Cisco 4700 Series Application Control Engine Appliance Command Reference

Software Version A3(2.4) and earlier
December 2009

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-16206-02

Cisco 4700 Series Application Control Engine Appliance Command Reference

CONTENTS

CLI COMMAND SUMMARY BY MODE

Preface

This guide provides the following information:

- The command-line interface (CLI) for the Cisco 4700 Series Application Control Engine (ACE) appliance and how to use the CLI.
- The CLI commands, including syntax, options, and related commands for software release A3(2.4) and earlier.

This preface contains the following major sections:

Audience

This guide is intended for the following trained and qualified service personnel who are responsible for configuring the ACE:

- Web master
- System administrator
- System operator

How to Use This Guide

This guide is organized alphabetically by command mode, as follows:

Chapter	Description
Chapter 1, Using the Command-Line Interface	Describes how to use the command-line interface (CLI) on the ACE.
Chapter 2, CLI Commands	Provides detailed information for the following types of CLI commands for the ACE: • Commands that you can enter after you log in to the ACE. • Configuration mode commands that allow you to access global configuration mode and its subset of modes after you log in to the ACE.

Related Documentation

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

Document Title	Description
Release Note for the Cisco 4700 Series Application Control Engine Appliance	Provides information about operating considerations, caveats, and command-line interface (CLI) commands for the ACE.
Cisco Application Control Engine Appliance Hardware Installation Guide	Provides information for installing the ACE appliance.
Regulatory Compliance and Safety Information for the Cisco Application Control Engine Appliance	Regulatory compliance and safety information for the ACE appliance.
Cisco 4700 Series Application Control Engine Appliance Quick Start Guide	Describes how to use the ACE appliance Device Manager and CLI to perform the initial setup and VIP load-balancing configuration tasks.

Document Title	Description
Cisco 4700 Series Application Control Engine Appliance Administration Guide	Describes how to perform the following administration tasks on the ACE: • Setting up the ACE • Establishing remote access • Managing software licenses • Configuring class maps and policy maps • Managing the ACE software • Configuring SNMP • Configuring redundancy • Configuring the XML interface • Upgrading the ACE software
Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide	Describes how to operate your ACE in a single context or in multiple contexts.
Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide	Describes how to configure the following routing and bridging features on the ACE: • Configuring Ethernet ports • VLAN interfaces • Routing • Bridging • Dynamic Host Configuration Protocol (DHCP)
Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide	Describes how to configure the following server load-balancing features on the ACE: • Real servers and server farms • Class maps and policy maps to load balance traffic to real servers in server farms • Server health monitoring (probes) • Stickiness • Firewall load balancing • TCL scripts
Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide	Describes the configuration of the application acceleration and optimization features of the ACE. It also provides an overview and description of those features.

Document Title	Description
Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide	Describes how to configure the following ACE security features: • Security access control lists (ACLs) • User authentication and accounting using a Terminal Access Controller Access Control System Plus (TACACS+), Remote Authentication Dial-In User Service (RADIUS), or Lightweight Directory Access Protocol (LDAP) server • Application protocol and HTTP deep packet inspection • TCP/IP normalization and termination parameters • Network Address Translation (NAT)
Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide	Describes how to configure the following Secure Sockets Layer (SSL) features on the ACE: • SSL certificates and keys • SSL initiation • SSL termination • End-to-end SSL
Cisco 4700 Series Application Control Engine Appliance Command Reference	Describes how to configure system message logging on the ACE. This guide also lists and describes the system log (syslog) messages generated by the ACE.
Cisco 4700 Series Application Control Engine Appliance Device Manager GUI Configuration Guide	Describes how to use the Device Manager GUI, which resides in flash memory on the ACE, to provide a browser-based interface for configuring and managing the appliance.
Cisco CSS-to-ACE Conversion Tool User Guide	Describes how to use the CSS-to-ACE conversion tool to migrate Cisco Content Services Switches (CSS) running- or startup-configuration files to the ACE.

Symbols and Conventions

This publication uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in **boldface**. Bold text also indicates a command in a paragraph.
italic font	Arguments for which you supply values are in *italics*. Italic text also indicates the first occurrence of a new term, book title, emphasized text.
{ }	Encloses required arguments and keywords.
[ ]	Encloses optional arguments and keywords.
{ x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Convention	Description
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter in a command line is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.

Notes use the following conventions:

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

Cautions use the following conventions:

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

For additional information about CLI syntax formatting, see Chapter 1, Using the Command-Line Interface.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

Using the Command-Line Interface

The command-line interface (CLI) is a line-oriented user interface that provides commands for configuring, managing, and monitoring the Cisco 4700 Series Application Control Engine (ACE) appliance. This chapter contains the following topics:

Note The CLI uses similar syntax and other conventions to the Cisco IOS CLI, but the ACE operating system is not a version of Cisco IOS software. Do not assume that a Cisco IOS CLI command works or has the same function with the ACE.

