier** command. Use the **no** form of this command to restore the default timeout for the port type.

flow-timeout-multiplier *timeout-multiplier*

no flow-timeout-multiplier

Syntax Description

timeout-multiplier	Value that the CSS multiplies by 16 to calculate the flow timeout in seconds. Enter an integer from 0 to 65533. The default value depends on the port type (see the **show flow-timeout default** command). This default value applies only to flows that are created under the specified content rule. A value of zero (no timeout) instructs the CSS to never tear down the flow, resulting in a permanent flow and lost resources. This is equivalent to entering the global configuration **flow permanent port** command.

Usage Guidelines

We do not recommend that you set the **flow-timeout multiplier** command to 0 for UDP flows on Layer 3 and Layer 4 content rules. If the value is set to 0, the CSS does not clean up the resources for the UDP flows.

Use the **flow-timeout-multiplier** command to configure flow inactivity timeout values for TCP and UDP flows on a per-rule and per-source group basis. Note that this timeout value is *not* the frequency with which a CSS reclaims flow resources, but the time period that must elapse for an idle flow before the CSS cleans up the flow.

If you configure a source group with destination services for client source NATing, you need to configure the **flow-timeout multiplier** command only on the content rule. The CSS sets the same flow timeout value for flows in both directions. If you configure different timeout values on the content rule and on the source group, the CSS uses the timeout value configured on the content rule for both flows.

The CSS tears down the FTP control channel after 10 minutes of idle time. This teardown may occur during a file transfer if the transfer exceeds 10 minutes. Use the **flow-timeout-multiplier** command on the associated content rule to configure the timeout to a value that can accommodate the expected duration of the FTP file transfers.

To set up and keep track of flows, a CSS uses data structures called flow control blocks (FCBs). For optimal performance, the CSS reuses FCBs that are no longer needed by flows. Flow resource reclamation involves removing FCBs from the TCP and UDP lists.

Normally, flow cleanup occurs at a rate that is directly related to the overall number of flows that are currently active on a CSS. The fewer the number of active flows there are on a CSS, the less frequently the CSS reclaims FCBs. A CSS also cleans up long-lived TCP flows that have received a FIN or a RST, or whose timeout values have been met.

The CSS uses the following precedence when reclaiming flow resources:

1. If a flow matches on a content rule, the CSS checks for a user-configured timeout value and uses that value if one exists.
2. If the flow matches on a source group, the CSS checks for a user-configured timeout and uses that value if one exists.
3. If you have configured a permanent port using the (config) **flow permanent port** command, the CSS sets the flow timeout value to 0, which means that the flow should never time out.
4. If none of the previous conditions are met, the CSS uses the default timeout value for the protocol type.

Related Commands

show flow-timeout
(config) flow permanent

(config-owner-content) header-field-rule

To associate a header-field group to a content rule, and optionally assign a weight value to the header-field group, use the **header-field-rule** command. Use the **no** form of this command to remove the header-field group from the rule.

header-field-rule *name* {**weight** *number*}

no header-field-rule

Syntax Description

name	Name of the header-field group used with the content rule. To see a list of groups, enter: `header-field-rule ?`
weight *number*	(Optional) Assigns the weight to the header-field group. Enter a number from 0 to 1024. The default weight is 0.

Usage Guidelines

Use weights to allow the CSS to prefer one content rule over a similar content rule. For example, suppose that you want to load balance French clients to a specific server, and you also want to differentiate French Internet Explorer clients from French Netscape clients. If it is more important to direct the French clients to a specific server than to direct them to a server based on whether they are using Internet Explorer or Netscape, then you need to weight the “French” content rule higher than the “Internet Explorer/Netscape” content rule.

Before you can change the header-field group, you must suspend the rule.

Related Commands

show rule
(config) header-field-group

(config-owner-content) hotlist

To enable the hot list for the content rule and configure hot-list parameters, use the **hotlist** command. A hot list lists the most requested content during a user-defined period of time. The options for this content mode command are:

- **hotlist** - Enables the hot list for the content rule
- **hotlist interval** - Sets the hot-list refresh interval
- **hotlist size** - Sets the size of the hot list
- **hotlist threshold** - Sets the hot-list threshold
- **hotlist type** - Sets the hot-list type to hit count

For more information on these options, see the following commands.

hotlist

To enable the hot list for the content rule, use the **hotlist** command. Use the **no** form of this command to disable the hot list for the content rule.

hotlist

no hotlist

Command Modes

Owner-Content

hotlist interval

To set the hot-list refresh interval, use the **hotlist interval** command. Use the **no** form of this command to reset the hot-list interval for the content rule to its default setting of 1 minute.

hotlist interval *time*

no hotlist interval

Syntax Description

time	Interval, in minutes, for refreshing the hot list. Enter an integer from 1 to 60. The default is 1.

Command Modes Owner-Content

hotlist size

To set the size of the hot list, use the **hotlist size** command. Use the **no** form of this command to reset the hot-list size for the content rule to its default setting of 10 entries.

hotlist size *entries*

no hotlist size

Syntax Description

entries	Total number of hot-list entries that is maintained for the rule. Enter an integer from 1 to 100. The default is 10.

Command Modes Owner-Content

hotlist threshold

To set the hot-list threshold, use the **hotlist threshold** command. Use the **no** form of this command to reset the hot-list threshold for the content rule to its default setting of 0.

hotlist threshold *threshold*

no hotlist threshold

Syntax Description

threshold	Threshold below which an item is not considered hot. Enter an integer from 0 to 65535. The default is 0.

Command Modes

Owner-Content

hotlist type

To set the hot-list type, use the **hotlist type** command. Currently, the CSS supports only the hit count hot-list type, which is the default setting. Hit count is the number of times that the content is accessed. Use the **no** form of this command to reset the hot-list type for the content rule to its default setting of hitCount.

hotlist type hitCount

no hotlist type

Command Modes

Owner-Content

(config-owner-content) load-threshold

To set the normalized load threshold for the availability of each local service on the content rule, use the **load-threshold** command. When the service load metric exceeds this threshold, the local service becomes unavailable and is redirected to the remote services.

Use the **no** form of this command to reset the load threshold for the content rule to its default setting of 254.

load-threshold *threshold*

no load-threshold

Syntax Description

threshold	Maximum load. Enter an integer from 2 to 254. The default is 254, which is the maximum load. To view the load on services, enter: `show service`

(config-owner-content) location-cookie

To configure the NAME=VALUE cookie string and expiration time for the local site, use the **location-cookie** command. Use the **no** form of this command to remove the location cookie.

location-cookie name *text* **value** *text* {**expiration** *dd:hh:mm:ss*}

no location-cookie name

Syntax Description

name *text*	First part of the NAME=VALUE cookie string. Enter an unquoted text string from 1 to 31 characters.
value *text*	Second part of the NAME=VALUE cookie string. Enter an unquoted text string from 1 to 31 characters.
expiration *dd:hh:mm:ss*	(Optional) The expiration date and time of the Location Cookie. This value indicates to the client browser when the cookie will expire based on a relative time from cookie generation. Enter a date and time in the following format: • *dd* - Number of days. Valid numbers are from 00 to 99. • *hh* - Number of hours. Valid numbers are from 00 to 99. • *mm* - Number of minutes. Valid numbers are from 00 to 99. • *ss* - Number of seconds. Valid numbers are from 00 to 99.

Usage Guidelines

Use the **location-cookie** command with the **cookie-domain** command to stick a client to a particular server and return the client to that server if a new DNS resolution sends the client to a different server. You must configure standard services or redirect services as location services to ensure that the new CSS returns the client to the original CSS. In addition, in a source group you must configure as destination services any standard services that you configure as location services in the content rule. For details on configuring the location cookie feature, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config-owner-content) cookie-domain
(config-owner-content) add

(config-owner-content) no

To negate a command or set it to its default for the content rule, use the **no** command. For information on general **no** commands you can use in this mode, see the general **no** command. The following options are available in content mode.

Syntax Description

no acl *index*	Deletes an ACL
no advanced-balance	Disables the advanced-balancing method for the content rule
no application	Resets the application type to its default setting of HTTP
no arrowpoint-cookie advanced	Disables the mapping of the Arrowpoint cookie flows in the fastpath (hardware)
no arrowpoint-cookie browser-expire	Resets the cookie expiration method to the time configured through the **arrowpoint-cookie expiration** command
no arrowpoint-cookie expiration	Resets the expiration time to one year after the timestamp on the cookie
no arrowpoint-cookie expire-services	Resets the default behavior of sending a new ArrowPoint cookie with the server information from the expired cookie
no arrowpoint-cookie name	Resets the default Arrowpoint cookie name to ARPT
no arrowpoint-cookie path	Resets the ArrowPoint cookie path to its default of “/”

no balance	Resets the load-balancing algorithm to its default setting of roundrobin
no cookie-domain	Removes a cookie domain from a content rule
no dns-disable-local	Enables DNS on the content rule
no dnsbalance	Resets the DNS load-balancing method to its default setting of using the method assigned to the owner
no failover	Resets the failover to its default setting of linear
no flow-reset-reject	Disables the sending of a TCP reset (RST) frame back to clients when active flows are rejected
no flow-timeout-multiplier	Restores the default flow timeout for the port type
no header-field-rule	Removes the header-field group from the content rule
no hotlist	Disables the hot list for the content rule
no hotlist interval	Resets the hot-list interval to its default setting of 1 minute
no hotlist size	Resets the hot-list size to its default setting of 10 entries
no hotlist threshold	Resets the hot-list threshold to its default setting of 0 entries
no hotlist type	Resets the hot-list type to its default setting of hit count
no load-threshold	Resets the load threshold to its default setting of 254
no location-cookie name	Deletes an existing location cookie from a content rule
no owner *existing_owner_name*	Deletes an existing owner
no persistent	Disables persistence
no port	Resets the port number to its default value of 0
no primarySorryServer	Removes the primary sorry service from the rule
no protocol	Resets the protocol for the content rule to its default of **any**
no redirect	Deletes the redirect URL

no redundancy-l4-stateless	Disables stateless redundancy failover
no redundant-index	Disables redundancy on the content rule
no secondarySorryServer	Removes the secondary sorry service from the rule
no sticky-inact-timeout	Disables the sticky connection inactivity timeout feature
no sticky-mask	Resets the sticky mask to 255.255.255.255
no sticky-no-cookie-found-action	Resets sticky-no-cookie-found-action to the default of loadbalance
no sticky-serverdown-failover	Sets the sticky server failover method to its default setting of using the configured load-balancing method
no string ascii-conversion	Enables the ASCII conversion of escaped special characters within the specified sticky range before applying any processing to the string
no string eos-char	Clears the end-of-string characters as the delimiters for the sticky string
no string operation	Resets the string operation to choose a server by matching a service cookie in the sticky string
no string prefix	Clears the string prefix
no string process-length	Resets the number of bytes that the string operation will use to its default of 0
no string range	Resets the string range within a cookie, URL, or URL extension from a client to its default setting of 1 to 100
no string skip-length	Resets the number of bytes to skip after the end of a prefix to find the string result to its default of 0
no url	Removes the URL for the content rule
no vip address	Clears the VIP address for the content rule

(config-owner-content) param-bypass

To enable content requests to bypass transparent caches when the CSS detects special terminators in the requests, use the **param-bypass** command. These terminators include “#” and “?” which indicate that the content is dependent on the arguments that follow the terminators. Because the content returned by the server is dependent on the content request itself, the returned content is not cacheable.

param-bypass disable|**enable**

Syntax Description

disable	Content requests with special terminators do not bypass transparent caches. This is the default setting.
enable	Content requests with special terminators bypass transparent caches and are forwarded to the origin server.

Related Commands

show rule

(config-owner-content) persistent

To maintain a persistent connection with a server, use the **persistent** command. By default, persistence is enabled. Use the **no** form of this command to disable persistence.

persistent

no persistent

Usage Guidelines

In content rule persistence, the CSS keeps the client on the same service connection specified by the content rule for an entire flow session as long as a new content request:

- Matches on the same content rule that specified the current service
- Matches on a new content rule that contains the current service, even if a different best service is specified by the content rule
- Does not match on a content rule, but matches on a previous content rule connected the client to the current service

If you are using transparent caches (which prefetch content) or mirrored-content servers, this scheme works well because the same content is available on each service.

Note If a request for content on a persistent connection matches on a new content rule that does not contain the current service, or persistence is disabled and there is a better service configured in the content rule, the CSS redirects or remaps the current connection to a new best service based on the setting of the **(config) persistence reset** command, if configured. If you do not configure persistence reset, the CSS performs an HTTP redirect by default.

Disabling persistence allows the CSS to move a connection to a better service on the same rule or to utilize cache bypass functionality (EQLs or failover bypass). Disable persistence on a content rule with:

- A balance method of domain or domain hash when using proxy caches
- A balance method of url or urlhash when using transparent caches
- A failover method of bypass when using transparent caches
- An EQL bypass with a transparent cache
- Adding a sorry server to a content rule

Related Commands

(config) bypass persistence
(config) persistence reset

(config-owner-content) port

To specify the content rule's TCP/UDP port number, use the **port** command. The port number for a content rule is the port number used by incoming requests for the content governed by the rule. Use the **no** form of this command to reset the port number to its default value of 0, which means any port.

port *number*

no port

Syntax Description

number	TCP or UDP incoming port number associated with the content rule. Enter an integer from 0 to 65535. The default value is 0, which means any port.

Usage Guidelines

Before you can change the port number, you must suspend the rule.

Related Commands

show rule
(config-owner-content) protocol

(config-owner-content) primarySorryServer

To configure the primary sorry service for the content rule, use the **primarySorryServer** command. A sorry service is a server that is used for content requests when all other services are unavailable. You can configure the service to contain content, or to provide a drop or redirect message. The service is not used in load balancing. Use the **no** form of this command to remove a primary sorry service.

primarySorryServer *service_name*

no primarySorryServer

Syntax Description

service_name	Name of the existing service. Enter the name as a case-sensitive unquoted text string with no spaces.

Usage Guidelines

Do not configure a sorry server on a content rule used for matching noncacheable content.

Related Commands

show rule
(config) service
(config-owner-content) secondarySorryServer

(config-owner-content) protocol

To specify the content rule's IP protocol, use the **protocol** command. The protocol for a content rule is the protocol used by incoming requests for the content governed by the rule. Use the **no** form of this command to reset the protocol to its default value of **any**.

protocol any|tcp|upd

no protocol

Syntax Description

any	Content rule uses any protocol. This is the default protocol.
tcp	Content rule uses the TCP protocol suite.
udp	Content rule uses the UDP protocol suite.

Usage Guidelines

Before you can change the protocol, you must suspend the rule.

Related Commands

show rule
(config-owner-content) port

(config-owner-content) redirect

To set HTTP status code 302 for the content rule, use the **redirect** command. Use the **no** form of this command to delete the redirect URL.

redirect "*url***"**

no redirect

Syntax Description

"*url*"	URL to send with HTTP status code 302. Enter a quoted text string with no spaces and a maximum of 252 characters.

Usage Guidelines

The **redirect** command makes the content at its current address unavailable to subsequent requests, and provides a message to send with the status code back to the requestor. Specify a message that returns the alternate location of the content governed by the rule.

Related Commands

show rule

(config-owner-content) redundancy-l4-stateless

To enable the Stateless Redundancy Failover feature for a content rule on a redundant CSS, use the **redundancy-l4-stateless** command. The CSS can set up a connection for a midstream TCP flow, allowing TCP traffic to continue when a failure occurs at the load-balancing CSS. By default, the CSS rejects TCP sessions that do not begin with a TCP/SYN frame. Use the **no** form of this command to reset the default behavior of the CSS.

redundancy-l4-stateless

no redundancy-l4-stateless

Command Modes

Owner-content configuration mode

Usage Guidelines

You cannot use the **redundancy-l4-stateless** command with the **(config) persistence reset remap** command.

The Stateless Redundancy Failover feature has specific environment and configuration requirements. The environment requirements are as follows:

- Layer 3 and Layer 4 content rules with a VIP address. This feature is not supported in Layer 5 configurations.
- Source IP address load balance method only.
- CSS-to-CSS identical server and content rule configuration including:
  - Content VIP address.
  - Content balance method.
  - Failover method.
  - Service IP address, number, and order. The CSS orders services alphabetically. Apply identical service names on the master and backup CSSs.
- Visibility of identical servers to keepalive traffic from CSS to CSS. This ensures that the redistribution of the balance method does not occur in a failover event.

Redundant routes in a high-availability topology surrounding the CSS are supported. However, the topology must not balance packets in a TCP/IP socket connection across more than one Ethernet port on the CSS.

IP and VIP redundant configurations are supported. The configuration requirement for each server farm is synchronization across all CSSs of:

- Membership and IP addresses of the server farms.
- Content rule VIP address. Each CSS must share the content VIP address that is used as a balance point for the server farm.
- Source group VIP address. Define each CSS with a source group VIP address as the content VIP address to NAT source addresses for packets returning from the server. In case of a failover, the source group handles connection setups for TCP/IP retransmissions that arrive at the CSS from a server. All servers on the farm must be a member of the source group.

  Do not configure source groups for outbound traffic from the servers because the backup CSS does not know which ports were mapped by the source group on the master CSS. This restriction also applies to active FTP because the server initiates the data connection.

For more detailed information on Stateless Redundancy Failover, refer to the *Cisco Content Services Switch Redundancy Configuration Guide*.

Related Commands

show redundancy
(config) ip redundancy
(config) group
(config) interface
(config) service
(config-group) redundancy-l4-stateless
(config-owner) content

(config-owner-content) redundant-index

To configure the global content index for a redundant content rule, use the **redundant-index** command. A CSS uses the global content index to keep track of redundant content rules and associated flow state information. Use the **no** form of this command to disable redundancy on the content rule.

redundant-index *number*

no redundant-index

Syntax Description

number	Redundant index for the content rule. Enter a unique integer from 0 to 32767, where a value of 0 disables ASR on a content rule. The default is 0, but it does not appear in the running-config even if you configure it explicitly.

Usage Guidelines

If you enter the **no redundant-index** command on an active redundant content rule for live redundancy peers, the command automatically suspends the content rule. Flows already mapped by a CSS are not affected. However, if a failover occurs during the life of an active flow that matches on such a suspended content rule, the backup CSS cannot map the flow because it cannot find the content rule with the same global index as that on the original master.

Note For implicit or explicit Layer 5 rules, where there is delayed binding, binding is not complete until the CSS processes the SYN/ACK from the server. This means that, if a failover occurs in the middle of a spanned content request, the master CSS will not receive the SYN/ACK from the server and the flow will not be replicated on the backup CSS. No data is lost and users can simply refresh their browsers to restart the connection.

For information on redundant indexes and configuring Adaptive Session Redundancy (ASR) on 11500 series CSS peers, including requirements and restrictions that apply to both CSS peers in an ASR configuration, refer to the *Cisco Content Services Switch Redundancy Configuration Guide*.

Related Commands

(config-group) redundant-index
(config-owner-content) vip address
(config-service) redundant-index

(config-owner-content) remove

To remove either a DNS name or an existing service from the content rule, use the **remove** command.

remove [**dns** *dns_name*|**location-service** *service_name*|**service** *service_name*]

Syntax Description

dns *dns_name*	Removes the DNS name from the content rule. Enter the name as a case-sensitive unquoted text string with no spaces and a maximum length of 32 characters. To see a list of DNS names, enter: **`remove dns ?`**
location-service *service_name*	Removes the specified location service from a content rule in a location cookie configuration. For more information about the location cookie feature, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

service *service_name*	Removes an existing service from the content rule. Removing a service removes it from the resource pool that the CSS uses for balancing the load of requests for the content governed by the rule. The CSS rebalances the remaining services. It does not use the **failover** command setting. Enter the service name as a case-sensitive unquoted text string with no spaces and a maximum length of 32 characters. To see a list of service names, enter: **`remove service ?`**

Related Commands

show rule
(config-owner-content) add

(config-owner-content) secondarySorryServer

To configure the secondary sorry service for the content rule, use the **secondarySorryServer** command. Use the **no** form of this command to remove a secondary sorry service.

secondarySorryServer *service_name*

no secondarySorryServer

Syntax Description

service_name	Name of the existing service. Enter the name as a case-sensitive unquoted text string with no spaces.