Accessing the ACE Command Modes

When you log in to the ACE, you enter Exec mode. The Exec mode prompt begins with the hostname followed by the context name and pound sign (#). By default, the hostname for the ACE is switch. For example, if you log in to the Admin context, the following prompt appears:

```
switch/Admin#
```

If you log in as a user context (for example, you log in as user context C1), the following prompt appears:

```
switch/C1#
```

Exec mode has a set of commands that allow you to maintain the ACE and access configuration mode. To access configuration mode, use the **configure** command. This mode is identified by a (config) prompt. For example:

```
switch/Admin# configure
switch/Admin(config)#
```

Configuration mode has a set of commands that allow you to configure the ACE and access its subordinate configuration modes. When you access any of the subordinate configuration modes, the ACE appends the mode name to the (config) prompt. For example, when you access real server host configuration mode from configuration mode, the prompt changes to (config-rserver-host).

To exit a configuration mode and access the previous mode, use the **exit** command. To exit any configuration mode and return to Exec mode, press **Ctrl-Z** or use the **end** command.

Using the CLI Commands

Table 1-1 lists CLI keyboard shortcuts to help you enter and edit command lines on the ACE. For further information on using the CLI commands, see the following sections:

- Abbreviating Commands
- Editing the Command Line
- Defining Object Names
- Understanding the Effect of Contexts and Roles on Commands in Modes
- Using Exec Mode Commands in a Configuration Mode
- Understanding CLI Syntax Checking and Error Messages

Table 1-1 CLI Command Keyboard Shortcuts

Action		Keyboard Shortcut
Cancel the current operation, delete the additional display of MORE output, or delete the current line.		Ctrl-c
Change:	The word at the cursor to lowercase.	Esc l
	The word at the cursor to uppercase.	Esc u
Delete:	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
	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
Display MORE output:	Exit from MORE output.	q, Q, or Ctrl-C
	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 Enter key.	Enter
Enter an Enter or Return key character.		Ctrl-m
Expand the command or abbreviation.		Ctrl-i or Tab

Table 1-1 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 the 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
Redraw the screen at the prompt.		Ctrl-l or Ctrl-r
Return to the Exec mode from any configuration mode.		Ctrl-z
Return to the previous mode or exit from the CLI from Exec mode.		**exit** command
Transpose a character at the cursor with a character to the left of the cursor.		Ctrl-t

Abbreviating Commands

The ACE allows you to abbreviate most command keywords or options to its fewest unique characters. For example, instead of entering the full **write terminal** command, you can enter:

```
host/Admin# w t
Generating configuration....
```

Editing the Command Line

The ACE allows you to view all previously entered commands with the up arrow. Once you have examined a previously entered command, you can move forward in the list with the down arrow.

When you view a command that you wish to reuse, you can edit it or press the **Enter** key to execute it.

Defining Object Names

The following objects are user-configurable items:

- Access lists
- Class maps
- Defined interfaces
- Parameter maps
- Policy maps
- Health probes
- Real servers
- Server farms

- Scripts
- Sticky groups

The objects that you create are specific to the context where they are created. If the context is partitioned into multiple domains, you allocate objects within each domain.

The ACE supports case sensitivity when you configure an object name. If you create a context named C11 and another context c11, the ACE considers them as two different contexts. For example, enter:

```
host/Admin(config)# context C11
host/Admin(config-context)# exit
host/Admin(config)# context c11
host/Admin(config-context)# exit
```

When you perform a query for contexts, both C11 and c11 appear as separate contexts.

```
host/Admin(config)# context ?
    <WORD>  Enter the context name (Max Size - 64)
    C11
    c11
```

Understanding the Effect of Contexts and Roles on Commands in Modes

All commands are available to the Admin and the Admin context. However not all commands are available in user contexts. The ACE provides role-based access control (RBAC), which is a mechanism that determines the commands and resources available to each user. A role defines a set of permissions for accessing the objects and resources in a context and the actions that you can perform on them. The global or context administrator assigns roles to users based on their network function and the resources to which you want them to have access. For more information, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Using Exec Mode Commands in a Configuration Mode

When you are in a configuration mode, you may need to use a **show** command or any other command that is only available in Exec mode. To enter an Exec command in any configuration mode, use the **do** command. The syntax for this command is as follows:

do *exec_command_string*

The *exec_command_string* argument is the Exec mode command that you want to execute.

For example, to display the running configuration in configuration mode, enter:

```
host1/Admin(config)# do show running-config
```

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:

```
host1/Admin# test
             ^
% invalid command detected at '^' marker.
```

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

```
host1/Admin(config)# interface
                              ^
% incomplete command detected at '^' marker.
```

Getting CLI Help

The CLI provides several types of context-sensitive help, as described in the following sections:

- Using the Question Mark (?)
- Using the Tab Key

Using the 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 **?**	Any keywords, options, or object names for a command
command keyword **?**	Any keywords, options, or object names for a command
*command-abbrev***?**	All commands that begin with specific letters

Using the 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:

```
host1/Admin# sh<Tab>
host1/Admin# show
```

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.

Creating Configuration Files Using a Text Editor

This section describes how to format a text configuration file using a text editor that you can download to the ACE and contains the following topics:

To copy the file to disk0:, see *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

How Commands Correspond with Lines in the Text File

The text configuration file includes lines that correspond with the commands described in this guide. In most cases, the command examples in this guide show how to enter the command preceded by the applicable CLI prompt. For example:

```
host1/Admin(config)# resource-class abc
```

In the text configuration file, you are not prompted to enter commands, so the prompt is omitted:

```
resource-class abc
```

Subordinate Commands

Subordinate commands appear indented under the main command when entered at the command line. Your text file lines do not need to be indented, as long as the subcommands appear directly following the main command. For example, the following unindented text is read the same as indented text:

```
resource-class abc
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource rate syslog minimum 0.00 maximum unlimited
```

Automatic Text Entries

When you download a configuration file to the ACE, the ACE inserts some lines automatically. For example, the ACE inserts lines for default settings and for the date and time that the configuration was modified. You do not need to enter these automatic entries when you create your text file.

Line Order

For the most part, commands can be in any order in the file. However, some lines, such as entries for access control lists (ACLs), are processed in the order that they appear, and the order can affect the function of the ACL. Other commands might also have order requirements. For example, you must enter the **interface vlan** command for an interface before you assign an IP address to it because many subsequent commands use the name of the interface. Also, subcommands must directly follow the main command.

Passwords

The user password is automatically encrypted before it is stored in the configuration. For example, the encrypted form of the letmein password might look like jMorNbK0514fadBh. You can copy the configuration passwords to another ACE in their encrypted form, but you cannot unencrypt the passwords yourself.

If you enter an unencrypted password in a text file, the ACE does not automatically encrypt them when you copy the configuration to the ACE. The ACE encrypts them only when you save the running configuration from the command line using the **copy running-config startup-config** or **write memory** command.

CHAPTER 2

CLI Commands

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

- Commands that you can enter after you log in to the ACE.
- Configuration mode commands that allow you to access configuration mode and its subset of modes after you log in to the ACE.

The description of each command includes the following:

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

Exec Mode Commands

You can access Exec mode commands immediately after you log in to an ACE. Many of these commands are followed by keywords that make them distinct commands (for example, **show aaa**, **show access-list**, **show accounting**, and so on). To increase readability of command syntax, these commands are presented separately in this command reference.

You can also execute Exec mode commands from any of the configuration modes using the **do** command. For example, to display the ACE running configuration from the Exec mode, use the **show running-config** command. To execute the same command from the configuration mode, use the **do show running-config** command.

capture

To enable the context packet capture function for packet sniffing and network fault isolation, use the **capture** command. As part of the packet capture process, you specify whether to capture packets from all interfaces or an individual VLAN interface.

capture *buffer_name* {{**all** | {**interface vlan** *number*}} **access-list** *name* [**bufsize** *buf_size* [**circular-buffer**]]} | **remove** | **start** | **stop**

Syntax Description

buffer_name	Name of the packet capture buffer. The *buffer_name* argument associates the packet capture with a name. Specify an unquoted text string with no spaces from 1 to 80 alphanumeric characters.
all	Specifies that packets from all input interfaces are captured.
interface	Specifies a particular input interface from which to capture packets.
vlan *number*	Specifies the VLAN identifier associated with the interface.
access-list *name*	Selects packets to capture based on a specific access list. A packet must pass the access list filters before the packet is stored in the capture buffer. Specify a previously created access list identifier. Enter an unquoted text string with a maximum of 64 characters. **Note** Ensure that the access list is for an input interface; input is considered with regards to the direction of the session that you wish to capture. If you configure the packet capture on the output interface, the ACE will fail to match any packets.
bufsize *buf_size*	(Optional) Specifies the buffer size, in kilobytes (KB), used to store the packet capture. The range is from 1 to 5000 KB.
circular-buffer	(Optional) Enables the packet capture buffer to overwrite itself, starting from the beginning, when the buffer is full.
remove	Clears the packet capture configuration.
start	Starts the packet capture function and displays the messages on the session console as the ACE receives the packets. The CLI prompt returns and you can type other commands at the same time that the ACE is capturing packets. To stop the capture process, use the **stop** option. The packet capture function automatically stops when the buffer is full unless you enable the circular buffer function.
stop	Stops the packet capture process after a brief delay.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	The **stop** option was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The packet capture function enables access control lists (ACLs) to control which packets are captured by the ACE on the input interface. If the ACLs are selecting an excessive amount of traffic for the packet capture operation, the ACE will see a heavy load, which can cause a degradation in performance. We recommend that you avoid using the packet capture function when high network performance is critical.

Under high traffic conditions, you may observe up to 64 packets printing on the console after you enter the **stop** keyword. These additional messages can occur because the packets were in transit or buffered before you entered the **stop** keyword.

The capture packet function works on an individual context basis. The ACE traces only the packets that belong to the context where you execute the **capture** command. You can use the context ID, which is passed with the packet, to isolate packets that belong to a specific context. To trace the packets for a single specific context, use the **changeto** command and enter the **capture** command for the new context.

The ACE does not automatically save the packet capture in a configuration file. To copy the capture buffer information as a file in flash memory, use the **copy capture** command.