Usage Guidelines

A secondary sorry service is a backup service that is used when the primary sorry service is unavailable. You can configure the service to contain content or to provide a drop or redirect message. The service is not used in load balancing.

Do not configure a sorry server on a content rule used for matching noncacheable content.

Related Commands

show rule
(config) service
(config-owner-content) primarySorryServer

(config-owner-content) show owner

To display configuration information and statistics for the owner of the current content rule, use the **show owner** command.

show owner {**statistics**}

Syntax Description

statistics	(Optional) Displays the statistics for the owner of the current content rule

Usage Guidelines

The **show owner** command without an option displays configuration information only.

For field descriptions displayed through the **show owner** command, see the **(config-owner) show owner** command.

Related Commands

(config-owner) address
(config-owner) billing-info
(config-owner) case
(config-owner) dns
(config-owner) email-address

(config-owner-content) show rule-header-field

To display information about the header-field rule and group associated with a content rule, use the **show rule-header-field** command.

show rule-header-field

Examples

To display information about the header-field rule and group associated with a content rule, enter:

```
(config-owner-content[test-rule1])# show rule-header-field
header-field-rule: palmpilot.
 lookup pass: 0, lookup fail: 0.

header field group : palmpilot              Description: Palm Pilot 
users
  header-field 1 user-agent contain "PalmPilot"
```

Related Commands

(config-owner-content) header-field-rule

(config-owner-content) sticky-inact-timeout

To specify the inactivity timeout period on a sticky connection for a content rule before the CSS removes the sticky entry from the sticky table, use the **sticky-inact-timeout** command. Use the **no** form of this command to disable the sticky connection inactivity timeout feature.

sticky-inact-timeout *minutes*

no sticky-inact-timeout

Syntax Description

minutes	Number of minutes of inactivity. Enter a number from 0 to 65535. The default value is 0, which means this feature is disabled. When disabled, the CSS does not remove the entry from the table until the sticky table is full. When the table is full, the CSS recycles the least-used sticky entry first.

Usage Guidelines

When you configure the inactivity timeout period, the CSS keeps the sticky entry in the sticky table for the specified amount of time. The CSS does not reuse the entry until the time expires. If the sticky table is full and none of the entries has expired, the CSS rejects the new sticky request. When the sticky connection expires, the CSS uses the configured load-balance method to choose an available server for the request.

When this feature is disabled, the new sticky connection uses the oldest used sticky entry. A sticky association could exist for a time depending on the sticky traffic load on the CSS.

Related Commands

show rule

(config-owner-content) sticky-mask

To mask a group of client IP addresses in order to preserve the client connection state when the client's source IP address changes, use the **sticky-mask** command. Use the **no** form of this command to reset the default sticky mask of 255.255.255.255.

sticky-mask *subnet_mask*

no sticky-mask

Syntax Description

subnet_mask	Subnet mask used for stickiness. Enter the IP mask in dotted-decimal format (for example, 255.255.255.0). The default is 255.255.255.255.

Usage Guidelines

The client's source IP address change occurs when a client-server connection is lost and the client sends a different IP address. The CSS needs to reconnect the client to the same server that is preserving the client information.

Related Commands

show rule
(config-owner-content) advanced-balance
(config-owner-content) string range

(config-owner-content) sticky-no-cookie-found-action

To specify the action the CSS should take for a sticky cookie content rule when it cannot locate the cookie header or the specified cookie string in the client request, use the **sticky-no-cookie-found-action** command. Use the **no** form of this command to reset sticky-no-cookie-found-action to the default of **loadbalance**.

sticky-no-cookie-found-action [**loadbalance**|**redirect** **"***URL***"**|**reject**|**service** *name*]

no sticky-no-cookie-found-action

Syntax Description

loadbalance	Uses the configured balanced method when no cookie is found in the client request. This keyword is the default setting.
redirect "*URL***"**	Redirects the client request to a specified URL string when no cookie found in the client request. When using this keyword, you must also specify a redirect URL. Enter the redirect URL as a quoted text string from 0 to 252 characters.
reject	Rejects the client request when no cookie is found in the request.
service *name*	Sends the no cookie client request to the specified service when no cookie is found in the request.

(config-owner-content) sticky-serverdown-failover

To define what will happen when a sticky string is found but the associated service has failed or is suspended, use the **sticky-serverdown-failover** command. Use the **no** form of this command to set the sticky failover method to its default setting of using the configured load-balancing method.

sticky-serverdown-failover
balance|redirect|reject|sticky-srcip|sticky-srcip-dstport

no sticky-serverdown-failover

Syntax Description

balance	Sets the failover method to use a service based on the configured load-balancing method.
redirect	Sets the failover method to use a service based on the currently configured redirect string.This command option supports a 252-character redirect string (URL). If a redirect string is not configured, the load-balancing method is used.
reject	Rejects the content request.
sticky-srcip	Sets the failover method to use a service based on the client IP address. This is dependent on the sticky configuration.
sticky-srcip-dstport	Sets the failover method to use a service based on the client IP address and the server destination port. This is dependent on the sticky configuration.

Related Commands

(config-owner-content) balance
(config-owner-content) redirect

(config-owner-content) string

To set string criteria to derive string results and the method to choose a destination server for the result, use the **string** command and its options. The string result is a sticky string in the cookie header, URL, or URL extension based on a sticky type being configured.

The options for this content mode command are:

- **string ascii-conversion**. - Enables or disables the ASCII conversion of escaped special characters within the specified sticky range before applying any processing to the string
- **string eos-char** - Specifies the delimiters for the sticky string
- **string match** - Determines how the CSS handles a string that contains multiple matches with configured strings on services
- **string operation** - Specifies the method to choose a destination server for a string result
- **string prefix** - Specifies the string prefix located in the sticky range
- **string process-length** - Specifies how many bytes, after the end of the prefix designated by the **string prefix** command and skipping the bytes designated by the **string skip-length** command, that the string operation will use
- **string range** - Specifies the starting and ending byte positions within a cookie, URL, or URL extension from a client
- **string skip-length** - Specifies how many bytes to skip after the end of prefix to find the string result

For more information on these options, see the following commands.

string ascii-conversion

To enable or disable the ASCII conversion of escaped special characters within the specified sticky range before applying any processing to the string, use the **string ascii-conversion** command. By default, ACSII conversion is enabled. Use the **no** form of this command to re-enable the ASCII conversion of special escaped characters.

string ascii-conversion enable|disable

no string ascii-conversion

Syntax Description

enable	Enables the ASCII conversion of escaped special characters within the specified sticky range before applying any processing to the string (default)
disable	Disables the ASCII conversion of escaped special characters within the specified sticky range before applying any processing to the string

Command Modes

Owner-Content

Related Commands

(config-owner-content) string range

string eos-char

To specify up to three ASCII characters as the delimiters for the sticky string, use the **string eos-char** command. For example, in a cookie header, a ";" character is usually used as a delimiter; in a URL extension, a "&" character is often used as a delimiter. Use the **no** form of this command to clear the end-of-string characters.

string eos-char "*characters***"**

no string eos-char

Syntax Description

"character"	End-of-string characters. Enter a quoted text string with a maximum of three characters.

Command Modes

Owner-Content

Usage Guidelines

The CSS uses this command if the **string process-length** command is not configured; the **string process-length** command has higher precedence. If neither commands are configured, the CSS uses the maximum 64 bytes for the final string operation.

Related Commands

(config-owner-content) string process-length

string match

To determine how the CSS handles an incoming string that contains multiple matches with configured strings on services, use the **string match** command. By default, the CSS matches the most specific string.

string match specific|first-service-match|first-string-found

Syntax Description

specific	Matches the most specific string match (default).
first-service-match	Allows the CSS to look at each service by its index number. The CSS compares the incoming string and compares it to the string in the service by the first occurring match.
first-string-found	Matches the first string in the incoming string.

Command Modes

Owner-Content

Usage Guidelines

Use **string match** command with the **advanced-balance cookies|cookiesurl|url** command.

In the following example, the incoming string is grapebananapear. The CSS service configuration is:

```
service s1
string pear

service s2
string grape

service s3
string banana
```

With the default setting or the **specific** keyword, the most specific match is the longest string. In this example, the string match is banana.

With the **first-service-match** keyword, the CSS looks at each service in the order of its index number. Then the CSS compares the incoming string and compares it to the string in the service for a match. In this example, the first-service-string match is pear.

With the **first-string-match** keyword, the CSS matches the incoming string to the first occurrence in a service string. In this example, the string match is grape.

Related Commands

(config-owner-content) advanced-balance

string operation

To determine the method to choose a destination server for a string result, derived from the settings of the **string** criteria commands, use the **string operation** command. You can choose a server by using the configured balance method or by using the hash key generated by the specified sticky hash type.

Use the **no** form of this command to reset the string operation to its default setting, choosing a server by matching a service cookie in the sticky string.

string operation match-service-cookie|hash-a|hash-crc32|hash-xor

no string operation

Syntax Description

match-service-cookie	Chooses a server by matching a service cookie in the sticky string. This is the default setting. When a match is not found, the server is chosen by using the configured balance method (for example, round robin).
hash-a	Chooses a server by applying a basic hash algorithm on the hash string to generate the hash key. If the selected server is out of service, the CSS performs a rehash to choose another server.
hash-crc32	Chooses a server by applying the CRC32 algorithm on the hash string to generate a hash key. If the selected server is out of service, the CSS performs a rehash to choose another server.
hash-xor	Chooses a server by performing an Exclusive OR (XOR) on each byte of the hash string to derive the final hash key. If the selected server is out of service, the CSS performs a rehash to choose another server.

Command Modes

Owner-Content

Related Commands

(config-owner-content) string ascii-conversion
(config-owner-content) string eos-char
(config-owner-content) string prefix
(config-owner-content) string process-length
(config-owner-content) string skip-length

string prefix

To specify the string prefix located in the sticky range, use the **string prefix** command. Use the **no** form of this command to clear the string prefix.

string prefix "*text***"**

no string prefix

Syntax Description

"*text*"	String prefix. Enter a quoted text string with a maximum of 30 characters. The default has no prefix. If you do not configure the string prefix, the string functions start from the beginning of the cookie, URL, or URL extension, depending on the sticky type. If the string prefix is configured but is not found in the specified sticky range, load balancing defaults to the roundrobin method.

Command Modes

Owner-Content

Related Commands

(config-owner-content) advanced-balance
(config-owner-content) string range

string process-length

To specify how many bytes, after the end of the prefix designated by the **string prefix** command and skipping the bytes designated by the **string skip-length** command, that the string operation will use, use the **string process-length** command. Use the **no** form of this command to set the number of bytes to its default setting of 0.

string process-length *bytes*

no string process-length

Syntax Description

bytes	Number of bytes. Enter a number from 0 to 64. The default is 0.

Command Modes

Owner-Content

Usage Guidelines

The **string process-length** command has higher precedence than the **string eos-char** command. If neither commands are configured, the CSS uses the maximum 64 bytes for the final string operation.

Related Commands

(config-owner-content) string eos-char
(config-owner-content) string operation
(config-owner-content) string prefix
(config-owner-content) string skip-length

string range

To specify the starting and ending byte positions within a cookie, URL, or URL extension from a client, use the **string range** command. Use the **no** form of this command to reset the range to its default setting of 1 to 100.

string range *start_byte* **to** *end_byte*

no string range

Syntax Description

start_byte	Starting byte position of the cookie, URL, or URL extension after the header. Enter an integer from 1 to 1999. The default is 1. Make sure that the starting byte position is less than the end byte.
end_byte	Ending byte position of the cookie, URL, or URL extension. Enter an integer from 2 to 2000. The default is 100. Make sure that the ending byte position is more than the start byte.

Command Modes

Owner-Content

Usage Guidelines

By specifying the range of bytes, the CSS processes the information located only within the range. This limits the amount of information that the CSS has to process when examining each cookie, URL, or URL extension, enhancing its performance.

Note If the starting position is beyond the cookie, URL, or URL extension, the CSS does not perform the string function. When the ending position is beyond the cookie, URL, or URL extension, the string processing stops at the end of the corresponding header.

Related Commands

(config-owner-content) advanced-balance
(config-owner-content) sticky-mask

string skip-length

To specify how many bytes to skip after the end of the prefix to find the string result, use the **string skip-length** command. Use the **no** form of this command to set the number of bytes to its default setting of 0.

string skip-length *bytes*

no string skip-length

Syntax Description

bytes	Number of bytes. Enter a number from 0 to 64. The default is 0.

Command Modes

Owner-Content

Related Commands

(config-owner-content) string prefix

(config-owner-content) suspend

To deactivate the content rule, denying access to the content governed by the rule, use the **suspend** command. Suspending a content rule does not affect existing flows to the content; it only applies to future requests for the content.

suspend

Related Commands

show rule
(config-owner-content) active

(config-owner-content) url

To specify the Uniform Resource Locator (URL) for the content, use the **url** command. Use the **no** form of this command to remove the URL or the URQL from the content rule.

url [**"/***url_name***"**|**"/***url_path***/*"** [**eql** *eql_name*|**dql** *dql_name* {*eql_name*}]|**urql** *urql_name*]
no url {**urql**}

Syntax Description

“url_name”

The URL for the content. Enter a quoted text string with a maximum length of 252 characters. You must place a slash character (/) at the beginning of the URL, for example, /files/test.gif. To specify a domain name, place two slashes at the beginning of the URL. For example, //www.*name*.com/* allows the rule to match on the HTTP traffic that contains the www.*name*.com domain name in the HTTP host tag.

Note Do not include the ? or # parameter character in the URL string. The CSS terminates the URL at these parameter characters.

To specify certain wildcard operations for wildcard matching, use a “*” character to specify a wildcard match. Examples of supported wildcards are:

- **/*.html** - Matches all requests with the .html extension
- **/newfiles/*.jpg** - Matches all requests for files beginning with /newfiles and have the .jpg extension
- **/newfiles/*** - Matches all requests for files beginning with /newfiles
- **/newfiles/1.jpg** - Matches requests for the /newfile/1.jpg file only

Normally, port 80 traffic does not use a port number in the domain name. To specify a port other than port 80, enter the domain name with the port number exactly. Separate the domain name and the port number with a colon. For example, enter:

```
(config-owner-content[arrowpoint-rule1])# url
“//www.arrowpoint.com:8080/*”
```

"*url_path*"	Path to any content file that has its file extension defined in the EQL or that has its domain defined in a DQL. Enter a quoted text string. You must place: • A slash character (/) at the beginning of the path • /* characters at the end of the path An example is /announcements/new/*. To specify a domain name, place two slashes at the beginning of the URL.
eql *eql_name*	The name of the EQL. To see a list of EQLs, enter: `eql ?`
dql *dql_name*	The name of the DQL. To see a list of DQLs, enter: `eql ?`
urql *urql_name*	Specifies a URQL consisting of a group of URLs to the content rule. Enter the name of the URQL. You can assign only one URQL per rule. To see a list of URQLs, enter: `urql ?`

Usage Guidelines

Before you can change the URL for the content rule, you must suspend the rule and you must remove the current URL.

When you configure content replication and staging, you must configure a URL in a content rule to define which files you want replicated. Then, add the subscriber services to the content rule.

You cannot configure a URQL with a subscriber service.

If you want all files in all directories replicated, you do not need to create a content rule. Create a content rule to specify only those files that you want replicated.

You cannot configure the **application ssl** and **url urql** commands on the same content rule.

For caching environments, you can configure a domain content rule by placing two slash characters (//) at the front of the *url_name* or *url_path*. The rule matches HTTP traffic that contains the domain name in the HTTP host tag.

Related Commands

show content
show rule
(config) eql
(config) urql

(config-owner-content) vip address

To specify the content rule virtual IP (VIP) address or a range of addresses, use the **vip address** command. Use the **no** form of this command to clear the VIP address.

vip address *ip_or_host* {**range** *number*}

no vip address

Syntax Description

ip_or_host	IP address or name for the content rule. Enter the address in either dotted-decimal IP notation (for example, 192.168.11.1) or mnemonic host-name format (for example, myhost.mydomain.com).
range *number*	(Optional) Allows you to specify a range of IP addresses starting with the VIP address (*ip_or_host*). Enter a number from 1 to 65535. The default range is 1. For example, if you enter an IP address of 203.1.1.1 with a range of 10, the VIP addresses range from 203.1.1.1 through 203.1.1.10.

Usage Guidelines

A virtual IP address (VIP) is an address that an Internet Domain Network System (DNS) provides when asked to resolve a domain name. Assigning a VIP to a content rule enables the CSS to translate, using Network Address Translation (NAT), the VIP to the IP address of the service where the content resides. By translating a VIP to the service IP address, the CSS enhances network security because it prevents users from accessing your private network IP addresses.

Ensure that all VIPs are unique IP addresses. Do not configure a VIP to the same address as an existing IP address on your network or a static ARP entry.

When you configure a rule without a VIP (wildcard VIP rule), the rule will match on any VIP that matches the other configured rule attributes (for example, port and protocol). When you configure a rule without a VIP and without a port (double-wildcard caching rule), the rule will match on any VIP or port that matches the other configured rule attributes (for example, protocol). If you have a configuration that requires either type of rule, be aware that the client request will match on this rule when the client request attempts to connect directly to a server IP address.

When you use an FTP content rule with a configured VIP address range, be sure to configure the corresponding source group with the same VIP address range.

When you ping a VIP, the CSS responds only if there is at least one live service, live sorry server, or redirect string configured for the VIP, or if the service is associated with a source group. If the services or sorry servers are down and you have not defined a redirect string for the VIP, the CSS does not respond to the ping.

The CSS supports stateless redundancy failover on CSSs operating in an IP redundancy or a VIP/interface redundancy configuration. Stateless redundancy failover requires a very specific redundant CSS configuration, which includes content rule VIP addresses. For details, refer to the *Cisco Content Services Switch Redundancy Configuration Guide*.

Related Commands

show rule

(config-owner-content) vip-ping-response

To include local and remote services in the decision by the CSS to respond to a ping request to a VIP address configured on a content rule, use the **vip-ping-response** command. By default, a CSS responds to a ping request to a VIP address configured on a content rule if any of the local services on the rule are alive.

vip-ping-response local|local-remote

Syntax Description

local	Includes only local services in the decision to respond to a ping request to the VIP address (default)
local-remote	Includes local services and remote services, for example services of type redirect, in the decision to respond to a ping request to the VIP address

(config-owner-content) zero

To set the counters for the current content rule or all content rules, or a specified service or all services of the current content rule to zero, use the **zero** command.

zero {**all**|**total-connections**|**total-reused-connections**
|**state-transitions** {**service** *name*}}

Syntax Description

all	(Optional) Zeros the counters for all content rules.
total-connections	(Optional) Sets the Total Connections counter for all services or a specified service to zero.
total-reused-connections	(Optional) Sets the Total Reused Conns counter for all services or a specified service to zero.
state-transitions	(Optional) Sets the State Transitions counter for all services or a specified service to zero.
service *name*	(Optional) Name for the service. Only the counter for the specified service is set to zero.

Usage Guidelines

The **show rule** command displays the content rule counters. The **show service** command displays the service counters.

If you enter the **zero** command without an option, the counters for the current content rule are set to zero.

If you do not define a service name with the **zero total-connections |total-reused-connections|state-transitions** command, the counter for all services of the rule is set to zero.

To set the counters to zero for all services on the CSS, use the **zero service** command.

Related Commands

show rule
show service

Reporter Configuration Mode Commands

Reporter configuration mode allows you to configure a reporter. A reporter is a software monitoring agent that you associate with critical interfaces and virtual routers (VRs). The reporter monitors the state of the critical interfaces and causes the associated VRs to fail over when the interfaces go down. You can also use a reporter to synchronize the state of associated VRs to prevent asymmetric flows. You can configure a maximum of 128 reporters on a CSS.

To access reporter configuration mode, enter the **reporter** command in global configuration mode. The prompt changes to (config-reporter [*reporter_name*]). For information about commands available in this mode, see the following commands.

In global configuration mode, use the **no** form of this command to delete an existing reporter.

(config) reporter *reporter_name*

(config) no reporter *reporter_name*

Syntax Description

reporter_name	Name of a reporter that you want to create. Enter an unquoted text string with no spaces from 1 to 31 characters. To see a list of existing reporter names, enter: `reporter ?`

(config-reporter) active

To activate a newly configured reporter or to reactivate a suspended reporter, use the **active** command. A new reporter remains in the Suspended state until you activate it.

active

Usage Guidelines

Use this command to initially activate a newly configured reporter or to reactivate a reporter after you have suspended it with the **suspend** command.

Related Commands

show reporter
(config) reporter
(config-reporter) phy
(config-reporter) suspend
(config-reporter) type
(config-reporter) vrid

(config-reporter) phy

To configure one or more physical interfaces that you want a reporter to monitor, use the **phy** command. Use the **no** form of this command to remove an interface and all of its attributes from the reporter.

phy *interface_name*

no phy *interface_name*

Syntax Description

interface_name	Name of the physical interface that you want to monitor. Enter an interface name in interface port format (for example, e1 on a CSS 11501) or slot/port format (for example, 1/1 on a CSS 11503 and CSS 11506).

Usage Guidelines

This command allows you to configure a maximum of 128 interfaces on a reporter of type **critical-phy-all-up** or **critical-phy-any-up**.

If you associate more than one reporter with the same VR, we recommend that you do not configure the same physical interfaces (ports) on two different reporter types (for example, ports 1/1 and 1/2 on a reporter of type **critical-phy-all-up** and ports 1/1 and 1/2 on a reporter of type **critical-phy-any-up**). Otherwise, unexpected VR failovers may occur.

Related Commands

show reporter
(config) reporter
(config-reporter) type

(config-reporter) vrid
(config-reporter) active
(config-reporter) suspend

(config-reporter) suspend

To suspend a reporter and stop it from monitoring configured critical interfaces or VRs, use the **suspend** command.

suspend

Usage Guidelines

Use this command to temporarily stop using a reporter or to change a reporter configuration. Once you have made the configuration changes and want to reactivate the reporter, enter the **active** command.

Related Commands

show reporter
(config) reporter
(config-reporter) active
(config-reporter) phy
(config-reporter) type
(config-reporter) vrid

(config-reporter) type

To configure the reporter type, use the **type** command. To remove a reporter type and all of its attributes, use the **no** form of this command.

type *reporter_type*

no type

Syntax Description

reporter_type	You can configure the following reporter types: • **vrid-peer** - Monitors the states of associated VRs and ensures that the VR states are synchronized. If one VR goes down, the reporters state goes down and causes any other associated VRs to go down. • **critical-phy-all-up** - Monitors the states of configured critical physical interfaces. If any critical interface goes down, the reporter goes down and mastership of the associated VR transitions from the master CSS to the backup CSS. To prevent a VR failover, all interfaces must remain up. • **critical-phy-any-up** - Monitors the states of configured critical physical interfaces. If all associated critical interfaces go down, the reporter goes down and mastership of the associated VR transitions from the master CSS to the backup CSS. Provided that one critical interface stays up, the reporter and the VR remain up.

Usage Guidelines

You can configure a maximum of 128 reporters of any combination of types on a CSS depending on available memory, with a maximum of four **vrid-peer** types. There is no default reporter type.

You can change the reporter type without removing the attributes associated with the type. For example, you can change the reporter type from **vrid-peer** to **critical-phy-all-up**.

Related Commands

show reporter
(config) reporter
(config-reporter) active
(config-reporter) phy
(config-reporter) suspend
(config-reporter) vrid

(config-reporter) vrid

To configure a VR that you want the reporter to monitor, use the **vrid** command. Use the **no** form of this command to remove a VRID and all of its attributes from the reporter.

vrid *ip_address vrid*

no vrid *ip_address vrid*

Syntax Description

ip_address	Destination network prefix. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
vrid	Identifier of an existing VR. Possible values are 1 to 255.

Usage Guidelines

This command allows you to configure a maximum of eight VRIDs on a reporter of type **vrid-peer**. You cannot configure the same circuit IP address and VRID on more than one reporter.

Related Commands

show reporter
(config) reporter
(config-reporter) active
(config-reporter) phy
(config-reporter) suspend
(config-reporter) type

RMON Alarm Configuration Mode Commands

RMON alarm configuration mode allows you to configure an RMON alarm. An RMON alarm allows you to monitor every SNMP object in the CSS for a desired transitory state.

To access RMON alarm configuration mode, use the **rmon-alarm** command from any configuration mode except boot configuration mode. The prompt changes to (config-rmonalarm [*index*]). You can also use this command in RMON alarm mode to configure another alarm. For information about commands available in this mode, see the following commands.

Use the **no** form of this command in global configuration mode to delete an RMON alarm.

rmon-alarm *index*

no rmon-alarm *index*

Syntax Description

index	RMON alarm index number. Enter an integer from 1 to 65535. The RMON alarm index 65535 is administratively predefined and cannot be modified. If you enter this index number, a message similar to the following appears: `%% Index internally used. Administrative control not allowed.`

(config-rmonalarm) active

To activate the RMON alarm, use the **active** command. Before you can activate an alarm, you must specify the owner parameter. To suspend an alarm to change its configuration, use the **suspend** command.

active

Related Commands

(config-rmonalarm) owner
(config-rmonalarm) suspend

(config-rmonalarm) falling-event

To specify the falling event index for the RMON alarm, use the **falling-event** command. When the falling threshold is exceeded, this is the RMON event that is triggered. Use the **no** form of this command to reset the event index to 0.

falling-event *falling_index*

no falling-event

Syntax Description

falling_index	Event index used when a falling threshold is crossed. Enter an integer from 0 to 65535. If you enter 0, no event is generated. The default is 0.

Usage Guidelines

You must suspend the alarm to change the index.

(config-rmonalarm) falling-threshold

To specify the falling threshold for the RMON alarm, use the **falling-threshold** command. A single event is generated when the sampled value is less than or equal to the threshold, and the value at the last sampling interval is greater than the threshold. Use the **no** form of this command to reset the threshold to 0.

falling-threshold *falling_value*

no falling-threshold

Syntax Description

falling_value	Threshold for the falling sample type. Enter an integer from 0 to 4294967295. The default is 0.

Usage Guidelines

You must suspend the alarm to change the threshold.

(config-rmonalarm) lookup

To look up an SNMP variable and to view the description associated with a MIB object, use the **lookup** command.

lookup *variable*

Syntax Description

variable	Name of the variable to look up. Enter an unquoted text string with a maximum length of 32 characters.

(config-rmonalarm) no

To negate a command or set it to its default, use the **no** command. For information on general **no** commands you can use in this mode, see the general **no** command. The following options are available in RMON alarm mode.

Syntax Description

no falling-event	Resets the event index to 0
no falling-threshold	Resets the threshold to 0
no owner	Deletes the owner
no rising-event	Resets the event index to 0
no rising-threshold	Resets the threshold to 0
no sample-interval	Resets the interval to 300
no sample-type	Resets the sample type to delta
no sample-variable	Deletes the variable
no startup-type	Resets the type to a rising alarm

(config-rmonalarm) owner

To specify the owner of the RMON alarm, use the **owner** command. Use the **no** form of this command to delete the owner.

owner “*owner_name*”

no owner

Syntax Description

“*owner_name*”	Name of the owner that configured this entry and is using its assigned resources. Enter a quoted text string with a maximum length of 32 characters.

Usage Guidelines

Before activating the alarm, you must specify an owner.

(config-rmonalarm) rising-event

To specify the rising event index for the RMON alarm, use the **rising-event** command. Use the **no** form of this command to reset the event to 0.

rising-event *rising_index*

no rising-event

Syntax Description

rising_index	Event index used when a rising threshold is crossed. Enter an integer from 0 to 65535. If you enter 0, no event is generated. The default is 0.

Usage Guidelines

You must suspend the alarm to change the index.

(config-rmonalarm) rising-threshold

To specify the rising threshold for the RMON alarm, use the **rising-threshold** command. When the sampled value is greater than or equal to the threshold and the value at the last sampling interval was less than the threshold, a single event is generated. Use the **no** form of this command to reset the threshold to 0.

rising-threshold *rising_value*

no rising-threshold

Syntax Description

rising_value	Threshold for the rising sample type. Enter an integer from 0 to 4294967295. The default is 0.

Usage Guidelines

You must suspend the alarm to change the threshold.

(config-rmonalarm) sample-interval

To specify the sampling interval for the RMON alarm, use the **sample-interval** command. Use the **no** form of this command to reset the interval to 300.

sample-interval *interval*

no sample-interval

Syntax Description

interval	Interval, in seconds, over which the data is sampled and compared with the rising and falling thresholds. Enter an integer from 1 to 65535. With delta sampling, be careful to set the interval short enough so that the sampled variable is not likely to increase or decrease by more than 2^{31}-1 during a single sampling interval. The default is 300.

Usage Guidelines

You must suspend the alarm to change the interval.

(config-rmonalarm) sample-type

To specify the sample type for the RMON alarm, use the **sample-type** command. Use the **no** form of this command to reset the type to delta sampling.

sample-type absolute|delta

no sample-type

Syntax Description

absolute	Uses absolute sampling
delta	Uses delta sampling (default)

Usage Guidelines

You must suspend the alarm to change the sample type.

(config-rmonalarm) sample-variable

To specify the sample variable for the RMON alarm, use the **sample-variable** command. Use the **no** form of this command to delete the variable.

sample-variable *snmp_object_id*

no sample-variable

Syntax Description

snmp_object_id	SNMP object ID. To see a list of SNMP object IDs, enter: `sample-variable ?`

Usage Guidelines

You must suspend the alarm to change the variable.

(config-rmonalarm) startup-type

To specify the initial alarm type for the RMON alarm, use the **startup-type** command. Use the **no** form of this command to reset the type to a rising alarm.

startup-type falling|rising|rising-and-falling

no startup-type

Syntax Description

falling	Uses a falling alarm
rising	Uses a rising alarm (default)
rising-and-falling	Uses both rising and falling alarms

Usage Guidelines

You must suspend the alarm to change the startup type.

(config-rmonalarm) suspend

To suspend the RMON alarm allowing you to change its configuration setting, use the **suspend** command.

suspend

Related Commands

(config-rmonalarm) active

RMON Event Configuration Mode Commands

RMON event configuration mode allows you to configure an RMON event. An RMON event defines what should occur when an RMON alarm is triggered.

To access RMON event configuration mode, use the **rmon-event** command from any configuration mode except boot configuration mode. The prompt changes to (config-rmonevent [*index*]). You can also use this command in RMON event mode to configure another event. For information about commands available in this mode, see the following commands.

Use the **no** form of this command to delete an RMON event. Use the **no** form of this command only in global configuration mode.

rmon-event *index*

no rmon-event *index*

Syntax Description

index	RMON event index number. Enter an integer from 1 to 65535. The RMON event index 65535 is administratively predefined and cannot be modified. If you enter this index number, a message similar to the following appears: `%% Index internally used. Administrative control not allowed.`

(config-rmonevent) active

To activate the RMON event, use the **active** command. Before you can activate an event, you must specify the owner of the event. To suspend an event to change its configuration, use the **suspend** command.

active

Related Commands

(config-rmonevent) owner
(config-rmonevent) suspend

(config-rmonevent) community

To specify the RMON event community where you want to send the SNMP trap, use the **community** command. Use the **no** form of this command to reset the community to public.

community *community_name*

no community

Syntax Description

community_name	Name of the community. This variable is the name of the SNMP community you configured using the **snmp trap-host** command. Enter an unquoted text string with a maximum length of 127 characters.

Usage Guidelines

If you have activated the event, you cannot specify a community. Suspend the event through the **(config-rmonevent) suspend** command.

Related Commands

snmp trap-host

(config-rmonevent) description

To specify the RMON event description, use the **description** command. Use the **no** form of this command to delete the description.

description "*description***"**

no description

Syntax Description

"*description*"	Description of the RMON event. Enter a quoted text string with a maximum length of 126 characters.

Usage Guidelines

If you have activated the event, you cannot specify a description. Suspend the event through the **(config-rmonevent) suspend** command.

(config-rmonevent) no

To negate a command or set it to its default, use the **no** command. For information on general **no** commands you can use in this mode, see the general **no** commands. The following options are available in RMON event mode.

Syntax Description

no community	Resets the community to public
no description	Deletes the description
no type	Resets the generated event type to log
no owner	Deletes the owner

(config-rmonevent) owner

To specify the owner of the RMON event, use the **owner** command. Use the **no** form of this command to delete the owner.

owner "*owner_name*"

no owner

Syntax Description

"*owner_name*"	Name of the owner that configured this entry and is using its assigned resources. Enter a quoted text string with a maximum of 126 characters.

Usage Guidelines

Before activating the event, you must specify an owner. To change the owner, first, suspend the event through the **(config-rmonevent) suspend** command.

Related Commands

(config-rmonevent) active

(config-rmonevent) type

To specify the generated RMON event type, use the **type** command. Use the **no** form of this command to reset the type to generate a log.

type log|log-and-trap|trap

no type

Syntax Description

log	Generates a log
log-and-trap	Generates a log and a trap
trap	Generates a trap

Usage Guidelines

If you have activated the event, you cannot specify this parameter. Suspend the event through the **(config-rmonevent) suspend** command.

(config-rmonevent) suspend

To suspend the RMON event allowing you to change its configuration setting, use the **suspend** command.

suspend

Related Commands

(config-rmonevent) suspend

RMON History Configuration Mode Commands

RMON history configuration mode allows you to configure the RMON history operation. To access RMON history configuration mode, use the **rmon-history** command from any configuration mode except boot configuration mode. The prompt changes to (config-rmonhistory [*index*]). For information about commands available in this mode, see the following commands.

Use the **no** form of this command to delete an RMON history. Use the **no** form of this command only in global configuration mode.

rmon-history *index*

no rmon-history *index*

Syntax Description

index	RMON history index number. Enter an integer from 1 to 65535. Some history index numbers are administratively predefined and cannot be modified. If you enter an index number under administrative control, a message similar to the following appears: `%% Index internally used. Administrative control not allowed.`

(config-rmonhistory) active

To activate an RMON history entry, use the **active** command.

active

Usage Guidelines

Before activating this command, you must specify an owner of the RMON history entry.

Related Commands

(config-rmonhistory) owner

(config-rmonhistory) data-source

To specify the object of the RMON history operation, use the **data-source** command.

data-source *data_object_id*

Syntax Description

data_object_id	Data object ID. To see a list of data object IDs, enter: `data-source ?`

Usage Guidelines

If you have activated the history, you cannot specify this object.

(config-rmonhistory) interval

To specify the bucket interval for the RMON history operation, use the **interval** command.

interval *value*

Syntax Description

value	Interval value in seconds. Enter an integer from 1 to 3600. The default is 1800.

Usage Guidelines

If you have activated the history, you cannot specify an interval.

(config-rmonhistory) no

To negate a command or set it to its default, use the **no** command. For information on general **no** commands you can use in this mode, see the general **no** command.

(config-rmonhistory) owner

To specify the owner of the RMON history event, use the **owner** command.

owner “*owner_name*”

Syntax Description

“*owner_name*”	Name of the owner that configured the entry and is using its assigned resources. Enter a quoted text string with a maximum length of 32 characters.

Usage Guidelines

Before activating the event, you must specify an owner.

Related Commands

(config-rmonhistory) active

(config-rmonhistory) requested-buckets

To specify the bucket count for the RMON history operation, use the **requested-buckets** command.

requested-buckets *count*

Syntax Description

count	Requested number of discrete time intervals in buckets over which to save data associated with the history entry. Enter an integer from 1 to 65535. The default is 50.

Usage Guidelines

If you have activated the history, you cannot specify this parameter.

Service Configuration Mode Commands

Service configuration mode allows you to configure a service on the CSS. A service is an entity that contains and provides Internet content. It is identified by a name, an IP address, and optimally, a protocol and a port number. When you create a service, you can apply content rules to it. The rules allow the CSS to direct or deny requests for content from the service.

To access service configuration mode, use the **service** command from global, circuit, IP, interface, and keepalive configuration modes. The prompt changes to (config-service [*name*]). You can also access another service from service configuration mode. For information about commands available in this mode, see the following commands.

Use the **no** form of this command to delete an existing service.

service *service_name*

no service *service_name*

Syntax Description

service_name	Name of a new service you want to create or an existing service you want to modify. Enter an unquoted text string with no spaces and a maximum length of 31 characters. To see a list of existing service names, enter: `service ?`

(config-service) access

To associate an FTP access mechanism with a service for moving content during publishing, subscribing, and demand-based replication activities, use the **access** command. Use the **no** form of this command to remove a service access mechanism.

access ftp *ftp_record*

no access ftp

Syntax Description

ftp_record	Name of an existing FTP record. Enter an unquoted text string with no spaces.

Usage Guidelines

You must use the **access** command for each service that offers publishing services. This command is optional for subscriber services; the subscriber service inherits the access mechanism from the publisher.

When you use this command to associate an FTP access mechanism to a service, the base directory of an existing FTP record becomes the tree root. To maintain coherent mapping between WWW daemons and FTP daemons, make the FTP access base directory equivalent to the WWW daemon root directory as seen by clients. For information on creating an FTP record, see the **(config) ftp-record** command.

Related Commands

(config) ftp-record

(config-service) active

To activate the specified service, use the **active** command. Activating a service puts it into the resource pool for load-balancing content requests.

active

Related Commands

(config-service) suspend

# (config-service) add ssl-proxy-list

To include an SSL proxy list as part of an SSL service, use the **add ssl-proxy-list** command. You can only add an SSL to a service that is an **ssl-accel** type. Activating a service puts it into the resource pool for load-balancing content requests.

add ssl-proxy-list *name*

Syntax Description

name	Name of a previously configured SSL proxy list. To see a list of existing SSL proxy lists, enter: `#(config-service) add ssl-proxy-list ?`

Related Commands

(config-service) remove ssl-proxy-list
(config-service) type ssl-accel

(config-service) bypass-hosttag

To allow the Client Side Accelerator (CSA) on the CSS to bypass a cache farm and establish a connection with the origin server to retrieve noncacheable content, use the **bypass-hosttag** command. The domain name from the host tag field is used to look up the origin IP address on the CSA. Use the **no** form of this command to disable the bypassing of cache for noncacheable content.

bypass-hosttag

no bypass-hosttag

Usage Guidelines

Before you can use this command, make sure that the service is suspended.

To bypass the cache farm for noncacheable content, you must also configure a service IP address of 0.0.0.0 and a keepalive type of **none**.

Related Commands

(config-service) ip address
(config-service) keepalive type none
(config-service) type

(config-service) cache-bypass

To disable applying content rules to requests originating from a proxy or transparent-cache type service when the CSS processes the requests, use the **cache-bypass** command. By default, no content rules are applied to requests from a proxy or transparent-cache type service. Use the **no** form of this command to apply content rules to requests from a proxy or transparent-cache type service.

cache-bypass

no cache-bypass

Related Commands

(config-service) type

(config-service) cookie

To specify the HTTP cookie for the service, use the **cookie** command. This command is replaced by the **(config-service) string** command.

cookie *cookie_name*

Syntax Description

cookie_name	Name of the cookie. Enter a unquoted text string with no spaces and a maximum length of 15 characters.