Examples

To start the packet capture function for CAPTURE1, enter:

```
host1/Admin# capture CAPTURE1 interface vlan50 access-list ACL1
host1/Admin# capture CAPTURE1 start
```

To stop the packet capture function for CAPTURE1, enter:

```
host1/Admin# capture CAPTURE1 stop
```

Related Commands

clear icmp statistics
copy capture
show capture

changeto

To move from one context on the ACE to another context, use the **changeto** command.

changeto *context_name*

Syntax Description

context_name	Name of an existing context. This argument is case sensitive.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(2.2)	You can apply the changeto feature to a rule for a user-defined role.

Usage Guidelines

This command requires the changeto feature in your user role, and as found in all of the predefined user roles. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Only users authorized in the admin context or configured with the changeto feature can use the **changeto** command to navigate between the various contexts. Context administrators without the changeto feature, who have access to multiple contexts, must explicitly log in to the other contexts to which they have access.

The command prompt indicates the context that you are currently in (see the following example).

The predefined user role that is enforced after you enter the **changeto** command is that of the Admin context and not that of the non-Admin context.

You cannot add, modify, or delete objects in a custom domain after you change to a non-Admin context.

- If you originally had access to the default-domain in the Admin context prior to moving to a non-Admin context, the ACE allows you to configure any object in the non-Admin context.
- If you originally had access to a custom domain in the Admin context prior to moving to a non-Admin context, any created objects in the non-Admin context will be added to the default-domain. However, an error message will appear when you attempt to modify existing objects in the non-Admin context.

User-defined roles configured with the changeto feature retain their privileges when accessing different contexts.

Examples

To change from the Admin context to the context CTX1, enter:

```
host1/Admin# changeto CTX1
host1/CTX1#
```

Related Commands

exit
show context
(config) context
(config-role) rule

checkpoint

To create or modify a checkpoint (snapshot) of the running configuration, use the **checkpoint** command.

checkpoint {**create** | **delete** | **rollback**} *name*

Syntax Description

create	Creates a new checkpoint with the value of *name*.
delete	Deletes the existing checkpoint with the value of *name.*

rollback	Reverts back to the checkpoint with the value of *name*.
name	Name of a new or existing checkpoint. Specify a text string from 1 to 64 alphanumeric characters (no spaces).

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To create the checkpoint CP102305, enter:

```
host1/Admin# checkpoint create CP102305
```

Related Commands

show checkpoint

clear access-list

To clear access control list (ACL) statistics, use the **clear access-list** command.

clear access-list *name*

Syntax Description

name	Name of an existing ACL.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the access-list feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To clear the access control list ACL1, enter:

```
host1/Admin# clear access-list ACL1
```

Related Commands

show access-list
(config) access-list ethertype
(config) access-list extended

clear accounting log

To clear the accounting log, use the **clear accounting log** command.

clear accounting log

Syntax Description

This command has no keywords or arguments.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To clear the accounting log, enter:

```
host1/Admin# clear accounting log
```

Related Commands

show accounting log
(config) aaa accounting default

clear arp

To clear the Address Resolution Protocol (ARP) entries in the ARP table or statistics with ARP processes, use the **clear arp** command.

clear arp [**no-refresh** | {**statistics** [**vlan** *number*] [*interface_name*]}]

Syntax Description

no-refresh	(Optional) Removes the learned ARP entries from the ARP table without refreshing the ARP entries.
statistics [**vlan** *number*]	(Optional) Clears ARP statistics counters globally or for the specified VLAN, **vlan** *number*.
[*interface_name*]	(Optional) Clears ARP statistics counters globally or for the specified interface, *interface_name*.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised with the **vlan** option.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

If you enter the **clear arp** command with no option, it clears all learned ARP entries and then refreshes the ARP entries.

Examples

To clear the ARP statistics, enter:

```
host1/Admin# clear arp statistics
```

To clear the ARP learned entries and then refresh the ARP entries, enter:

```
host1/Admin# clear arp
```

Related Commands

show arp
(config) arp

clear buffer stats

To clear the control plane buffer statistics, use the **clear buffer stats** command.

clear buffer stats

Syntax Description

This command has no keywords or arguments.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

This command is intended for use by trained Cisco personnel for troubleshooting purposes only.

Examples

To clear the control plane buffer statistics, enter:

```
host1/Admin# clear buffer stats
```

Related Commands

show buffer

clear capture

To clear an existing capture buffer, use the **clear capture** command.

clear capture *name*

Syntax Description

name	Name of an existing capture buffer.

Command Modes

Exec

Admin and user context

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Use the **dir** command to view the capture files that you copied to the disk0: file system using the **copy capture** command.