(config-service) domain

To specify the domain name to prepend to a requested piece of content when an HTTP redirect service generates an “object moved” message for the service, use the **domain** command. Use the **no** form of this command to clear the redirect domain for the service.

domain *domain_name*

no domain

Syntax Description

domain_name	Name of the domain. Enter a unquoted text string with no spaces and a maximum length of 64 characters. The CSS automatically prepends the domain name with http://. To disable the prepending of http:// to the domain name, use the **(config-service) prepend-http** command.

Usage Guidelines

The CSS uses the configured domain name in the redirect message as the new location for the requested content. The CSS prepends the domain name to the requested URL. If the domain name is not configured, the CSS uses the domain in the host-tag field from the original request. If no host tag is found, the CSS uses the IP address of the service to generate the redirect.

You can only use a service redirect domain on a service of type redirect.

Note The **domain** and **(config-service) redirect-string** commands are similar. The CSS returns the **(config-service) redirect-string** command string verbatim as configured. With the **domain** command, the CSS prepends the domain to the original requested URL. You cannot simultaneously configure the **domain** and **(config-service) redirect-string** commands on the same service.

Related Commands

show service
(config-service) prepend-http

(config-service) ip address

To specify the service IP address or a range of addresses, use the **ip address** command. Use the **no** form of this command to clear the IP address for a service and set it to its default value of 0.0.0.0.

ip address *ip_address* {**range** *number*}

no ip address

Syntax Description

ip_address	IP address for the service. Enter the address in dotted-decimal notation (for example, 192.168.11.1). The default is 0.0.0.0.
range *number*	(Optional) Allows you to specify a range of IP addresses starting with the IP address (*ip_address*). Enter a number from 1 to 65535. The default range is 1. For example, if you enter an IP address of 203.1.1.1 with a range of 10, the IP addresses range from 203.1.1.1 through 203.1.1.10.

Usage Guidelines

Before you can change the address, make sure that the service is suspended.

Some services do not require an IP address. Services that does not require an IP address are:

- Services configured with the **ssl-accel** service type
- Services configured with the **redirect** service type
- Services configured with the **bypass-hosttag** command

You must configure these services with a keepalive type of **none**.

Related Commands

(config-service) keepalive
(config-service) port
(config-service) type

(config-service) keepalive

To configure keepalive message parameters for the service, use the **keepalive** command. The options for this service mode command are:

- **keepalive frequency** - Specifies the keepalive message frequency
- **keepalive hash** - Specifies the MD5 hash for the keepalive
- **keepalive http-rspcode** - Specifies the response code expected from the HTTP daemon when the CSS issues a HEAD request
- **keepalive logging** - Configures script keepalive logging
- **keepalive maxfailure** - Specifies how many times the service can fail to respond to a keepalive message before it is considered offline
- **keepalive method** - Specifies the HTTP method for the service
- **keepalive port** - Specifies the keepalive port
- **keepalive retryperiod** - Specifies the keepalive retry period for the service
- **keepalive tcp-close** - Specifies the keepalive to close a TCP socket with a FIN or a RST
- **keepalive type** - Specifies the type of keepalive message, if any, appropriate for the service
- **keepalive uri** - Specifies the content information of the HTTP keepalive URI for the service

For more information on these options and associated variables, see the following commands.

Usage Guidelines

The CSS divides the keepalive types into two categories, Class A and Class B keepalives. The CSS supports a maximum of 2048 Class A keepalives. The CSS supports a maximum of 512 Class B keepalives. Table 2-3 lists the keepalive types in each class, the maximum number of each type, and the maximum number of each keepalive type that can execute concurrently.

Table 2-3 Keepalive Class, Types, and Limitations

Class	Type	CSS Maximum	Concurrent Maximum
A (The CSS limits 2048 keepalives per Class A.)	ICMP	2048	2048
	HTTP-HEAD non-persistent	2048	2048
	SSL (Hello)	2048	2048
	TCP	2048	2048
B (The CSS limits 512 keepalives per Class B.)	FTP	256	32
	HTTP-GET persistent and non-persistent	256	32
	HTTP-HEAD persistent	256	32
	Script	256	16

Caution For an 11500 series CSS, do not configure more than 2048 total keepalives, including a total of 512 Class B keepalives. Any services assigned to keepalives over the supported total number will not be eligible for content rule selection.

Configure global keepalives through the **(config) keepalive** command. Regardless of the number of services you assign to a global keepalive through the **(config-service) keepalive type named** command, the CSS always counts it as one keepalive.

For more information on configuring keepalives, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

keepalive frequency

To specify the keepalive message frequency, use the **keepalive frequency** command. Use the **no** form of this command to reset the frequency to its default value of 5.

keepalive frequency *frequency*

no keepalive frequency

Syntax Description

frequency	Time in seconds between sending keepalive messages to the service. Enter an integer from 2 to 255. The default is 5.

Usage Guidelines

For script keepalives, configure a higher frequency time value. A time interval of over 10 seconds ensures that the script keepalive has enough time to finish. Otherwise, state transitions may occur more often than usual.

If you configure more than 16 keepalives, the CSS automatically adjusts the keepalive frequency time to a value that best fits the resource usage. Note that this adjustment also affects the keepalive retry period value by adjusting that value to a number that is one-half the adjusted frequency time. If this occurs, you may observe in the running-configuration that your previously set keepalive frequency and retry period times change to a different value, as determined by the CSS.

The timeout for a keepalive is related to the configured keepalive frequency. In WebNS 5.1 and earlier versions, the timeout is equivalent to the keepalive frequency. In version 5.2, the timeout is one second less than the keepalive frequency.

Command Modes

Service

keepalive hash

To specify the MD5 hash for the keepalive, use the **keepalive hash** command. The keepalive process compares the hash with the computed hash of all HTTP GET responses. A successful comparison results in the keepalive maintaining an ALIVE state. Use the **no** form of this command to clear the hash value.

keepalive hash "*object***"**

no keepalive hash

Syntax Description

"*object*"	Object containing the MD5 hash in hexadecimal value for the keepalive. To determine the value for the hash, use the **show keepalive** command after you configure the keepalive without the hash option. Enter a quoted text string up to 32 characters.

Command Modes

Service

Related Commands

show keepalive

keepalive http-rspcode

To specify the response code expected from the HTTP daemon when the CSS issues a HEAD request, use the **keepalive http-rspcode** command. This command could be helpful for checking a redirect by specifying the 302 response code, or triggering another non-200 HTTP response code. Use the **no** form of the command to reset the response code to its default value of 200.

keepalive http-rspcode *value*

no keepalive http-rspcode

Syntax Description

value	Response code expected from the HTTP daemon. Enter the response code as an integer from 100 to 999. The default is 200.

Command Modes

Service

Related Commands

(config-keepalive) http-rspcode

keepalive logging

To specify where to either capture the output from a script keepalive or turn off script keepalive logging, use the **keepalive logging** command.

keepalive logging *log_filename*|**none**

Syntax Description

log_filename	Name of the log file where you want to log the output from a script keepalive. This file is saved in the log directory on the CSS disk. Enter an unquoted text string with a maximum of 32 characters.
none	Turns off script keepalive logging.

Command Modes

Service

Related Commands

(config-service) keepalive type

keepalive maxfailure

To specify the number of times the service can fail to respond to a keepalive message before being considered dead, use the **keepalive maxfailure** command. Use the **no** form of this command to reset the maximum failure number to its default value of 3.

keepalive maxfailure *number*

no keepalive maxfailure

Syntax Description

number	Maximum failure number. Enter an integer from 1 to 10. The default is 3.

Command Modes

Service

keepalive method

To specify the HTTP keepalive method for the service, use the **keepalive method** command.

keepalive method get|head

Syntax Description

get	Uses the get method. The CSS issues a HTTP GET method to the service, computes a hash value on the page, and stores the hash value as a reference hash. Subsequent GETs require a 200 OK status (HTTP command completed OK response) and the hash value to equal the reference hash value. If the 200 OK status is not returned, or if the 200 OK status is returned but the hash value is different from the reference hash value, the CSS considers the service down. When you specify the content information of an HTTP Uniform Resource Identifier (URI) for an HTTP keepalive, the CSS calculates a hash value for the content. If the content information changes, the hash value no longer matches the original hash value and the CSS assumes that the service is down. To prevent the CSS from assuming that a service is down due to a hash value mismatch, specify the **keepalive method** as **head**.
head	Uses the head method (default). The CSS issues a HTTP HEAD method to the service and a 200 OK status is required. The CSS does not compute a reference hash value for this type of keepalive. If the 200 OK status is not returned, the CSS considers the service down.

Command Modes

Service

Usage Guidelines

If you change the keepalive method on an active service, suspend and reactivate the service for the change to take effect.

keepalive port

To define a port number for the keepalive, use the **keepalive port** command. Use the **no** form of this command to reset the keepalive port to its default setting.

keepalive port *number*

no keepalive port

Syntax Description

number	Port number for the keepalive. Enter the number as an integer from 0 to 65535. The default setting is based on the configured service port number. Otherwise, the default setting is based on the keepalive type. If the keepalive type is: • Not configured - The default port number is 0 • HTTP or TCP - The default port number is 80 • FTP - The default port number is 21

Command Modes

Service

Usage Guidelines

If you do not configure the port, the keepalive uses the service port configured with the **(config-service) port** command. If you do not configure either port, the keepalive is based on the configured keepalive type.

Related Commands

(config-service) keepalive type

keepalive retryperiod

To specify the keepalive retry period for the service, use the **keepalive retryperiod** command. Use the **no** form of this command to reset the retry period to its default value of 5.

keepalive retryperiod *period*

no keepalive retryperiod

Syntax Description

period	Time in seconds between sending retry messages to the service. Enter an integer from 2 to 255. The default is 5.

Command Modes

Service

Usage Guidelines

When a service has failed to respond to a given keepalive message (the service is now transitioned to the dying state), the retry period specifies how frequently the CSS tests the service to see if it is functional.

keepalive tcp-close

To specify the keepalive to close a TCP socket with a FIN or a RST, use the **keepalive tcp-close** command.

keepalive tcp-close [**fin**|**rst**]

Syntax Description

fin	Specifies that the keepalive closes the TCP socket with a FIN rather than a RST
rst	Specifies that the keepalive closes the TCP socket with a RST (default)

Command Modes

Service

Usage Guidelines

By default and in compliance with RFC 1122, the CSS sends a reset (RST) to close the socket on a server port for TCP keepalives. A RST is faster than a FIN, because a RST requires only one packet, while a FIN can take up to four packets. If your servers require a graceful closing of a socket using a FIN, use the **keepalive tcp-close fin** command.

The **keepalive tcp-close fin** and keepalive mode **tcp-close** fin commands may be applied to a total of 100 TCP keepalives.

Related Commands

(config-service) keepalive type

keepalive type

To specify the type of keepalive message, if any, appropriate for the service, use the **keepalive type** command.

keepalive type [**ftp** *ftp_record*|**http** {**non-persistent**}|**icmp**|**none**
|**script** *script_name* {**"***arguments***"**} {**use-output**}|**ssl**|**tcp**]

Syntax Description

ftp *ftp_record*	Defines a keepalive method in which the CSS logs in to an FTP server as defined in the FTP record file. Enter the name of an existing FTP record for the FTP server as an unquoted text string with no spaces. To create an FTP record, use the **(config) ftp-record** command.
http {**non-persistent**}	Defines an HTTP index page request. By default, HTTP keepalives attempt to use persistent connections. To disable this behavior, include the **non-persistent** option.
icmp	Defines an ICMP echo message (default).
named *name*	Defines a global keepalive defined in keepalive configuration mode. To view a list of defined keepalive names, enter: `keepalive type named ?` Before using this command, make sure that the keepalive is activated through the **(config-service) active** command. Assigning this global keepalive to a service overrides any keepalive properties configured in service mode.
none	Do not send keepalive messages to the service.
script *script_name*	Defines a script keepalive is to be used by the service. The script is played every time the keepalive is issued. Enter the name of the script keepalive. To view a list of scripts, enter: `keepalive type script ?`

"*arguments*"	(Optional) Arguments to pass into the keepalive script. Enter a quoted text string with a maximum of 128 characters including spaces.
use-output	(Optional) Allows the script to parse the output for each executed command. This optional keyword allows the use **grep** and file direction within a script. By default, the script does not parse the output.
ssl	SSL HELLO keepalives for this service. Use this keepalive for all backend services supporting SSL. The CSS sends a client HELLO to connect the SSL server. After the CSS receives a HELLO from the server, the CSS closes the connection with a TCP RST. When the CSS is using an SSL module, use the keepalive type of **none**. The SSL module is an integrated device in the CSS and does not require the use of keepalive messages for the service.
tcp	Defines the TCP connection handshake request. To define a port for a TCP keepalive, use the **(config-service) keepalive port** command.

Usage Guidelines

The CSS divides the keepalive types into two categories, Class A and Class B keepalives. The CSS supports a maximum of 2048 Class A keepalives. The CSS supports a maximum of 512 Class B keepalives. Table 2-4 lists the keepalive types in each class, the maximum number of each type, and the maximum number of each keepalive type that can execute concurrently.

Table 2-4 Keepalive Class, Types, and Limitations

Class	Type	CSS Maximum	Concurrent Maximum
A (The CSS limits 2048 keepalives per Class A.)	ICMP	2048	2048
	HTTP-HEAD non-persistent	2048	2048
	SSL (Hello)	2048	2048
	TCP	2048	2048

Table 2-4 Keepalive Class, Types, and Limitations (continued)

Class	Type	CSS Maximum	Concurrent Maximum
B	FTP	256	32
(The CSS limits 512 keepalives per Class B.)	HTTP-GET persistent and non-persistent	256	32
	HTTP-HEAD persistent	256	32
	Script	256	16

Caution For an 11500 series CSS, do not configure more than 2048 total keepalives, including a total of 512 Class B keepalives. Any services assigned to keepalives over the supported total number will not be eligible for content rule selection.

When the CSS is using an SSL module, use the keepalive type of **none**. The SSL module is an integrated device in the CSS and does not require the use of keepalive messages for the service.

The **keepalive tcp-close fin** and keepalive mode **tcp-close** fin commands may be applied to a total of 100 TCP keepalives.

Command Modes

Service

keepalive uri

To specify the HTTP keepalive content information for the service, use the **keepalive uri** command. Use the **no** form of this command to clear the content information of the URI for the service.

keepalive uri "*uri***"**

no keepalive uri

Syntax Description

uri	The HTTP keepalive URI for the service. Enter the content information of the URI as a quoted text string with a maximum of 64 characters. Do not include the host information in the string. The CSS derives the host information from the service IP address and the keepalive port number.

Usage Guidelines

When you specify the content information of a URI for an HTTP keepalive, the CSS calculates a hash value for the content. If the content information changes, the hash value no longer matches the original hash value and the CSS assumes that the service is down. To prevent the CSS from assuming that a service is down due to a hash value mismatch, define **keepalive method** as **head**. The CSS does not compute a hash value for this type of keepalive.

If you specify a Web page with changeable content and do not specify the head keepalive method, you must suspend and reactivate the service each time the content changes.

Command Modes

Service

(config-service) load

To configure a load on a service and bypass the CSS load calculation method (relative or absolute), use the **load** command in service configuration mode. Use the **no** form of the command to reset the load value to the default of 2.

load *number*

no load

Syntax Description

number	Load value that you assign to a service. A service with a higher load number receives fewer hits than a service with a lower load number. The CSS considers a service with a load of 254 as unavailable, and, therefore, the service receives no hits. Enter an integer from 2 to 254. The default is 2.

Command Modes

Service

Usage Guidelines

To use the **load** command, you must disable global load reporting by entering the **no load reporting** command in global configuration mode. Do not reenable load reporting. If you do, the load value you entered with the **load** command will no longer apply to the service. To recover, you must then disable load reporting and reenter the **load** command on the service at the CLI.

Use the **load** command with the ACA load-balancing method when you want to take into account server load parameters, for example:

- CPU utilization
- Free memory
- Application threads
- Other server tasks

You can set the **load** command value with your application or server using SNMP or the CSS XML interface. For information about ACA, refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*. For information about SNMP and the XML interface, refer to the *Cisco Content Services Switch Administration Guide*.

Related Commands

(config-service) show load

(config-service) max age

To define the maximum age for replicated objects on services defined as type **rep-cache-redir**, **rep-store**, or **rep-store-redir**, use the **max age** command. The CSS deletes the dynamic content rule after the maximum age time elapses. Use the **no** form of this command to set the maximum age for replicated objects to its default value of 120.

max age *minutes*

no max age

Syntax Description

minutes	Maximum time in minutes. Enter a number from 1 to 1440. The default value is 120.

(config-service) max connections

To define the maximum number of TCP connections on the services, use the **max connections** command. Use the **no** form of this command to set the maximum TCP connections to the default of 65534.

max connections *number*

no max connections

Syntax Description

number	Maximum number of TCP connections on the service. Enter the maximum number of connections from 6 to 65534. The default is 65534, which indicates that there is no limit on the number of connections.

Usage Guidelines

Do not use service max connections on UDP content rules. The service connection counters do not increment and remain at 0 because UDP is a connectionless protocol.

(config-service) max content

To define the maximum pieces of content for replication on services defined as type **rep-cache-redir**, **rep-store**, or **rep-store-redir**, use the **max content** command. Use the **no** form of this command to set the maximum content to its default value of 100.

max content *number*

no max content

Syntax Description

number	Maximum content for replication. Enter a number from 1 to 65535. The default is 100.

(config-service) max usage

To define the maximum disk space allowed for replication on services defined as type **rep-cache-redir**, **rep-store**, or **rep-store-redir**, use the **max usage** command. Use the **no** form of this command to set the maximum disk space to its default value of 1 megabyte.

max usage *mbytes*

no max usage

Syntax Description

mbytes	Maximum disk space in megabytes. Enter a number from 1 to 1000. The default is 1.

(config-service) no

To negate a command or set it to its default, use the **no** command. For information on general **no** commands you can use in this mode, see the general **no** command. The following option is available in service mode.

Syntax Description

no access ftp	Removes the service access mechanism.
no acl *index*	Deletes an ACL.
no bypass-hosttag	Disables the bypassing of cache for noncacheable content.
no cache-bypass	Allows the applying of content rules to requests from a proxy or transparent cache service.
no domain	Clears the redirect domain for the service.
no ip address	Clears the IP address for the service and sets it to its default value of 0.0.0.0.
no keepalive frequency	Resets the keepalive frequency to its default value of 5 seconds.
no keepalive hash	Clears the keepalive MD5 hash object.
no keepalive http-rspcode	Resets the response code to its default value of 200.
no keepalive maxfailure	Resets the keepalive maximum failures to its default value of 3.
no keepalive port	Resets the keepalive port to its default setting based on the configured service port. Otherwise, the default setting is based on the configured keepalive type.
no keepalive retryperiod	Resets the keepalive retry period to its default value of 5 seconds.
no keepalive uri	Clears the content information for the HTTP keepalive URI.
no load	Resets the manually configured load value on a service to the default of 2.
no max age	Resets the maximum age for replicated content to the default of 120 minutes.

no max content	Resets the maximum content for replication to the default of 100 pieces.
no max usage	Resets the maximum disk space allowed for replication to the default of 1 megabyte.
no owner *existing_owner_name*	Deletes an existing owner.
no port	Resets the IP port for the service to the default of **any**.
no prepend-http	Disables the prepending of http:// on string configured through the **(config-service) redirect-string** and **(config-service) domain** commands for the service.
no protocol	Resets the IP protocol for the service to the default of **any**.
no publisher	Removes publishing on a service.
no publisher interval	Disables the publisher resynchronization interval by setting it to its default of 0.
no redirect-string	Removes the redirect string from the service.
no redundant-index	Disables redundancy on the service.
no string	Removes the cookie from the service.
no subscriber	Unsubscribes the service from a publishing service.
no transparent-hosttag	Disables destination NATing for the transparent cache service type.
no type	Resets the type for the service to its default setting of local.
no weight	Resets the service weight to its default setting of 1.