Examples

To clear the capture buffer CAPTURE1, enter:

```
host1/Admin# clear capture CAPTURE1
```

Related Commands

capture
copy capture
dir
show capture

clear conn

To clear a connection that passes through, terminates, or originates with the ACE, use the **clear conn** command.

clear conn [**all** | **flow** {*prot_number* | **icmp** | **tcp** | **udp** {*source_ip* | *source_port* | *dest_ip* | *dest_port*}} | **rserver** *name* [*port_number*] **serverfarm** *sfarm_name*]

Syntax Description

all	(Optional) Clears all connections that go through the ACE, originate with the ACE, or terminate with the ACE.
flow	(Optional) Clears the connection that matches the specified flow descriptor.
prot_number	Protocol number of the flow.
icmp	Specifies the flow types using ICMP.
tcp	Specifies the flow types using TCP.
udp	Specifies the flow types using UDP.
source_ip	Source IP address of the flow. Enter an IP address in dotted-decimal notation (for example, 172.27.16.10).
source_port	Source port of the flow.
dest_ip	Destination IP address of the flow. Enter an IP address in dotted-decimal notation (for example, 172.27.16.10).
dest_port	Destination port of the flow.
rserver *name*	(Optional) Clears all connections to the specified real server.
port_number	(Optional) Port number associated with the specified real server. Enter an integer from 1 to 65535.
serverfarm *sfarm_name*	Clears all connections to the specified real server associated with this server farm.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised.

Usage Guidelines

This command requires the loadbalance, inspect, NAT, connection, or SSL feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To clear only the connections that go through the ACE (flows that pass through the ACE between the originating network host and the terminating network host), use the **clear conn** command without any keywords. When you do not include any keywords, the connections that terminate or originate with the ACE are not cleared.

Examples

To clear the connections for the real server RSERVER1, enter:

```
host1/Admin# clear conn rserver RSERVER1
```

Related Commands

show conn

clear cores

To clear all of the core dumps stored in the core: file system, use the **clear cores** command.

clear cores

Syntax Description

This command has no keywords or arguments.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Note The ACE creates a core dump when it experiences a fatal error. Core dump information is for Cisco Technical Assistance Center (TAC) use only. We recommend that you contact TAC for assistance in interpreting the information in the core dump.

To view the list of core files in the core: file system, use the **dir core:** command.

To save a copy of a core dump to a remote server before clearing it, use the **copy capture** command.

To delete a specific core dump file from the core: file system, use the **delete core:** command.

Examples

To clear all core dumps, enter:

```
host1/Admin# clear cores
```

Related Commands

copy capture
delete
dir

clear crypto session-cache

To clear the session cache information in the context, use the **clear crypto session-cache** command.

clear crypto session-cache [**all**]

Syntax Description

all	(Optional) Clears the session cache information for all contexts. This option is available in the Admin context only.

Command Modes

Exec

Admin and user context. The **all** option is available in the Admin context only.

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To clear the session cache information in the context, enter:

```
host1/Admin# clear crypto session-cache
```

Related Commands

This command has no related commands.

clear debug-logfile

To remove a debug log file, use the **clear debug-logfile** command.

clear debug-logfile *filename*

Syntax Description

filename	Name of an existing debug log file.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The ACE debug commands are intended for use by trained Cisco personnel only. Entering these commands may cause unexpected results. Do not attempt to use these commands without guidance from Cisco support personnel.

Examples

To clear the debug log file DEBUG1, enter:

```
host1/Admin# clear debug-logfile DEBUG1
```

Related Commands

debug
show debug

clear fifo stats

To clear the control plane packet first in, first out (FIFO) statistics, use the **clear fifo stats** command.

clear fifo stats

Syntax Description

This command has no keywords or arguments.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

This command is intended for use by trained Cisco personnel for troubleshooting purposes only.

Examples

To clear the control plane FIFO statistics, enter:

```
host1/Admin# clear fifo stats
```

Related Commands

show fifo

clear ft

To clear the various fault-tolerant (FT) statistics, use the **clear ft** command.

clear ft {**all** | **ha-stats** | **hb-stats** | **history** {**cfg_cntlr** | **ha_dp_mgr** | **ha_mgr**} | **track-stats** [**all**]}

Syntax Description

all	Clears all redundancy statistics, including all TL, heartbeat, and tracking counters.
ha-stats	Clears all transport layer-related counters that the ACE displays as part of the **show ft peer detail** command output.
hb-stats	Clears all heartbeat-related statistics. When you enter this command for the first time, the ACE sets the heartbeat statistics counters to zero and stores a copy of the latest statistics locally. From that point on, when you enter the **show ft hb-stats** command, the ACE displays the difference between the statistics that are stored locally and the current statistics.
history	Clears the redundancy history statistics.
track-stats	Clears tracking-related statistics for the Admin FT group only, a user context FT group only, or for all FT groups that are configured in the ACE.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was extensively revised. This version of software introduced the **all**, **ha-stats**, **hb-stats**, **history**, and **track-stats** keywords, and removed the original **stats** keyword.

Usage Guidelines

This command requires the fault-tolerant feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To clear all fault-tolerant statistics, enter:

```
host1/Admin# clear ft all
```

Related Commands

show ft
(config) ft auto-sync
(config) ft group
(config) ft interface vlan
(config) ft peer
(config) ft track host
(config) ft track interface

clear icmp statistics

To clear the Internet Control Message Protocol (ICMP) statistics, use the **clear icmp statistics** command.

clear icmp statistics

Syntax Description This command has no keywords or arguments.

Command Modes Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples To clear the ICMP statistics, enter:

```
host1/Admin# clear icmp statistics
```

Related Commands **show icmp statistics**

clear interface

To clear the interface statistics, use the **clear interface** command.

clear interface [**bvi** *number* | **vlan** *number* | **gigabitEthernet** *slot_number/port_number*]

Syntax Description

bvi *number*	(Optional) Clears the statistics for the specified Bridge Group Virtual Interface (BVI).

vlan *number*	(Optional) Clears the statistics for the specified VLAN.
gigabitEthernet *slot_number/ port_number*	(Optional) Clears the statistics for the specified Gigabit Ethernet slot and port. • The *slot_number* represents the physical slot on the ACE containing the Ethernet ports. This selection is always 1. • The *port_number* represents the physical Ethernet port on the ACE. Valid selections are 1 through 4. This keyword is available in the Admin context only.

Command Modes

Exec

BVI and VLAN—Admin and user contexts

Ethernet data port—Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the interface feature in your user role. In addition, the Ethernet data port interface command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To clear all of the interface statistics, enter the **clear interface** command without using the optional keywords.

Examples

To clear all of the interface statistics for VLAN 212, enter:

```
host1/Admin# clear interface vlan 212
```

To clear the statistics for Ethernet port 3, enter:

```
host1/Admin# clear interface gigabitEthernet 1/3
```

Related Commands

show interface
(config) interface

clear ip

To clear the IP and Dynamic Host Configuration Protocol (DHCP) relay statistics, use the **clear ip** command.

clear ip [**dhcp relay statistics** | **statistics**]

Syntax Description

dhcp relay statistics	(Optional) Clears all of the DHCP relay statistics.
statistics	(Optional) Clears all of the statistics associated with IP normalization, fragmentation, and reassembly.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the DHCP feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To clear the IP and DHCP relay statistics, execute the **clear ip** command without using the optional keywords.

Examples

To clear all of the IP normalization, fragmentation, and reassembly statistics, enter:

```
host1/Admin# clear ip statistics
```

Related Commands

show ip

clear line

To close a specified virtual terminal (VTY) session, use the **clear line** command.

clear line *vty_name*

Syntax Description

vty_name	Name of a VTY session. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To terminate the VTY session VTY1, enter:

```
host1/Admin# clear line VTY1
```

Related Commands

(config) line vty

clear logging

To clear information stored in the logging buffer, use the **clear logging** command.

clear logging [**disabled** | **rate-limit**]

Syntax Description

disabled	(Optional) Clears the logging buffer of "disabled" messages.
rate-limit	(Optional) Clears the logging buffer of "rate-limit configuration" messages.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To clear all of the information stored in the logging buffer, enter the **clear logging** command without using either of the optional keywords.

Examples

To clear all of the information stored in the logging buffer, enter:

```
host1/Admin# clear logging
```

Related Commands

show logging
(config) logging buffered

clear netio stats

To clear the control plane network I/O statistics, use the **clear netio stats** command.

clear netio stats

Syntax Description

This command has no keywords or arguments.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

This command is intended for use by trained Cisco personnel for troubleshooting purposes only.

Examples

To clear the control plane network I/O statistics, enter:

```
host1/Admin# clear netio stats
```

Related Commands

show netio

clear ntp statistics

To clear the NTP statistics that display when you enter the **show ntp** command, use the **clear ntp** command.

clear ntp statistics {**all-peers** | **io** | **local** | **memory**}

Syntax Description

all-peers	Clears all peer statistics.
io	Clears the I/O statistics.
local	Clears the local statistics.
memory	Clears the memory statistics.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To clear the NTP memory statistics, enter:

```
host1/Admin# clear ntp statistics memory
```

Related Commands

(config) ntp

clear probe

To clear the probe statistics displayed through the **show probe** command, use the **clear probe** command.

clear probe *name*

Syntax Description

name	Name of an existing probe.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the probe feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To clear all the statistics for the probe HTTP1, enter:

```
host1/Admin# clear probe HTTP1
```

Related Commands

show probe
(config) probe

clear processes log

To clear the statistics for the processes log, use the **clear processes log** command.

clear processes log {**all** | **pid** *id*}

Syntax Description

all	Clears all statistics for the processes logs.
pid *id*	Specifies the processes log to clear.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To display the list of process identifiers assigned to each of the processes running on the ACE, use the **show processes** command.

Examples

To clear all the statistics for the processes log, enter:

```
host1/Admin# clear processes log all
```

Related Commands

show processes

clear rserver

To clear the real server statistics of all instances of a particular real server regardless of the server farms that it is associated with, use the **clear rserver** command.

clear rserver *name*

Syntax Description

name	Name of the real server.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the rserver feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

If you have redundancy configured, then you need to explicitly clear real-server statistics on both the active and the standby ACEs. Clearing statistics on the active appliance only will leave the standby appliance's statistics at the old values.