(config-service) port

To specify the service TCP/UDP port number or a range of port numbers, use the **port** command. Use the **no** form of this command to reset the port to **any**.

port *number1* {**range** *number2*}

no port

Syntax Description

number1	TCP or UDP destination port number associated with a service. Enter the number from 0 to 65535. The default is **any**.
range *number2*	(Optional) Allows you to specify a range of ports starting with the port *number1*. Enter a number from 1 to 65535. The default range is 1. For example, if you enter a port number of 101 with a range of 10, the ports range from 101 through 110.

Usage Guidelines

Before you can change the port, make sure that the service is suspended.

Related Commands

(config-service) ip address
(config-service) protocol

(config-service) prepend-http

To enable the prepending of http:// to a redirect string configured through the **(config-service) redirect-string** command, or a domain configured through the **(config-service) domain** command for the service. By default, prepending is enabled. Use the **no** form of this command to disable the prepending of http://.

prepend-http

no prepend-http

Related Commands

(config-service) domain
(config-service) redirect-string

(config-service) protocol

To specify the service IP protocol, use the **protocol** command. The default setting for this command is **any**, for any IP protocol. Use the **no** form of this command to reset the protocol to the default of **any**.

protocol tcp|udp

no protocol

Syntax Description

tcp	Uses the TCP protocol suite.
udp	Uses the UDP protocol suite.

Usage Guidelines

Before you can change the protocol, make sure that the service is suspended.

Related Commands

(config-service) ip address
(config-service) keepalive type
(config-service) port

(config-service) publisher

To configure a service as a publishing service and define its synchronization interval, use the **publisher** command. Use the **no** form of this command to remove publishing on a service or disable the publisher resynchronization interval by setting it to its default of 0.

publisher {**interval** *minutes* {*trigger_file*}}

no publisher {**interval**}

Syntax Description

interval	(Optional) Defines a recurrent interval in minutes to synchronize content among the subscribers. You can only enter this command after you configure the service as a publishing service. When this option is used with the no form of the command, it disables the publisher resynchronization interval by setting it to its default of 0
number	Synchronization interval in minutes. Enter the number from 0 to 3600. The default is 0 which disables the interval.
trigger_file	(Optional) Path and filename to a file, when modified, triggers the publishing service to synchronize the content among the subscribers. Enter an unquoted character string with a maximum of 64 characters.

Usage Guidelines

Use the **publisher** command to configure a service as a publishing service.

A publishing service can synchronize content among associated subscriber services. To move the content during publishing activities, configure an access mechanism by using the **(config-service) access** command.

When you define the interval to synchronize the subscriber, the interval begins at the time that you enter the command. Subscribers that are unavailable for synchronization are placed in an offline state and retried until the operation is completed.

The publisher service does not become active until it has at least one configured subscriber. You do not need to configure the publisher before configuring the subscriber, but the publisher must be configured before the subscriber can receive any content synchronization updates.

Related Commands

replicate
(config) ftp-record
(config-service) access
(config-service) subscriber

(config-service) redirect-string

To specify an HTTP redirect string to be used when an HTTP redirect service generates an "object moved" message for the service, use the **redirect-string** command. Use the **no** form of this command to remove the redirect string from the service.

redirect-string *string*

no redirect-string

Syntax Description

string	HTTP redirect string. Enter a quoted or an unquoted text string with no spaces and a maximum of 252 characters. The CSS automatically prepends the string with http://. To disable the prepending of http:// to the string, use the **(config-service) prepend-http** command.

Usage Guidelines

The CSS uses the entire configured redirect string as the new location for the requested content. If no string is configured, the CSS prepends the domain configured with the **(config-service) domain** command to the original request. If neither the redirect string nor the domain name is configured, the CSS uses the domain in the host-tag field from the original request combined with the requested HTTP content URL. If no host tag is found, the CSS uses the IP address of the service to generate the redirect.

Note You can use a redirect string only on a service of type redirect.

Note The **redirect-string** and **(config-service) domain** commands are similar. The CSS returns the **redirect-string** command string verbatim as configured. However, the CSS prepends the domain configured with the **(config-service) domain** command to the original requested URL. You cannot simultaneously configure the **redirect-string** and **(config-service) domain** commands on the same service.

Related Commands

(config-service) prepend-http

(config-service) redundant-index

To configure the global content index for a redundant service, use the **redundant-index** command. A CSS uses the global content index to keep track of redundant services and associated flow state information. Use the **no** form of this command to disable redundancy on the service.

redundant-index *number*

no redundant-index

Syntax Description

number	Redundant index for the service. Enter a unique integer from 0 to 32767, where a value of 0 disables ASR for a service. The default is 0, but it does not appear in the running-config even if you configure it explicitly.

Usage Guidelines

If you enter the **no redundant-index** command on an active redundant service for live redundancy peers, the command automatically suspends the service. Flows already mapped by a CSS are not affected. However, if a failover occurs during the life of an active flow that matches on such a suspended service, the backup CSS cannot map the flow because it cannot find the service with the same global index as that on the original master.

Note For implicit or explicit Layer 5 rules, where there is delayed binding, binding is not complete until the CSS processes the SYN/ACK from the server. This means that, if a failover occurs in the middle of a spanned content request, the master CSS will not receive the SYN/ACK from the server and the flow will not be replicated on the backup CSS. No data is lost and users can simply refresh their browsers to restart the connection.

For information on redundant indexes and configuring Adaptive Session Redundancy (ASR) on 11500 series CSS peers, including requirements and restrictions that apply to both CSS peers in an ASR configuration, refer to the *Cisco Content Services Switch Redundancy Configuration Guide*.

Related Commands

(config-group) redundant-index
(config-owner-content) redundant-index
(config-service) ip address

(config-service) remove ssl-proxy-list

To remove an SSL proxy list that is part of an SSL service, use the **remove ssl-proxy-list** command. Removing a service removes it from the resource pool for load-balancing content requests.

remove ssl-proxy-list *name*

Syntax Description

name	Name of a previously configured SSL proxy list.

Related Commands

(config-service) add ssl-proxy-list

(config-service) session-cache-size

To reconfigure the size of the SSL session ID cache for the service, use the **session-cache-size** command. The cache size is the maximum number of SSL session IDs that can be stored in a dedicated session cache on the SSL module. Use the **no** form of this command to reset the cache to its default value of 10000.

session-cache-size *sessions*

no session-cache-size

Syntax Description

sessions	Number of sessions in the SSL session ID cache. Enter a number from 0 to 100000. A value of 0 disables the cache.

Usage Guidelines

If you disable the SSL session cache by setting it to 0, ensure the following are properly configured to turn off the use of SSL session ID:

- Set the **ssl-server** *number* **session-cache timeout** setting for the SSL proxy list to 0 (disabled).
- Disable the **advanced-balance ssl** command in the content rule to disable SSL sticky.

The backend session ID cache is set to 4096 entries and is not configurable.

(config-service) slot

To specify the slot in a CSS in which the SSL Acceleration module is located, use the **slot** command. The SSL service requires the SSL module slot number to correlate the SSL proxy list to a specific module. The CSS 11501 supports a single integrated SSL module. The CSS 11503 and CSS 11506 support multiple SSL modules; a maximum of two in a CSS 11503 and a maximum of four in a CSS 11506.

slot *number*

Syntax Description

number	Slot number. The valid entry for the CSS 11501 is 2. The valid entries for the CSS 11503 are 2 and 3. The valid entries for the CSS 11506 CSS are 2 to 6. Slot 1 is reserved for the SCM.

Usage Guidelines

The CSS supports one active SSL service for each SSL module in the CSS (one SSL service per slot). You can configure more than one SSL service for a slot but only a single SSL service can be active at a time.

(config-service) string

To specify the HTTP cookie for the service, use the **string** command. Use the **no** form of this command to remove the cookie for the service.

string *cookie_name*

no string

Syntax Description

cookie_name	Name of the cookie. Enter a unquoted text string with no spaces and a maximum length of 15 characters.

(config-service) subscriber

To configure a service as a subscriber to a publishing service, use the **subscriber** command. Use the **no** form of this command to unsubscribe the service from a publishing service.

subscriber *publisher*

no subscriber

Syntax Description

publisher	Name of the publishing service

Usage Guidelines

By default, the subscriber inherits the access mechanism of the publisher for the movement of content. But if you want to configure an alternative mechanism, use the **(config-service) access** command.

You can define a maximum of 31 subscribers to a publisher.

Related Commands

(config) ftp-record
(config-service) access
(config-service) publisher

(config-service) suspend

To remove the service from the pool for future load-balancing content requests, use the **suspend** command. Suspending a service does not affect existing content flows, but it does prevent additional connections from accessing the service for its content.

suspend

Usage Guidelines

If you suspend a service, the CSS uses the **failover** command setting to handle content requests.

Related Commands

(config-service) active

(config-service) transparent-hosttag

To enable destination network address translation (NAT) for the transparent cache service type, use the **transparent-hosttag** command. Use the **no** form of this command to disable destination network address translation for the transparent cache service type.

transparent-hosttag

no transparent-hosttag

Usage Guidelines

Before you can use this command, make sure that the service is suspended.

Currently, you can use this command only in a CSA environment.

You do not need to configure source groups in a CSA environment. The transparent cache environment does not require the client source IP NATing that occurs as a result of a source group configuration.

Related Commands

(config-service) type

(config-service) type

To specify the type for the service, use the **type** command. If you do not define a type for the service, the default service type is local. Use the **no** form of this command to reset the type for the service to its default setting of local.

type nci-direct-return|nci-info-only|proxy-cache|redirect |redundancy-up|rep-cache-redir|rep-store|rep-store-redir|ssl-accel |ssl-accel-backend|ssl-init|transparent-cache

no type

Syntax Description

nci-direct-return	Specifies a NAT Channel Indication (NCI) service for NAT peering. NAT peering allows the building of forward TCP-switched connections between CSSs until the destination CSS is reached and the destination CSS performs the final transformations, which allows return traffic packets to flow to the client through any network path. This service type informs the CSS to include the NCI option in the TCP packet. This keyword indicates to the server-side CSS that NAT parameters are in use and contains the original source and destination IP addresses and TCP port numbers. If a Layer 5 rule is matched, the spoof bit in the NCI option is set to indicate that part of the flow has been spoofed and the rest of the forward path must be established before the destination CSS can use the information in the packet to perform the NAT transformations for the reverse path. Configure the VIP for the service to the VIP on the server-side CSS to indicate an endpoint for the connection. You must create a source group for the client traffic. The CSS will translate the client IP address to the IP address defined in the source group.
nci-info-only	Specifies the service is NAT Channel indication for information only.

proxy-cache	Specifies the service is a proxy cache. This keyword bypasses content rules for requests from the cache. Bypassing content rules prevents a loop from forming between the cache server and the CSS. To allow the applying of content rules to requests, enter: `no cache-bypass`
redirect	Specifies the service is not directly accessible and requires redirection. The CSS must use the HTTP redirect mechanism to direct the client request to the desired content.
redundancy-up	Designates one or more routers as type redundancy-up critical services. A typical configuration contains 10 or fewer routers. Within a redundant configuration, the CSS allows you to configure multiple redundancy uplink critical services (up to a maximum of 512). This critical service type enables the master CSS to ping a router service using the default keepalive Internet Control Message Protocol (ICMP). If the master CSS fails or it detects that all router uplink critical services have failed, the backup CSS becomes the master. In a redundant configuration that does not configure the routers as type redundancy-up critical services, a backup CSS becomes master only when the current master CSS fails. In this configuration, a switchover *does not* occur when the router services fail. You cannot add redundancy uplink critical services to a content rule. You cannot use this service type and the **(config) ip redundancy master** command simultaneously. Before you can specify a redundant uplink, you must enter the **(config) no ip redundancy master** command.
rep-cache-redir	Specifies the service is a replication cache with redirect. The CSS uses the replication cache as a redirect service instead of load balancing between the local service and the cache.

rep-store	Specifies the service is a replication store server for hot content. The service is a local overflow service used to load-balance content requests. The CSS moves hot content to the server, and then creates a dynamic content rule for the hot content automatically. The dynamic content rule inherits all the attributes of the existing rule with the following changes: • Specifically identifies the hot content • Changes the server type from replication-store to type local The CSS deletes the dynamic content rule after the maximum age time elapses or the service keepalive indicates failure.
rep-store-redir	Specifies the service is a replication store to which content requests are redirected. The service is a remote overflow service. No content rules are applied to requests from this service type.
ssl-accel	Specifies that this is an SSL acceleration service. You add an active SSL proxy list to an **ssl-accel** type service to initiate the transfer of SSL configuration data for the SSL module. This allows you to: • Configure the service as an SSL acceleration service. • Add the SSL proxy list to an SSL service through the **(config-service) add ssl-proxy-list** command.
ssl-accel-backend	Specifies that this is a backend SSL service. You add an active SSL proxy list to an **ssl-accel-backend** type service to initiate the transfer of SSL configuration data for the SSL module. This allows you to: • Configure the service as a backend SSL service. • Add the SSL proxy list to an SSL service through the **(config-service) add ssl-proxy-list** command.

ssl-init	Specifies that this is an SSL initiation service. You add an active SSL proxy list to an **ssl-init** type service to initiate the transfer of SSL configuration data for the SSL module. This command allows you to: • Configure the service as an SSL initiation service. • Add the SSL proxy list to an SSL service through the **(config-service) add ssl-proxy-list** command.
transparent-cache	Specifies the service is a transparent cache. No content rules are applied to requests from the cache. Bypassing content rules prevents a loop from forming between the cache server and the CSS. To allow the applying of content rules to requests, enter: **`no cache-bypass`**

Usage Guidelines

Before you can change the type, make sure that the service is suspended.

(config-service) weight

To specify the relative weight of the service, use the **weight** command. The weight is used in ArrowPoint Content Awareness (ACA) and weighted roundrobin load-balancing decisions. Use the **no** form of this command to reset the service weight to its default value of 1.

weight *weight*

no weight

Syntax Description

weight	Service weight used with load metrics to make load-allocation decisions. You can use the weight to bias flows toward the specified service. Enter an integer from 0 to 10. The default is 1.

Usage Guidelines

The weight for the service set through the **(config-owner-content) add service** command takes precedent over the **(config-service) weight** command. For information about using a service weight of 0 (graceful shutdown), refer to the *Cisco Content Services Switch Content Load-Balancing Configuration Guide*.

Related Commands

(config-owner-content) add service
(config-owner-content) balance

(config-service) zero

To set statistics counters for all or specified services on the CSS to zero, use the **zero** command. The **show service** command displays the counters.

zero total-connections|total-reused-connections|state-transitions {**service** *name*}

Syntax Description

total-connections	Sets the Total Connections counter for all services or a specified service to zero.
total-reused-connections	Sets the Total Reused Conns counter for all services or a specified service to zero.
state-transitions	Sets the State Transitions counter for all services or a specified service to zero.
service *name*	(Optional) Name of the service. Only the counter for the specified service is set to zero.

Command Modes

All modes

Related Commands

show service

SSL-Proxy-List Configuration Mode Commands

The ssl-proxy list configuration mode allows you to configure an SSL proxy configuration list on a CSS containing an SSL Acceleration module. An SSL proxy configuration list is a group of related virtual or back-end SSL servers that are associated with an SSL service. The SSL modules in the CSS use the virtual servers to properly process and terminate SSL communications between the client and the Web server. The SSL module uses the back-end SSL servers to initiate a connection between the module and the back-end SSL server.

To access ssl-proxy-list configuration mode, use the **ssl-proxy-list** command from any configuration mode except from the ACL, boot, group, RMON, or owner configuration modes. The prompt changes to (ssl-proxy-list [*name*]). You can also use this command from this mode to access another SSL proxy list. For information about commands available in this mode, see the commands in this section.

In global configuration mode, use the **no** form of this command to remove an existing SSL-proxy list.

ssl-proxy-list *name*

(config) **no ssl-proxy-list** *name*

Syntax Description

name	Name of a new SSL proxy list you want to create or an existing list you want to modify. Enter an unquoted text string with no spaces and a maximum length of 31 characters. To see a list of existing names, enter: `(config)# ssl-proxy-list ?`

Usage Guidelines

You add an active SSL proxy list to a service (an **ssl-accel** type for a virtual SSL server and an **ssl-accel-backend** type for a back-end SSL server) to initiate the transfer of SSL configuration data for the SSL Acceleration Module. The SSL services are added to SSL content rules.

You cannot delete an SSL proxy list if an SSL service is in use and contains the active SSL proxy list. You must first suspend the SSL service to delete a specific list.

Each SSL proxy list can have a maximum of 256 virtual or back-end SSL servers.

Each service may have only one SSL proxy list configured on it. You may only have one active SSL service for each slot in the chassis. You can configure more than one on a slot but only one can be activated at a time.

Content rules can have multiple SSL services.

For detailed information on SSL and SSL proxy lists, refer to the *Cisco Content Services Switch SSL Configuration Guide*.

Related Commands

show ssl-proxy-list
(config-service) add ssl-proxy-list
(config-service) remove ssl-proxy-list
(config-service) slot

(ssl-proxy-list) active

To activate the specified SSL proxy list, use the **active** command.

active

Usage Guidelines

Before you can activate an SSL proxy list, ensure that you create at least one server in the list. The CSS checks the SSL proxy list servers to verify that all of the necessary components are configured, including verifying the certificate and key pair against each other. If the verification fails, the certificate name is not accepted and the CSS logs the following error message and does not activate the SSL proxy list.

```
Certificate and key pair do not match
```

You must either remove the configured key pair or configure an appropriate certificate.

You cannot modify an active SSL proxy list. You must first suspend the SSL proxy list to make modifications to any server in the list. Once you have modified the SSL proxy list, suspend the SSL service, activate the SSL proxy list, and then activate the SSL service.

Related Commands

(ssl-proxy-list) suspend

(ssl-proxy-list) backend-server

To create a back-end SSL server and configure it for an SSL proxy list, use the **backend-server** *number* command. Use the **no** form of the **backend-server** *number* command to delete the back-end server. For information on the other **no** forms of this command, see the commands in the following sections.

backend-server *number* {**cacert**...|**cipher**...|**dhparam**...|**dsacert**...|**dsakey**...
|**handshake**...|**ip address**...|**port**...|**rsacert**...|**rsakey**...|**server-ip**...
|**server-port**...|**session-cache**...|**tcp**...|**type**...|**version**...}

no backend-server *number* {**cacert**...|**cipher**...|**dhparam**...|**dsacert**...
|**dsakey**...|**handshake**...|**ip address**...|**port**...|**rsacert**...|**rsakey**...
|**server-ip**...|**server-port**...|**session-cache**...|**tcp**...|**type**...|**version**...}

Syntax Description

number	The index number for the SSL server. This variable without an option creates a back-end server. When you enter this variable with an option, the number identifies the server for configuration. An SSL proxy list can have a maximum of 256 servers. Enter a number from 1 to 256.
cacert...	(Optional) Specifies the certificate authority (CA) certificate of the SSL server. See the **backend-server number cacert** command.
cipher...	(Optional) Specifies the cipher suite for the server. See the **backend-server number cipher** command.
dhparam...	(Optional) Specifies the Diffie-Hellman parameter file for the back-end server. See the **backend-server number dhparam** command.
dsacert...	(Optional) Specifies the back-end server DSA certificate. See the **backend-server number dsacert** command.
dsakey...	(Optional) Specifies the back-end server DSA key name. See the **backend-server number dsakey** command.
handshake...	(Optional) Specifies the handshake negotiation data and timeout value for the server. See the **backend-server number handshake** command.

ip address...	(Optional) Specifies an IP address for the server. This IP address corresponds to the address of the service. See the **backend-server number ip address** command.
port...	(Optional) Specifies a virtual TCP port for the server. See the **backend-server number port** command.
rsacert...	(Optional) Specifies the back-end server RSA certificate. See the **backend-server number rsacert** command.
rsakey...	(Optional) Specifies the back-end server RSA key pair name. See the **backend-server number rsakey** command.
server-ip	(Optional) Specifies the IP address for the back-end SSL server. See the **backend-server number server-ip** command.
server-port	(Optional) Specifies the port for the back-end SSL server. See the **backend-server number server-port** command.
session-cache...	(Optional) Specifies the session cache timeout value for the server. See the **backend-server number session-cache** command.
tcp...	(Optional) Specifies a timeout value to terminate a TCP connection or specifies the Nagle algorithm for a TCP connection. See the **backend-server number tcp** command.
type...	(Optional) Specifies that the back-end server is either a back-end SSL server or an SSL initiation server. See the **backend-server number type** command.
version...	(Optional) Specifies the SSL or Transport Layer Security (TLS) protocol version. See the **backend-server number version** command.

Usage Guidelines

You must create a back-end SSL server before you can configure its parameters.

backend-server *number* cacert

To configure the certificate authority (CA) certificate, use the **backend-server** *number* **cacert** *name* command. Configuring this command in the SSL proxy list allows the CSS to use the public key in the CA certificate to verify the digital signature of the CA in the SSL server certificate. Use the **no** form of this command to remove the configured CA certificate from the SSL proxy list.

backend-server *number* **cacert** *name*

no backend-server *number* **cacert**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
cacert	Specifies a CA certificate.
name	Name of the CA certificate. Enter an unquoted text string from 1 to 31 characters.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

The CA certificate must already be loaded on the SCM. If the certificate name does not exist, the CSS logs an error message.

Related Commands

show ssl-proxy-list
(ssl-proxy-list) active

backend-server *number* cipher

To assign a cipher suite to the back-end SSL server, use the **backend-server** *number* **cipher** command. For each available SSL version, there is a distinct list of supported cipher suites representing a selection of cryptographic algorithms and parameters. Your choice depends on your environment, certificates and keys in use, and security requirements. By default, all supported cipher suites are enabled. Use the **no** form of this command to remove a cipher suite from the server.

backend-server *number* **cipher** *name* {**weight** *number*}

no backend-server *number* **cipher**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
name	The name of a specific cipher suite. See the “Usage Guidelines” section.
weight *number*	(Optional) Assigns a priority to the cipher suite, with 10 being the highest weight. When negotiating which cipher suite to use, the SSL module selects from the client list based on the cipher suite configured with the highest weight. To set the weight for a cipher suite, enter a number from 1 to 10. By default, all configured cipher suites have a weight of 1.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

Table 2-5 lists all supported cipher suites and values for the specific SSL server (and corresponding SSL proxy list). The table also lists whether those cipher suites are exportable from the CSS, along with the authentication certificate and encryption key required by the cipher suite.

If you use the default setting or select the **all-cipher-suite** option, the CSS sends the suites in the same order as they appear in Table 2-5, starting with rsa-with-rc4-128-md5.

Note The **all-cipher-suites** setting works only when no specifically-defined ciphers are configured. To return to using the **all-cipher-suites** setting, you must remove all specifically-defined ciphers.

Caution The dh-anon series of cipher suites are intended for completely anonymous Diffie-Hellman communications in which neither party is authenticated. Note that this cipher suite is vulnerable to man-in-the-middle attacks and is strongly discouraged.

Table 2-5 SSL Cipher Suites Supported by the CSS

Cipher Suite	Exportable	Authentication Certificate Used	Key Exchange Algorithm Used
all-cipher-suites	No	RSA certificate, DSA certificate	RSA key exchange, Diffie-Hellman
rsa-with-rc4-128-md5	No	RSA certificate	RSA key exchange
rsa-with-rc4-128-sha	No	RSA certificate	RSA key exchange
rsa-with-des-cbc-sha	No	RSA certificate	RSA key exchange
rsa-with-3des-ede-cbc-sha	No	RSA certificate	RSA key exchange
dhe-dss-with-des-cbc-sha	No	DSA (DSS) certificate	Ephemeral Diffie-Hellman
dhe-dss-with-3des-ede-cbc-sha	No	DSA (DSS) certificate	Ephemeral Diffie-Hellman
dhe-rsa-with-des-cbc-sha	No	RSA certificate	Ephemeral Diffie-Hellman key exchange
dhe-rsa-with-3des-ede-cbc-sha	No	RSA certificate	Ephemeral Diffie-Hellman key exchange
dh-anon-with-rc4-128-md5	No	Neither party is authenticated	Diffie-Hellman

Table 2-5 SSL Cipher Suites Supported by the CSS (continued)

Cipher Suite	Exportable	Authentication Certificate Used	Key Exchange Algorithm Used
dh-anon-with-des-cbc-sha	No	Neither party is authenticated	Diffie-Hellman
dh-anon-with-3des-ede-cbc-sha	No	Neither party is authenticated	Diffie-Hellman
dhe-dss-with-rc4-128-sha	No	DSA (DSS) certificate	Ephemeral Diffie-Hellman
rsa-export-with-rc4-40-md5	Yes	RSA certificate	RSA key exchange
rsa-export-with-des40-cbc-sha	Yes	RSA certificate	RSA key exchange
dhe-dss-export-with-des40-cbc-sha	Yes	DSA (DSS) certificate	Ephemeral Diffie-Hellman key exchange
dhe-rsa-export-with-des40-cbc-sha	Yes	RSA certificate	Ephemeral Diffie-Hellman
dh-anon-export-with-rc4-40-md5	Yes	Neither party is authenticated	Diffie-Hellman
dh-anon-export-with-des40-cbc-sha	Yes	Neither party is authenticated	Diffie-Hellman
rsa-export1024-with-des-cbc-sha	Yes	RSA certificate	RSA key exchange
dhe-dss-export1024-with-des-cbc-sha	Yes	DSA (DSS) certificate	Ephemeral Diffie-Hellman
rsa-export1024-with-rc4-56-sha	Yes	RSA certificate	RSA key exchange
dhe-dss-export1024-with-rc4-56-sha	Yes	DSA (DSS) certificate	Ephemeral Diffie-Hellman

Related Commands

show ssl-proxy-list

backend-server *number* dhparam

To configure the back-end server Diffie-Hellman (DH) parameter file, use the **backend-server** *number* **dhparam** *name* command. Use the **no** form of this command to remove the configured DH parameter file from the SSL proxy list.

backend-server *number* **dhparam** *name*

no backend-server *number* **dhparam**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
dhparam	Specifies a Diffie-Hellman parameter file.
name	Name of the DH parameter file. Enter an unquoted text string from 1 to 31 characters.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

The DH parameters file must already be loaded on the SCM. If the parameter file does not exist, the CSS logs an error message.

Related Commands

show ssl-proxy-list
(ssl-proxy-list) active

backend-server *number* dsacert

To configure the back-end server DSA certificate, use the **backend-server** *number* **dsacert** *name* command. Use the **no** form of this command to remove the configured DSA certificate from the SSL proxy list.

backend-server *number* **dsacert** *name*

no backend-server *number* **dsacert**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
dsacert	Specifies a DSA certificate.
name	Name of the DSA certificate. Enter an unquoted text string from 1 to 31 characters.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

The certificate must already be loaded on the SCM. If the certificate name does not exist, the CSS logs an error message.

Related Commands

show ssl-proxy-list
(ssl-proxy-list) active

backend-server *number* dsakey

To configure the back-end server DSA key pair name, use the **backend-server** *number* **dsakey** *name* command. Use the **no** form of this command to remove the configured DSA key pair from the SSL proxy list.

backend-server *number* **dsakey** *name*

no backend-server *number* **dsakey**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
dsakey	Specifies a DSA key pair.
name	Name of the DSA key pair. Enter an unquoted text string from 1 to 31 characters.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

The key pair must already be loaded on the SCM. If the key pair name does not exist, the CSS logs an error message.

Related Commands

show ssl-proxy-list
(ssl-proxy-list) active

backend-server *number* handshake

To configure SSL session handshake renegotiation to reestablish an SSL session between the SSL module and the back-end SSL server, use the **backend-server** *number* **handshake** command. This command sends the SSL HelloRequest message to a client to restart SSL handshake negotiation. Reestablishing the SSL handshake is useful in instances when a connection has been established for a lengthy period of time and you want to ensure security by reestablishing the SSL session. Use the **no** form of this command to disable handshake data exchange or timeout.

backend-server *number* **handshake** [**data** *kbytes*|**timeout** *seconds*]

no backend-server *number* **handshake data**|**timeout**

Syntax Description

number	Index number for the back-end SSL server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
data *kbytes*	Sets the maximum amount of data to be exchanged between the CSS and the back-end SSL server, after which the CSS transmits the SSL handshake message and reestablishes the SSL session. The *kbytes* variable is the SSL handshake data value in Kbytes. Enter a value from 0 to 512000. The default is 0, disabling the handshake data exchange.
timeout *seconds*	Sets a maximum timeout value, after which the CSS transmits the SSL handshake message and reestablishes the SSL session. The *seconds* variable is the SSL handshake timeout value in seconds. Enter a value from 0 to 72000 (20 hours). The default is 0, disabling the handshake timeout.

Command Modes

ssl-proxy-list configuration mode

Related Commands

show ssl-proxy-list

backend-server *number* ip address

To specify an IP address for the back-end SSL server, use the **backend-server** *number* **ip address** command. The IP address corresponds to the address of the service. Use the **no** form of this command to remove the address from the server.

backend-server *number* **ip address** *ip_or_host*

no backend-server *number* **ip address**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
ip address *ip_or_host*	IP address that corresponds to the address of the service. Enter a valid VIP address in either dotted-decimal IP notation (for example, 192.168.11.1) or mnemonic host-name format (for example, myhost.mydomain.com).

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

When you use the mnemonic host-name format for the address, the CSS includes a Domain Name System (DNS) facility that translates host names to IP addresses. If the host name cannot be resolved, the IP address setting is not accepted and an error message appears indicating host resolution failure. For details about configuring a Domain Name System, refer to the *Cisco Content Services Switch Administration Guide.*

If the IP address has not been defined when you activate the SSL proxy list through the **active** command, the CSS logs the following error message and does not activate the SSL proxy list.

```
SSL-server/Backend-server must have valid IP Address
```

Related Commands

show ssl-proxy-list
(ssl-proxy-list) active

backend-server *number* port

To specify a virtual TCP port number for the back-end SSL server, use the **backend-server** *number* **port** command. Use the **no** form of this command to remove a virtual port from an SSL server.

backend-server *number* **port** *number2*

no backend-server *number* **port** *number2*

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
port *number2*	TCP port number that matches the TCP port number for an SSL content rule. The SSL module uses the port to determine which traffic it should accept. Enter a port number from 1 to 65535. The default port is 80.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

If you configure the **backend-server** *number* **ip address** and **server-ip** commands with the same address, configure the **backend-server** *number* **port** and **server-port** commands with different port numbers.

Related Commands

show ssl-proxy-list
(config-owner-content) port

backend-server *number* rsacert

To configure the back-end server RSA certificate, use the **backend-server** *number* **rsacert** *name* command. Use the **no** form of this command to remove the configured RSA certificate from the SSL proxy list.

backend-server *number* **rsacert** *name*

no backend-server *number* **rsacert**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
rsacert	Specifies an RSA certificate.
name	Name of the RSA certificate. Enter an unquoted text string from 1 to 31 characters.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

The certificate must already be loaded on the SCM. If the certificate name does not exist, the CSS logs an error message.

Related Commands

show ssl-proxy-list
(ssl-proxy-list) active

backend-server *number* rsakey

To configure the back-end server RSA key pair name, use the **backend-server** *number* **rsakey** *name* command. Use the **no** form of this command to remove the configured RSA key pair from the SSL proxy list.

backend-server *number* **rsakey** *name*

no backend-server *number* **rsakey**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
rsakey	Specifies an RSA key pair.
name	Name of the RSA key pair. Enter an unquoted text string from 1 to 31 characters.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

The key pair must already be loaded on the SCM. If the key pair name does not exist, the CSS logs an error message.

Related Commands

show ssl-proxy-list
(ssl-proxy-list) active

backend-server *number* server-ip

To specify an IP address for the back-end SSL server, use the **backend-server** *number* **server-ip** command. Use the **no** form of this command to remove the address from the server.

backend-server *number* **server-ip** *ip_or_host*

no backend-server *number* **server-ip**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
server-ip *ip_or_host*	IP address for the server. Enter a valid IP address in either dotted-decimal IP notation (for example, 192.168.11.1) or mnemonic host-name format (for example, myhost.mydomain.com).

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

When you use the mneumonic host-name format for the VIP, the CSS includes a Domain Name Service (DNS) facility that translates host names such as myhost.mydomain.com to IP addresses such as 192.168.11.1. If the host name cannot be resolved, the VIP address setting is not accepted and an error message appears indicating host resolution failure. For details about configuring a Domain Name Service, refer to the *Cisco Content Services Switch Administration Guide.*

If the IP address has not been defined when you activate the SSL proxy list through the **active** command, the CSS logs the following error message and does not activate the SSL proxy list.

```
SSL-server/Backend-server must have valid IP Address
```

Related Commands

show ssl-proxy-list
(ssl-proxy-list) active
(config-owner-content) vip address

backend-server *number* server-port

To specify a port number for the back-end SSL server, use the **backend-server** *number* **server-port** command. Use the **no** form of this command to remove a virtual port from an SSL server.

backend-server *number* **server-port** *number2*

no backend-server *number* **server-port** *number2*

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
server-port *number2*	The port number for the back-end SSL server. Enter a port number from 1 to 65535. The default port is 443.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

If you configure the **backend-server** *number* **ip address** and **server-ip** commands with the same address, configure the **backend-server** *number* **port** and **server-port** commands with different port numbers.

Related Commands

show ssl-proxy-list
(config-owner-content) port

backend-server *number* session-cache

To set the SSL cache timeout value, use the **backend-server** *number* **session-cache** command. In SSL, a new session ID is created every time the SSL module and back-end SSL server go through a full key exchange and establish a new master secret key. Specifying an SSL session cache timeout allows the reuse of the master key on subsequent connections between the client and the CSS SSL module, which can speed up the SSL negotiation process. Use the **no** form of this command to reset the SSL session reuse timeout back to 300 seconds.

backend-server *number* **session-cache** *seconds*

no backend-server *number* **session-cache**

Syntax Description

number	Index number for the back-end SSL server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
seconds	SSL session cache timeout in seconds. Enter a value from 0 to 72000 (20 hours). The default is 300 seconds (5 minutes). To disable the timeout, set the value to 0. The full SSL handshake occurs for each new connection between the client and the SSL module.

Command Modes

ssl-proxy-list configuration mode

Related Commands

show ssl-proxy-list

backend-server *number* tcp

To configure TCP connections with a back-end server, use the **backend-server** *number* **tcp** command. You can specify:

- A timeout value that the CSS uses to terminate a TCP connection for inactivity or for an unsuccessful TCP three-way handshake with a back-end SSL server
- The Nagle algorithm for the TCP connection

Use the **no** form of this command to reset the buffer size to 32768, restore the timeout period to 240 seconds for inactivity or 30 seconds for the three-way handshake.

backend-server *number* **tcp** [**buffer-share** [**rx**|**tx**] *number2*|[**server**|**virtual**] **inactivity-timeout** *seconds*|**nagle** [**enable**|**disable**]|**syn-timeout** *seconds2*]

no backend-server *number* **tcp** [**buffer-share** [**rx**|**tx**]| [**server**|**virtual**] **inactivity-timeout** |**syn-timeout**]

Syntax Description

number	Index number for the back-end SSL server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
buffer-share [**rx**|**tx**] *number2*	Sets the TCP buffering from the client or server on a given connection. • To set the amount of data in bytes that a given connection can buffer from the client traffic, use the **rx** *number2* keyword and variable. • To set the amount of data in bytes that a given connection can buffer from the server to the client, use the **tx** *number2* keyword and variable. By default, the buffer size is 32768. The buffer size can range from 16400 to 262144.
server	Specifies the TCP connection for the back-end SSL server.

virtual	Specifies the TCP connection for the client.
inactivity-timeout *seconds*	Specifies the timeout value that the CSS waits to receive inbound flows before terminating the TCP connection. Enter a TCP inactivity timeout value in seconds, from 0 (disabling the TCP inactivity timeout) to 3600 (1 hour). The default is 240 seconds.
nagle enable|disable	Specifies the Nagle algorithm for the TCP connection. By default, the Nagle algorithm is enabled for each TCP connection. Use the **disable** keyword to disable the Nagle algorithm when you observe an unacceptable delay in the TCP connection. Use the **enable** keyword to reenable the Nagle algorithm.
syn-timeout *seconds2*	Specifies a timeout value that the CSS uses to terminate a TCP connection with client or a server that has not successfully completed the TCP three-way handshake prior to transferring data. Enter a TCP SYN timeout value in seconds, from 0 to 3600 (1 hour). The default is 30 seconds. To disable the TCP SYN timeout period, set the value to 0. The timer becomes inactive and the retransmit timer eventually terminates a broken TCP connection. The connection timer should always be shorter than the retransmit termination time for new SSL/TCP connections.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

The TCP Nagle algorithm automatically concatenates a number of small buffer messages transmitted over the TCP connection between a client and the SSL module or between a back-end server and the SSL module. This process increases the throughput of your CSS by decreasing the number of packets sent over each TCP connection. However, the interaction between the Nagle algorithm and the TCP delay acknowledgment may increase latency in your TCP connection. Disable the Nagle algorithm when you observe an unacceptable delay in a TCP connection (clear-text or SSL).

Related Commands

show ssl-proxy-list

backend-server *number* type

To configure a back-end SSL server as an SSL initiation server or to reconfigure an SSL initiation server as a back-end SSL server (the default), use the **backend-server** *number* **type** command. An SSL initiation server allows a CSS to accept clear text from a client and to initiate an SSL session with an SSL server. Use the **no** form of this command to reset the back-end server type to the default of **backend-ssl**.

backend-server *number* **type** [**backend-ssl|initiation**]

no backend-server *number* **type**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
type	Keyword that specifies the type of back-end server on the CSS.
backend-ssl	(Default) Specifies a back-end SSL server that allows a CSS to: • Receive encrypted data from a client • Decrypt the data for load balancing • Re-encrypt the data and send it to an SSL server over an SSL connection **Note** Use back-end SSL with SSL termination. For information about SSL termination, refer to the *Cisco Content Services Switch SSL Configuration Guide*.
initiation	Specifies an SSL initiation server that allows a CSS to: • Receive clear text from a client • Encrypt the data and send it to an SSL server over an SSL connection

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

By default, a back-end server is a server of type **backend-ssl** for use with services of type **ssl-accel-backend**. To use the back-end server for SSL initiation, you must configure it as an initiation server for use with services of type **ssl-accel**. If you have configured an SSL initiation server and want to reconfigure it as a back-end SSL server, enter the **backend-server** *number* **type backend-ssl** command.

Related Commands

show ssl-proxy-list
(ssl-proxy-list) active

backend-server *number* version

To specify the SSL or Transport Layer Security (TLS) protocol version, use the **backend-server** *number* **version** command. Use the **no** form of the command to reset the default SSL version setting to SSL version 3.0 and TLS version 1.0. The SSL module sends a ClientHello that has an SSL version 3 header with the ClientHello message set to TLS version 1.0.

backend-server *number* **version** *protocol*

no backend-server *number* **version**

Syntax Description

number	Index number for the back-end SSL server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# backend-server ?`
protocol	Protocol version. Enter one of the following keywords: • **ssl-tls -** SSL protocol version 3.0 and TLS protocol version 1.0 (default). • **ssl -** SSL protocol version 3.0 • **tls** - TLS protocol version 1.0

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

The CSS supports SSL version 3.0 and TLS version 1.0. The CSS understands and accepts an SSL version 2.0 ClientHello message to allow dual version clients to communicate with the CSS through the SSL module. In this case, the client indicates an SSL version of 3.0 in the version 2.0 ClientHello. This indicates to the SSL module that the client can support SSL version 3.0, and the SSL module returns a version 3.0 ServerHello message.