Examples

To clear the statistics for the real server RS1, enter:

```
host1/Admin# clear rserver RS1
```

Related Commands

show rserver
(config) rserver

clear rtcache

To clear the route cache, use the **clear rtcache** command.

clear rtcache

Syntax Description

This command has no keywords or arguments.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To clear the route cache, enter:

```
host1/Admin# clear rtcache
```

Related Commands This command has no related commands.

clear screen

To clear the display screen, use the **clear screen** command.

clear screen

Syntax Description This command has no keywords or arguments.

Command Modes Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples To clear the display screen, enter:

```
host1/Admin# clear screen
```

Related Commands This command has no related commands.

clear serverfarm

To clear the statistics for all real servers in a specific server farm, use the **clear serverfarm** command.

clear serverfarm *name* [**retcode**]

Syntax Description

name	Name of an existing server farm.
retcode	(Optional) Clears the return-code statistics for the server farm.

Command Modes Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised.

Usage Guidelines

This command requires the serverfarm feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To clear the statistics for the server farm SFARM1, enter:

```
host1/Admin# clear serverfarm SFARM1
```

Related Commands

show serverfarm
(config) serverfarm

clear service-policy

To clear the service policy statistics, use the **clear service-policy** command.

clear service-policy *policy_name*

Syntax Description

policy_name	Name of an existing policy map that is currently in service (applied to an interface).

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the interface feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To clear the statistics for the service policy HTTP1, enter:

```
host1/Admin# clear service-policy HTTP1
```

Related Commands show service-policy

clear ssh

To clear a Secure Shell (SSH) session or clear the public keys of all SSH hosts, use the **clear ssh** command.

clear ssh {*session_id* | **hosts**}

Syntax Description

session_id	Identifier of the SSH session to clear, terminating the session.
hosts	Clears the public keys of all trusted SSH hosts.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To obtain the specific SSH session ID value, use the **show ssh session-info** command.

Examples

To clear the SSH session with the identifier 345, enter:

```
host1/Admin# clear ssh 345
```

Related Commands

clear telnet
show ssh
(config) ssh key
(config) ssh maxsessions

clear startup-config

To clear the startup configuration of the current context, use the **clear startup-config** command.

clear startup-config

Syntax Description

This command has no keywords or arguments.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Clearing the startup configuration does not affect the context running-configuration.

The **clear startup-config** command does not remove license files or crypto files (certs and keys) from the ACE. To remove license files, see the **license uninstall** command. To remove crypto files, see the **crypto delete** command.

To clear the startup configuration, you can also use the **write erase** command.

Before you clear a startup configuration, we recommend that you back up your current startup configuration to a file on a remote server using the **copy startup-config** command. Once you clear the startup configuration, you can perform one of the following processes to recover a copy of an existing configuration:

- Use the **copy running-config startup-config** command to copy the contents of the running configuration to the startup configuration.
- Upload a backup of a previously saved startup-configuration file from a remote server using the **copy startup-config** command.

Examples

To clear the startup configuration, enter:

```
host1/Admin# clear startup-config
```

Related Commands

copy capture
show startup-config
write

clear stats

To clear the statistical information stored in the ACE buffer, use the **clear stats** command.

clear stats {**all** | **connection** | {**crypto** [**client** | **server** [**alert** | **authentication** | **cipher** | **termination**]]} | **http** | **inspect** | **kalap** | **loadbalance** [**radius** | **rdp** | **rtsp** | **sip**] | **optimization** | **probe** | **resource-usage** | **sticky**}

Syntax Description

all	Clears all statistical information in a context. The **all** keyword also clears the resource usage counters.
connection	Clears connection statistical information.
crypto	Clears TLS and SSL statistics from the context. If you do not enter the **client** or **server** option, the ACE clears both the client and server statistics.
client	(Optional) Clears the complete TLS and SSL client statistics for the current context.
server	(Optional) Clears the complete TLS and SSL server statistics for the current context.
alert	(Optional) Clears the back-end SSL alert statistics.
authentication	(Optional) Clears the back-end SSL authentication statistics.
cipher	(Optional) Clears the back-end SSL cipher statistics.
termination	(Optional) Clears the back-end SSL termination statistics.
http	Clears HTTP statistical information.
inspect	Clears HTTP inspect statistical information.
kalap	Clears the global server load-balancing (GSLB) statistics.
loadbalance	Clears load-balancing statistical information.
radius	(Optional) Clears Remote Authentication Dial-In User Service (RADIUS) load-balancing statistical information.
rdp	(Optional) Clears Reliable Datagram Protocol (RDP) load-balancing statistical information.
rtsp	(Optional) Clears Real-Time Streaming Protocol (RTSP) load-balancing statistical information.
sip	(Optional) Clears Session Initiation Protocol (SIP) load-balancing statistical information.
optimization	Clears HTTP optimization statistics
probe	Clears probe statistical information.
resource-usage	Clears resource usage-related context statistics
sticky	Clears sticky statistical information.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	The **resource-usage** keyword was added.
A3(2.1)	The **crypto** keyword and **client** | **server** [**alert** | **authentication** | **cipher** | **termination**] options were added.