If the client only supports SSL version 2.0 (SSL version 2.0 compliant), the CSS cannot to pass network traffic.

Related Commands

show ssl-proxy-list

(ssl-proxy-list) description

To provide a description for the SSL proxy list, use the **description** command.

description "*text***"**

Syntax Description

"*text*"	Description for the SSL proxy list. Enter a quoted text string with a maximum length of 64 characters including spaces.

(ssl-proxy-list) no

To negate a command or set it to its default, use the **no** command. For information on general **no** commands you can use in this mode, see the general **no** command. The following options are available in this mode.

Syntax Description

no acl *index*	Deletes an ACL.
no backend-server *number*	Removes the back-end SSL server from the SSL proxy list.

no backend-server *number* **cacert**	Removes the CA certificate from the SSL proxy list.
no backend-server *number* **cipher**	Removes the cipher suite from the back-end SSL server.
no backend-server *number* **dhparam**	Removes the DH parameter file from the SSL proxy list.
no backend-server *number* **dsacert**	Removes the DSA certificate from the SSL proxy list.
no backend-server *number* **dsakey**	Removes the DSA key pair name from the SSL proxy list.
no backend-server *number* **handshake data**	Disables the handshake data exchange.
no backend-server *number* **handshake timeout**	Disables the handshake timeout period.
no backend-server *number* **ip address**	Removes the IP address from the back-end SSL server. The IP address corresponds to address of the service.
no backend-server *number* **port**	Resets the port number to 80.
no backend-server *number* **rsacert**	Removes the RSA certificate from the SSL proxy list.
no backend-server *number* **rsakey**	Removes the RSA key pair name from the SSL proxy list.
no backend-server *number* **server-ip**	Removes the IP address from the back-end SSL server.
no backend-server *number* **server-port**	Resets the port number to 443.
no backend-server *number* **session-cache**	Resets the SSL session reuse timeout to 300 seconds.
no backend-server *number* **tcp server inactivity-timeout**	Resets the TCP inactivity timer to 240 seconds between the back-end SSL server and the CSS.
no backend-server *number* **tcp server syn-timeout**	Resets the TCP SYN timeout to 30 seconds between the back-end SSL server and the CSS.

no backend-server *number* **tcp virtual inactivity-timeout**	Resets the TCP inactivity timer to 240 seconds between the server and the CSS.
no backend-server *number* **tcp virtual syn-timeout**	Resets the TCP SYN timeout to 30 seconds between the server and the CSS.
no backend-server *number* **version**	Resets the SSL version to the default of SSL version 3.0 and TLS version 1.0.
no description	Removes the description for an SSL proxy list.
no ssl-server *number*	Removes the virtual SSL server from the SSL proxy list.
no ssl-server *number* *association_type*	Removes the association from the virtual SSL server. The association type is **dhparam**, **dsacert**, **dsakey**, **rsacert**, or **rsakey**.
no ssl-server *number* **cacert** *name*	Removes a CA certificate association from the virtual SSL server.
no ssl-server *number* **cipher**	Removes the cipher suite from the virtual SSL server.
no ssl-server *number* **crl** *crl_record_name*	Removes the CRL from the virtual SSL server.
no ssl-server *number* **failure-url**	Removes the redirect URL used by the **ssl-server** *number* **failure redirect** command.
no ssl-server *number* **handshake data**	Disables the handshake data exchange.
no ssl-server *number* **handshake timeout**	Disables the handshake timeout period.
no ssl-server *number* **http-header client-cert**	Disables the insertion of client certificate fields and information in the HTTP request header.
no ssl-server *number* **http-header prefix**	Deletes the configured prefix for client certificate fields, server certificate fields, or session fields inserted in the HTTP request header.
no ssl-server *number* **http-header server-cert**	Disables the insertion of server certificate fields and information in the HTTP request header.
no ssl-server *number* **http-header session**	Disables the insertion of SSL session fields and information in the HTTP request header.

no ssl-server *number* **http-header static**	Disables the insertion of the static string in the HTTP request header and deletes the string.
no ssl-server *number* **port**	Resets the port number to 443.
no ssl-server *number* **session-cache**	Resets the SSL session reuse timeout to 300 seconds.
no ssl-server *number* **tcp server inactivity-timeout**	Resets the TCP inactivity timer to 240 seconds between the web server and the CSS.
no ssl-server *number* **tcp server syn-timeout**	Resets the TCP SYN timeout to 30 seconds between the web server and the CSS.
no ssl-server *number* **tcp virtual inactivity-timeout**	Resets the TCP inactivity timer to 240 seconds between the client and the CSS.
no ssl-server *number* **tcp virtual syn-timeout**	Resets the TCP SYN timeout to 30 seconds between the client and the CSS.
no ssl-server *number* **unclean-shutdown**	Resets the CSS default behavior of sending both a Close-Notify alert and a TCP FIN message to close the client connection.
no ssl-server *number* **urlrewrite**	Removes a URL rewrite rule from the virtual SSL server.
no ssl-server *number* **version**	Resets the SSL version to the default of SSL version 3.0 and TLS version 1.0.
no ssl-server *number* **vip address**	Removes the VIP address from the virtual SSL server.

(ssl-proxy-list) show ssl-proxy-list

To display information about the current SSL proxy configuration list, use the **show ssl-proxy-list** command. You can display detailed information about the list, or a virtual or back-end server in the list.

show ssl-proxy-list {**ssl-server**|**backend-server** {*number*}}

Syntax Description

ssl-server	(Optional) Displays information for all virtual SSL servers in the list.
backend-server	(Optional) Displays information for the back-end SSL servers in the list.
number	(Optional) Displays information for a specific virtual or back-end SSL server.

Usage Guidelines

For information on using the **show ssl-proxy-list** command to display information about other SSL proxy lists, see the **show ssl-proxy-list** command in the "General Commands" section.

The **show ssl-proxy-list** command without an option displays detailed configuration information about the current SSL proxy list.

For information about the fields in the **show ssl-proxy-list** command output, refer to the *Cisco Content Services Switch Security Configuration Guide*.

Related Commands

(config) ssl-proxy-list
(ssl-proxy-list) description
(ssl-proxy-list) ssl-server

(ssl-proxy-list) ssl-server

To create a virtual SSL server and configure it for an SSL proxy list, use the **ssl-server** command. Use the **no** form of the **ssl-server** command to delete the SSL server. For information on the other **no** forms of this command, see the commands in the following section.

ssl-server *number* {*association_type*...|**authentication**|**cacert**...
|**cipher**...|**crl**...|**failure**...|**failure-url**...|**handshake**...|**http-header**...
|**port**...|**session-cache**...|**ssl-queue-delay**...|**tcp**...|**unclean-shutdown**
|**urlrewrite**...|**version**...|**vip address**...}

```
no ssl-server number{association_type...|authentication|cacert...
    |cipher...|crl...|failure-url|handshake....|http-header...|port...
    |session-cache...|ssl-queue-delay|tcp...|unclean-shutdown
    |urlrewrite...|version...|vip address...}
```

Syntax Description

number	The index number for the virtual SSL server. This variable without an option creates a server. When you enter this variable with an option, the number identifies the server for configuration. An SSL proxy list can have a maximum of 256 virtual servers. Enter a number from 1 to 256.
association_type...	(Optional) Creates a key pair, certificate, or key parameter association for the server. See the **ssl-server number association_type** command.
authentication	(Optional) Specifies whether to enable or disable client authentication. See the **ssl-server number authentication** command.
cacert	(Optional) Assigns the certificate association to the virtual SSL server. See the **ssl-server number cacert** command.
cipher...	(Optional) Specifies the cipher suite for the server. See the **ssl-server number cipher** command.
crl...	(Optional) Assigns the CRL record to the server. See the **ssl-server number crl** command.
failure...	(Optional) Specifies how the CSS handles a client authentication failure. See the **ssl-server number failure** command.
failure-url...	(Optional) Specifies the URL to redirect a client connection when a failure occurs and the CSS is configured to redirect the connection. See the **ssl-server number failure-url** command.
handshake...	(Optional) Specifies the handshake negotiation data and timeout value for the server. See the **ssl-server number handshake** command.

http-header...	(Optional) Specifies the information to insert in the HTTP request header to a back-end server. See the **ssl-server number http-header** command.
port...	(Optional) Specifies a virtual TCP port for the server. See the **ssl-server number port** command.
session-cache...	(Optional) Specifies the session cache timeout value for the server. See the **ssl-server number session-cache** command.
ssl-queue-delay...	(Optional) Specifies the time to wait before sending queued data for encryption. See the **ssl-server number ssl-queue-delay** command.
tcp...	(Optional) Specifies a timeout value to terminate a TCP connection, the Nagle algorithm for a TCP connection, or buffer size for the TCP connection. See the **ssl-server number tcp** command.
unclean-shutdown	(Optional) Instruct the CSS to send only a TCP FIN message to terminate a client connection (the CSS does not send a Close Notify alert). See the **ssl-server number unclean-shutdown** command.
urlrewrite...	(Optional) Adds a URL rewrite rule to the virtual SSL server to avoid nonsecure HTTP 300-series redirects by the server. See the **ssl-server number urlrewite** command.
version...	(Optional) Specifies the SSL or Transport Layer Security (TLS) protocol version. See the **ssl-server number version** command.
vip address...	(Optional) Specifies a VIP address for the server. See the **ssl-server number vip address** command.

Usage Guidelines

You must create a virtual SSL server before you can configure its parameters.

You cannot modify a server in an active SSL proxy list. You must first suspend the SSL proxy list to make modifications to any server in the list. Once you have modified the SSL proxy list, suspend the SSL service, activate the SSL proxy list, and then activate the SSL service.

ssl-server *number association_type*

To specify the certificate, key pair, or Diffie-Hellman key exchange parameter file association for the virtual SSL server, use the **ssl-server** *number association_type* command. Use the **no** form of this command to remove the association.

ssl-server *number association_type name*

no ssl-server *number association_type*

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, use the **ssl-server ?** command.
association_type	Identifies the association type. Enter one of the following options: • **dhparam** - A Diffie-Hellman key exchange parameter file association. The Diffie-Hellman key exchange parameter file ensures that the two sides in a data exchange cooperate to generate a symmetric (shared) key for packet encryption and authentication. • **dsacert** - A DSA certificate association to be used in the exchange of digital signatures. • **dsakey** - A DSA key pair association. DSA key pairs are used to sign packet data, and they are a requirement before another device (client or web server) can exchange an SSL certificate with the CSS. • **rsacert** - An RSA certificate association to be used in the exchange of a public and private key pair for authentication and packet encryption. • **rsakey** - An RSA key pair association. RSA key pairs are a requirement before another device (client or web server) can exchange an SSL certificate with the CSS.
name	The name of the association. To see a list of existing associations, use the **ssl-server** *number association_type* **?** command.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

The certificate, key pair, or Diffie-Hellman parameter file must already be loaded on the CSS and an association made. If there is not a proper association upon activation of the SSL proxy list, the CSS logs an error message and does not activate the list.

Related Commands

copy ssl
show ssl-proxy-list
(config) ssl associate

ssl-server *number* authentication

To enable or disable client authentication on a virtual SSL server, use the **ssl-server** *number* **authentication** command. By default, client authentication is disabled. Use the **no** form of this command or the **disable** keyword to disable client authentication on the virtual SSL server.

ssl-server *number* **authentication** [**enable**|**disable**]

no ssl-server *number* **authentication**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, use the **ssl-server ?** command.
enable	Enables client authentication on the virtual SSL server.
disable	Disables client authentication on the virtual SSL server (default).

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

After you enable client authentication on the CSS, you must specify a CA certificate that the CSS uses to verify client certificates.

Related Commands

show ssl statistics
show ssl-proxy-list ssl-server
(config) ssl associate
(config-ssl-proxy-list) ssl-server number cacert

ssl-server *number* cacert

To assign a Certificate Authority (CA) certificate association to a virtual SSL server, use the **ssl-server** *number* **cacert** command. Use the **no** form of this command to remove a CA certificate association from the virtual SSL server.

ssl-server *number* **cacert** *association_name*

no ssl-server *number* **cacert** *association_name*

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, use the **ssl-server ?** command.
association_name	Name of the CA certificate association. To see a list of existing associations, use the **ssl-server** *number* **cacert ?** command.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

If you configure a virtual SSL server for client authentication, you must configure the server with a CA certificate. The CSS uses the public key in the certificate to verify the digital signature in the client certificate.

Before you configure the CA certificate on a virtual SSL server, you must import the CA certificate on the CSS and then associate it to a filename.

You must configure at least one certificate; however, you can configure a maximum of four. If you try to configure more than four certificates, the CSS displays an error message.

You must configure a CA certificate before you activate the SSL proxy list.

Related Commands

copy ssl
show ssl-proxy-list ssl-server
(config) ssl associate
(config-ssl-proxy-list) ssl-server number authentication

ssl-server *number* cipher

To assign a cipher suite to the virtual SSL server, use the **ssl-server** *number* **cipher** command. For each available SSL version, there is a distinct list of supported cipher suites representing a selection of cryptographic algorithms and parameters. Your choice depends on your environment, certificates and keys in use, and security requirements. By default, no supported cipher suites are enabled. Use the **no** form of this command to remove a cipher suite from the server.

ssl-server *number* **cipher** *name ip_or_host port* {**weight** *number*}

no ssl-server *number* **cipher**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
name	The name of a specific cipher suite. See the "Usage Guidelines" section for detailed information.
ip_or_host	IP address to assign to the back-end content rule/server used with the cipher suite. Specify the IP address in either dotted-decimal IP notation (for example, 192.168.11.1) or mnemonic host-name format (for example, myhost.mydomain.com).

port	TCP port of the back-end content rule/server through which the back-end HTTP connections are sent.
weight *number*	(Optional) Assigns a priority to the cipher suite, with 10 being the highest weight. When negotiating which cipher suite to use, the SSL module selects from the client list based on the cipher suite configured with the highest weight. To set the weight for a cipher suite, enter a number from 1 to 10. By default, all configured cipher suites have a weight of 1.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

Table 2-6 lists all supported cipher suites and values for the specific SSL server (and corresponding SSL proxy list). The table also lists whether those cipher suites are exportable from the CSS, along with the authentication certificate and encryption key required by the cipher suite.

If you use the default setting or select the **all-cipher-suite** option, the CSS sends the suites in the same order as they appear in Table 2-6, starting with rsa-with-rc4-128-md5.

Note The **all-cipher-suites** setting works only when no specifically-defined ciphers are configured. To return to using the **all-cipher-suites** setting, you must remove all specifically-defined ciphers.

Caution The dh-anon series of cipher suites are intended for completely anonymous Diffie-Hellman communications in which neither party is authenticated. Note that this cipher suite is vulnerable to man-in-the-middle attacks and is strongly discouraged.

Table 2-6 SSL Cipher Suites Supported by the CSS

Cipher Suite	Exportable	Authentication Certificate Used	Key Exchange Algorithm Used
all-cipher-suites	No	RSA certificate, DSA certificate	RSA key exchange, Diffie-Hellman
rsa-with-rc4-128-md5	No	RSA certificate	RSA key exchange
rsa-with-rc4-128-sha	No	RSA certificate	RSA key exchange
rsa-with-des-cbc-sha	No	RSA certificate	RSA key exchange
rsa-with-3des-ede-cbc-sha	No	RSA certificate	RSA key exchange
dhe-dss-with-des-cbc-sha	No	DSA (DSS) certificate	Ephemeral Diffie-Hellman
dhe-dss-with-3des-ede-cbc-sha	No	DSA (DSS) certificate	Ephemeral Diffie-Hellman
dhe-rsa-with-des-cbc-sha	No	RSA certificate	Ephemeral Diffie-Hellman key exchange
dhe-rsa-with-3des-ede-cbc-sha	No	RSA certificate	Ephemeral Diffie-Hellman key exchange
dh-anon-with-rc4-128-md5	No	Neither party is authenticated	Diffie-Hellman
dh-anon-with-des-cbc-sha	No	Neither party is authenticated	Diffie-Hellman
dh-anon-with-3des-ede-cbc-sha	No	Neither party is authenticated	Diffie-Hellman
dhe-dss-with-rc4-128-sha	No	DSA (DSS) certificate	Ephemeral Diffie-Hellman
rsa-export-with-rc4-40-md5	Yes	RSA certificate	RSA key exchange
rsa-export-with-des40-cbc-sha	Yes	RSA certificate	RSA key exchange

Table 2-6 SSL Cipher Suites Supported by the CSS (continued)

Cipher Suite	Exportable	Authentication Certificate Used	Key Exchange Algorithm Used
dhe-dss-export-with-des40-cbc-sha	Yes	DSA (DSS) certificate	Ephemeral Diffie-Hellman key exchange
dhe-rsa-export-with-des40-cbc-sha	Yes	RSA certificate	Ephemeral Diffie-Hellman
dh-anon-export-with-rc4-40-md5	Yes	Neither party is authenticated	Diffie-Hellman
dh-anon-export-with-des40-cbc-sha	Yes	Neither party is authenticated	Diffie-Hellman
rsa-export1024-with-des-cbc-sha	Yes	RSA certificate	RSA key exchange
dhe-dss-export1024-with-des-cbc-sha	Yes	DSA (DSS) certificate	Ephemeral Diffie-Hellman
rsa-export1024-with-rc4-56-sha	Yes	RSA certificate	RSA key exchange
dhe-dss-export1024-with-rc4-56-sha	Yes	DSA (DSS) certificate	Ephemeral Diffie-Hellman

Related Commands

show ssl-proxy-list

ssl-server *number* crl

To assign a certificate revocation list (CRL) record to a virtual SSL server, use the **ssl-server** *number* **crl** command. Use the **no** form of this command to remove the CRL from the virtual SSL server.

ssl-server *number* **crl** *crl_record_name*

no ssl-server *number* **crl** *crl_record_name*

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, use the **ssl-server ?** command.
crl_record_name	Name of the configured CRL record. To see a list of existing associations, use the **ssl-server** *number* **crl ?** command.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

Before you configure the CRL record on a virtual SSL server, you must configure the CRL record by using the global configuration **ssl crl-record** command.

You can configure only one CRL record for each SSL server.

Related Commands

show ssl crl-record
(config) ssl crl-record

ssl-server *number* failure

To configure how the CSS handles client authentication failures, use the **ssl-server** *number* **failure** command. A client certificate can fail if it is invalid, expired, or revoked by a CA. By default, the CSS rejects the client connection when client authentication fails.

ssl-server *number* **failure** [**ignore**|**redirect**|**reject**]

Syntax Description

number	Index number for the virtual SSL server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
ignore	Ignores client authentication failures and allows both invalid and valid certificates to connect.
redirect	Sends client connections of a failed authentication to a configured URL. To configure the URL where the CSS redirects the client connection, use the **ssl-server number failure-url** command.
reject	Resets the CSS default behavior of rejecting the client connection when client authentication fails.

Command Modes

ssl-proxy-list configuration mode

Related Commands

show ssl-proxy-list ssl-server

ssl-server *number* failure-url

To configure the URL where the CSS redirects the client connection when authentication fails, use the **ssl-server** *number* **failure-url** command. Use this command when you configure the CSS to redirect connections through the **ssl-server** *number* **failure redirect** command. Use the **no** form of this command to remove the URL.

ssl-server *number* **failure-url** *url*

no ssl-server *number* **failure-url**

Syntax Description

number	Index number for the virtual SSL server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
url	URL to redirect the client connection when authentication fails. Enter a URL with a maximum of 168 characters and no spaces.

Usage Guidelines

To change an existing redirect URL, you must first remove the existing URL by using the **no ssl-server** *number* **failure-url** command. Then you can reissue the **ssl-server** *number* **failure-url** command to configure the new URL.

You must suspend an activated virtual SSL server before modifying it.

Command Modes

ssl-proxy-list configuration mode

Related Commands

show ssl-proxy-list ssl-server
ssl-server number failure redirect

ssl-server *number* handshake

To configure SSL session handshake renegotiation to reestablish an SSL session between the SSL module and a client, use the **ssl-server** *number* **handshake** command. This command send the SSL HelloRequest message to a client to restart SSL handshake negotiation. Reestablishing the SSL handshake is useful in instances when a connection has been established for a lengthy period of time and you want to ensure security by reestablishing the SSL session. Use the **no** form of this command to disable handshake data exchange or timeout.

ssl-server *number* **handshake** [**data** *kbytes*|**timeout** *seconds*]

no ssl-server *number* **handshake data**|**timeout**

Syntax Description

number	Index number for the virtual SSL server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
data *kbytes*	Sets the maximum amount of data to be exchanged between the CSS and the client, after which the CSS transmits the SSL handshake message and reestablishes the SSL session. The *kbytes* variable is the SSL handshake data value in Kbytes. Enter a value from 0 to 512000. The default is 0, disabling the handshake data exchange.
timeout *seconds*	Sets a maximum timeout value, after which the CSS transmits the SSL handshake message and reestablishes the SSL session. The *seconds* variable is the SSL handshake timeout value in seconds. Enter a value from 0 to 72000 (20 hours). The default is 0, disabling the handshake timeout.

Command Modes

ssl-proxy-list configuration mode

Related Commands **show ssl-proxy-list**

ssl-server *number* http-header

To insert client certificate, server certificate, SSL session, or static text information in the HTTP request header during a client connection, use the **ssl-server** *number* **http-header** command. You can also insert a prefix in SSL fields when you configure the insertion of client certificate, server certificate, or session information. Use the **no** form of this command to disable the insertion of information into the HTTP request header.

ssl-server *number* **http-header** [**client-cert**|**server-cert**|**session** |**prefix** "*text_string*"|**static** "*text_string*"]

no ssl-server *number* **http-header** [**client-cert**|**server-cert**|**session**|**prefix**|**static**]

Syntax Description

number	Index number for the virtual SSL server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
client-cert	Inserts SSL client certificate fields and associated information in the HTTP request header to the back-end server. For a list of inserted fields, refer to the *Cisco Content Services Switch SSL Configuration Guide*.
server-cert	Inserts SSL server certificate fields and associated information in the HTTP request header to the back-end server. For a list of inserted fields, refer to the *Cisco Content Services Switch SSL Configuration Guide*.
session	Inserts SSL session fields and associated information in the HTTP request header to the back-end server. For a list of inserted fields, refer to the *Cisco Content Services Switch SSL Configuration Guide*.

prefix "*text_string*"	Changes the prefix on each HTTP inserted field when you configure the insertion of client certificate, server certificate, or SSL session information. By default, no prefix is added to each HTTP inserted field. Enter a quoted text string with a maximum of 16 characters.
static "*text_string*"	Inserts a static text string in the HTTP request header to the back-end server. Enter a quoted text string with a maximum of 199 characters including spaces. For Microsoft Outlook Web Access (OWA) application support, enter the text string "FRONT-END-HTTPS: on". You can also insert multiple strings on different lines by using the \r\n characters in between each line. Note that these characters use 4 out of the 199 characters

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

During an SSL session, a client may need to pass specific information to a back-end server. HTTP request header insertion allows the embedding of information into an HTTP request header during a client connection. For example, when a client connects to the HTTP request head virtual SSL server and the CSS decrypts the data, the CSS can insert information about the SSL session and the client and server certificates into the HTTP request header, and then the CSS passes the header to the back-end server.

Note HTTP header insertion only occurs on the first HTTP request for a persistent HTTP 1.1 connection. Subsequent requests within the same TCP connection are sent unmodified. For HTTP 1.0, in which persistence is not implemented, all HTTP requests contain the inserted header.

The CSS can insert one or more of the following into the HTTP request header after it decrypts the client data:

- Client certificate fields and associated information

- Server certificate fields and associated information
- SSL session fields and associated information
- Static text string

You can also configure the CSS to place a prefix in the client certificate, server certificate, or SSL session fields inserted in the HTTP request header. The prefix has no effect on the insertion of a static text string.

The primary purpose of text string insertion through the **static** keyword is to support Microsoft OWA applications, however, you may have other reasons to insert static text.

Related Commands

show ssl-proxy-list ssl-server

ssl-server *number* port

To specify a virtual TCP port number for the virtual SSL server, use the **ssl-server** *number* **port** command. Use the **no** form of this command to remove a virtual port from an SSL server.

ssl-server *number* **port** *number2*

no ssl-server *number* **port** *number2*

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
port *number2*	TCP port number that matches the TCP port number for an SSL content rule. The SSL module uses the port to determine which traffic it should accept. Enter a port number from 1 to 65535. The default port is 443.

Command Modes

ssl-proxy-list configuration mode

Related Commands

show ssl-proxy-list
(config-owner-content) port

ssl-server *number* session-cache

To set the SSL cache timeout value, use the **ssl-server** *number* **session-cache** command. In SSL, a new session ID is created every time the client and CSS SSL module go through a full key exchange and establish a new master secret key. Specifying an SSL session cache timeout allows the reuse of the master key on subsequent connections between the client and the CSS SSL module, which can speed up the SSL negotiation process. Use the **no** form of this command to reset the SSL session reuse timeout back to 300 seconds.

ssl-server *number* **session-cache** *seconds*

no ssl-server *number* **session-cache**

Syntax Description

number	Index number for the virtual SSL server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
seconds	SSL session cache timeout in seconds. Enter a value from 0 to 72000 (20 hours). The default is 300 seconds (5 minutes). To disable the timeout, set the value to 0. The full SSL handshake occurs for each new connection between the client and the SSL module.

Command Modes

ssl-proxy-list configuration mode

Related Commands

show ssl-proxy-list

ssl-server *number* ssl-queue-delay

To set the amount of time for the CSS virtual SSL server to wait for packets before emptying the queued data for encryption, use the **ssl-server** *number* **ssl-queue-delay** command. Use the **no** form of this command to reset the delay to 200 milliseconds.

ssl-server *number* **ssl-queue-delay** *number2*

no ssl-server *number* **ssl-queue-delay**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
ssl-queue-delay *number2*	The time in milliseconds to wait for packets before emptying the queued data for encryption. Enter a value from 0 to 10000. The default delay is 200. Setting the value to 0 disables the queuing of data.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

The virtual SSL server on the CSS empties the data from the queue and encrypts it for transmission to the client when:

- The queue fills to 16,400 bytes (the maximum SSL record size)
- The server sends a TCP FIN packet
- When the delay time on the CSS has passed, even though the queue has less than 16,400 bytes

When you set the value to 0 to disable the queuing of data, the virtual SSL server on the CSS encrypts the data as soon as it arrives from the server and then sends the data to the client.

ssl-server *number* tcp

To configure TCP connections with a virtual SSL server, use the **ssl-server** *number* **tcp** command. You can specify:

- A timeout value that the CSS uses to terminate a TCP connection for inactivity or an unsuccessful TCP three-way handshake with a back-end SSL server
- The Nagle algorithm for the TCP connection
- The buffer size for the TCP connection

Use the **no** form of this command to reset the buffer size to 32768, restore the timeout period to 240 seconds for inactivity or 30 seconds for the three-way handshake.

ssl-server *number* **tcp** [**buffer-share** [**rx**|**tx**] *number2*|[**server**|**virtual**] **inactivity-timeout** *seconds*|**nagle** [**enable**|**disable**]|**syn-timeout** *seconds2*]

no ssl-server *number* **tcp** [**buffer-share** [**rx**|**tx**]| [**server**|**virtual**] **inactivity-timeout** |**syn-timeout**]

Syntax Description

number	Index number for the virtual SSL server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
buffer-share [**rx**|**tx**] *number2*	Sets the TCP buffering from the client or server on a given connection. • To set the amount of data in bytes that a given connection can buffer from the client traffic, use the **rx** *number2* keyword and variable. • To set the amount of data in bytes that a given connection can buffer from the server to the client, use the **tx** *number2* keyword and variable. By default, the buffer size is 32768. The buffer size can range from 16400 to 262144.
server	Specifies the TCP connection for the web server.

virtual	Specifies the TCP connection for the client.
inactivity-timeout *seconds*	Specifies the timeout value that the CSS waits to receive inbound flows before terminating the TCP connection. Enter a TCP inactivity timeout value in seconds, from 0 disabling the TCP inactivity timeout to 3600 (1 hour). The default is 240 seconds.
nagle enable|disable	Specifies the Nagle algorithm for the TCP connection. By default, the Nagle algorithm is enabled for each TCP connection. Use the **disable** keyword to disable the Nagle algorithm when you observe a delay on the TCP connection. Use the **enable** keyword to reenable the Nagle algorithm.
syn-timeout *seconds2*	Specifies a timeout value that the CSS uses to terminate a TCP connection with a web server or client that has not successfully completed the TCP three-way handshake prior to transferring data. Enter a TCP SYN timeout value in seconds, from 0 to 3600 (1 hour). The default is 30 seconds. To disable the TCP SYN timeout period, set the value to 0. The timer becomes inactive and the retransmit timer will eventually terminate a broken TCP connection. The connection timer should always be shorter than the retransmit termination time for new SSL/TCP connections.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

The TCP Nagle algorithm automatically concatenates a number of small buffer messages transmitted over the TCP connection between a client and the SSL module or between a server and the SSL module. This process increases the throughput of your CSS by decreasing the number of packets sent over each TCP connection. However, the interaction between the Nagle algorithm and the TCP delay acknowledgment may increase latency in your TCP connection. Disable the Nagle algorithm when you observe an unacceptable delay in a TCP connection (clear-text or SSL).

Related Commands

show ssl-proxy-list

ssl-server *number* unclean-shutdown

To instruct the CSS to send only a TCP FIN message to terminate a client connection, use the **ssl-server** *number* **unclean-shutdown** command. The CSS does not send a Close-Notify alert to close a client connection. The **no** version of this command resets the CSS default behavior of sending both a Close-Notify alert and a TCP FIN message to close the client connection.

ssl-server *number* **unclean-shutdown**

no ssl-server *number* **unclean-shutdown**

Usage Guidelines

Normally, the SSL Close-Notify alert terminates a connection without an error. However, some versions of MSIE browsers do not close the connection upon receiving the Close-Notify alert. The browser may attempt to reuse the connection even though it appears to be closed to the CSS. Because the CSS cannot reply to a new request on this connection, the browser may display an error.

ssl-server *number* urlrewite

To add a URL rewrite rule to the virtual SSL server and avoid nonsecure HTTP 300-series redirects by the server, use the **ssl-server** *number* **urlrewrite** command. This command instructs the CSS, through the SSL Acceleration module, to examine every HTTP header field received from the server for a 300-series redirection response (such as 302 Found or 304 Not Modified). If the CSS finds a 300-series return code, it searches the Location response-header field in the HTTP header to determine if the field matches the hostname defined in a URL rewrite rule. If there is a match, the CSS rewrites the Location field to contain an HTTPS location and the SSL port for the response. Use the **no** form of this command to remove a URL rewrite rule.

ssl-server *number* **urlrewrite** *number hostname* [**sslport** *port* {**clearport** *port*}]

no ssl-server *number* **urlrewrite** *number*

Syntax Description

number	The number used to identify the virtual SSL server in the SSL proxy list. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
urlrewrite *number*	The number of the URL rewrite rule to be added to the virtual SSL server. Enter a value between 1 and 32 corresponding to the URL rewrite rule. You can add a maximum of 32 URL rewrite rules to each SSL server for handling HTTP to HTTPS redirects.
hostname	The domain name of the URL to be redirected (for example, www.mydomain.com). Enter an unquoted text string with a maximum length of 240 characters that corresponds to the domain name of the URL rewrite host. Do not include the directory path as part of the hostname. You can use wildcards in domain names as part of the matching criteria for a URL redirect rule. An asterisk (*) wild card character may be used in the domain name to identify more than one host in a single domain. You can specify a wildcard-only hostname (for example, *), a prefix wildcard (for example, *.mydomain.com), or a suffix wildcard (for example, www.mydomain.*). name is the * character and all HTTP redirects that come through this VIP from the server are rewritten to HTTPS. In this case, there is no need to have additional URL rewrite rules for this SSL server.
sslport *port*	(Optional) Specifies the port used for SSL network traffic. Enter a TCP port number that corresponds with an SSL content rule, which uses the specified TCP port number. The SSL module rewrites an HTTP redirect matching the URL redirect rule with the specified SSL port (or default port 443 if no port number is specified). Enter a port value from 1 to 65535. The default value is 443.
clearport *port*	(Optional) Specifies the port used for clear text network traffic. The SSL module matches redirects in the Location Response-Header field with the specified clear text port (or default port 80 if no port number is specified). Enter a port value from 1 to 65535. The default value is 80.

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

Use care when specifying wildcards in domain names to avoid the unwanted rewriting of all URL references by the SSL Acceleration module. Review your redirects and ensure that every URL that matches a specified wildcard rule needs to be rewritten.

Related Commands

show ssl

ssl-server *number* version

To specify the SSL or Transport Layer Security (TLS) protocol version, use the **ssl-server** *number* **version** command. Use the **no** form of this command to reset the SSL version to the default of SSL version 3.0 and TLS version 1.0.

ssl-server *number* **version** *protocol*

no ssl-server *number* **version**

Syntax Description

number	Index number for the virtual SSL server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
protocol	Protocol version. Enter one of the following keywords: • **ssl-tls -** SSL protocol version 3.0 and TLS protocol version 1.0 (default) • **ssl -** SSL protocol version 3.0 • **tls** - TLS protocol version 1.0

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

The CSS supports SSL version 3.0 and TLS version 1.0. The CSS understands and accepts an SSL version 2.0 ClientHello message to allow dual version clients to communicate with the CSS through the SSL module. In this case, the client indicates an SSL version of 3.0 in the version 2.0 ClientHello. This indicates to the SSL module that the client can support SSL version 3.0, and the SSL module returns a version 3.0 ServerHello message.

If the client only supports SSL version 2.0 (SSL version 2.0 compliant), the CSS will be unable to pass network traffic.

Related Commands

show ssl-proxy-list

ssl-server *number* vip address

To specify a VIP address for the virtual SSL server that corresponds to a VIP address configured in a content rule, use the **ssl-server** *number* **vip address** command. Use the **no** form of this command to remove the address from the server.

ssl-server *number* **vip address** *ip_or_host*

no ssl-server *number* **vip address**

Syntax Description

number	Index number for the server. This variable identifies a server for configuration. To see a list of servers, enter: `(ssl-proxy-list)# ssl-server ?`
vip address *ip_or_host*	VIP address for the server that matches the address for an SSL content rule. The SSL module uses the address to determine which traffic it should accept. Enter a valid VIP address in either dotted-decimal IP notation (for example, 192.168.11.1) or mnemonic host-name format (for example, myhost.mydomain.com).

Command Modes

ssl-proxy-list configuration mode

Usage Guidelines

When you use the mneumonic host-name format for the VIP, the CSS includes a Domain Name Service (DNS) facility that translates host names such as to IP addresses. If the host name cannot be resolved, the VIP address setting is not accepted and an error message appears indicating host resolution failure. For details about configuring a Domain Name Service, refer to the *Cisco Content Services Switch Administration Guide.*

If the VIP address has not been defined when you activate the SSL proxy list through the **active** command, the CSS logs the following error message and does not activate the SSL proxy list.

```
VIP address or port/protocol must be specified
```

When the **active** command is entered for a content rule with a configured SSL service, the CSS verifies that each VIP address configured in the content rule matches at least one VIP address configured in the SSL proxy list in each of the added services. If a match is not found, the CSS logs the following error message and does not activate the content rule.

```
VIP address must have matching ssl-proxy-list entry
```

Related Commands

show ssl-proxy-list
(ssl-proxy-list) active
(config-owner-content) vip address

(ssl-proxy-list) suspend

To suspend an active SSL proxy list, use the **suspend** command.

suspend

Usage Guidelines

You cannot modify a server in an active SSL proxy list. You must first suspend the SSL proxy list to make modifications to any server in the list. Once you have modified the SSL proxy list, suspend the SSL service, activate the SSL proxy list, and then activate the SSL service.

Related Commands

(ssl-proxy-list) active

URQL Configuration Mode Commands

URQL configuration mode allows you to configure a Uniform Resource Locator qualifier list (URQL). A URQL is a group of URLs for content requests associated with one or more content rules. The CSS uses this list to identify which requests to send to a service.

To access URQL configuration mode, use the **urql** command from any configuration mode except ACL, boot, DQL, group, keepalive, NQL, and owner configuration modes. The prompt changes to (config-urql [*name*]). You can also use this command from URQL mode to access another URQL. For information about commands available in this mode, see the following commands.

In global configuration mode, use the **no** form of this command to delete an existing URQL.

urql *urql_name*

(config) **no urql** *existing_urql_name*

Syntax Description

urql_name	Name of a new URQL you want to create or of an existing list. Enter an unquoted text string with no spaces and a maximum length of 31 characters. To see a list of existing URQL names, enter: `urql ?`

Usage Guidelines

When you create a URQL, you must activate it with the **(config-urql) active** command.

Related Commands

show urql
(config-owner-content) url

(config-urql) active

To activate a suspended URQL, use the **active** command. By default, the URQL is initially suspended.

active

Usage Guidelines

Before you can activate a URQL, you must assign the domain for the URLs. See the **(config-urql) domain** command.

Related Commands

show urql
(config-owner-content) url
(config-urql) domain
(config-urql) suspend

(config-urql) description

To provide a description for the URL qualifier list (URQL), use the **description** command. Use the **no** form of this command to clear a description for the URQL.

description "*text*"

no description

Syntax Description

"*text*"	Description for the URQL. Enter a quoted text string with a maximum length of 64 characters.

(config-urql) domain

To assign the domain name or address of the URLs to the URQL, use the **domain** command.

domain "*name_or_ip*"

Syntax Description

"*name_or_ip*"	Name or address for the domain. Enter a quoted text string containing either: • The domain name in mnemonic host-name format (for example, myhost.mydomain.com) with a maximum of 63 characters • A valid address for the domain in dotted-decimal IP notation (for example, 192.168.11.1)

Usage Guidelines

You must assign a domain before you can activate a URQL. To change the domain address on an existing URQL, suspend the URQL, and then change the domain.

Related Commands

show urql
(config-urql) active
(config-urql) suspend

(config-urql) no

To negate a command or set it to its default, use the **no** command. For information on general **no** commands you can use in this mode, see the general **no** command. The following options are available in URQL mode.

Syntax Description

no acl *index*	Deletes an ACL
no description	Clears a description for the URQL
no owner *existing_owner_name*	Deletes an existing owner
no url number *index_number*	Deletes a URL entry from the URQL
no url number *index_number* **url**	Removes a URL from the URL entry
no url number *index_number* **description**	Clears the description for the URL entry

(config-urql) suspend

To deactivate a URQL on all currently assigned content rules, use the **suspend** command.

suspend

Usage Guidelines

To reactivate the URQL, use the **(config-urql) active** command.

Related Commands

show urql
(config-urql) active

(config-urql) url

To include the URL for content requests you want as part of the URQL, and optionally provide a description, use the **url** command. Use the **no** form of this command to remove a URL entry from a URQL, a URL from a URL number, or a description about the URL.

url *number* {**url “***name***”|description “***description***”**}

no url *number* {**url |description**}

Syntax Description

number	Number for the URL entry in the URQL. Enter a number from 1 to 1000.
url “*name***”**	Defines the URL that appears on the content request. Enter a quoted text string with a maximum length of 252 characters. The URL must match the URL GET request exactly. Wildcards, partial URL paths, and a trailing “/” character in the URL are not allowed in a URQL URL entry.
description “*description***”**	Provides a description about the URL. Enter a quoted text string with a maximum length of 64 characters.

Usage Guidelines

You must create the URL index entry before you can associate the URL name or a description to it.

Before you can reassign a different URL name to an existing URL entry, you must remove the previously assigned URL.

Related Commands

show urql
(config-owner-content) url