Usage Guidelines

This command requires the loadbalance, inspect, NAT, connection, or SSL feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

If you have redundancy configured, then you need to explicitly clear sticky statistics on both the active and the standby ACEs. Clearing statistics on the active appliance only will leave the standby appliance's statistics at the old values.

Examples

To clear sticky statistics, enter:

```
host1/Admin# clear stats sticky
```

Related Commands

show stats

clear sticky database

To clear sticky database entries, use the **clear sticky database** command.

clear sticky database {**all** | **group** *name*}

Syntax Description

all	Clears all dynamic sticky database entries in a context.
group *name*	Clears all dynamic sticky database entries for the specified sticky group.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the interface feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

This command does not clear static sticky database entries. To clear static sticky database entries, use the **no** form of the appropriate sticky configuration mode command. For example, enter **(config-sticky-cookie) static cookie-value** or **(config-sticky-header) static header-value**.

Examples

To clear all dynamic sticky database entries in the Admin context, enter:

```
host1/Admin# clear sticky database all
```

Related Commands

show sticky database

clear syn-cookie

To clear the SYN cookie statistics, use the **clear syn-cookie** command. To clear SYN cookie statistics for all VLANs that are configured in the current context, enter the command with no arguments.

clear syn-cookie [**vlan** *number*]

Syntax Description

vlan *number*	(Optional) Instructs the ACE to clear SYN cookie statistics for the specified interface. Enter an integer from 2 to 2024.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To clear SYN cookie statistics for VLAN 100, enter:

```
host1/C1# clear syn-cookie vlan 100
```

Related Commands

show syn-cookie

clear tcp statistics

To clear all of the TCP connections and normalization statistics, use the **clear tcp statistics** command.

clear tcp statistics

Syntax Description

This command has no keywords or arguments.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the interface feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To clear the TCP statistics, enter:

```
host1/Admin# clear tcp statistics
```

Related Commands

show tcp statistics

clear telnet

To clear a Telnet session, use the **clear telnet** command.

clear telnet *session_id*

Syntax Description

session_id	Identifier of the Telnet session to clear, terminating the session.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To obtain the specific Telnet session identification number, use the **show telnet** command.

Examples

To clear the Telnet session with the identification number of 236, enter:

```
host1/Admin# clear telnet 236
```

Related Commands

clear ssh
show telnet

telnet

clear udp statistics

To clear the User Datagram Protocol (UDP) connection statistics, use the **clear udp statistics** command.

clear udp statistics

Syntax Description This command has no keywords or arguments.

Command Modes Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines This command requires the interface feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples To clear the UDP statistics, enter:

```
host1/Admin# clear udp statistics
```

Related Commands show udp statistics

clear user

To clear a user session, use the **clear user** command.

clear user *name*

Syntax Description

name	Name of the user to log out.

Command Modes Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To display the list of users that are currently logged in to the ACE, use the **show users** command.

Examples

To log out the user USER1, enter:

```
host1/Admin# clear user USER1
```

Related Commands

show users
(config) username

clear vnet stats

To clear control plane virtual network (VNET) device statistics, use the **clear vnet stats** command.

clear vnet stats

Syntax Description

This command has no keywords or arguments.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

This command is intended for use by trained Cisco personnel for troubleshooting purposes only.

Examples

To clear the VNET statistics, enter:

```
host1/Admin# clear vnet stats
```

Related Commands show vnet

clear xlate

To clear the global address to the local address mapping information based on the global address, global port, local address, local port, interface address as global address, and NAT type, use the **clear xlate** command.

clear xlate [{**global** | **local**} *start_ip* [*end_ip* [**netmask** *netmask*]]] [{**gport** | **lport**} *start_port* [*end_port*]] [**interface vlan** *number*] [**state static**] [**portmap**]

Syntax Description

global	(Optional) Clears the active translation by the global IP address.
local	(Optional) Clears the active translation by the local IP address.
start_ip	Global or local IP address or the first IP address in a range of addresses. Enter an IP address in dotted-decimal notation (for example, 172.27.16.10).
end_ip	(Optional) Last IP address in a global or local range of IP addresses. Enter an IP address in dotted-decimal notation (for example, 172.27.16.10).
netmask *netmask*	(Optional) Specifies the network mask for global or local IP addresses. Enter a mask in dotted-decimal notation (for example, 255.255.255.0).
gport	(Optional) Clears active translations by the global port.
lport	(Optional) Clears active translations by the local port.
start_port	Global or local port number.
end_port	(Optional) Last port number in a global or local range of ports.
interface vlan *number*	(Optional) Clears active translations by the VLAN number.
state static	(Optional) Clears active translations by the state.
portmap	(Optional) Clears active translations by the port map.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the NAT feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

When you enter this command, the ACE releases sessions that are using the translations (Xlates).

If you configure redundancy, then you need to explicitly clear Xlates on both the active and the standby ACEs. Clearing Xlates on the active appliance does not clear Xlates in the standby appliance.

Examples

To clear all static translations, enter:

```
host1/Admin# clear xlate state static
```

Related Commands

show xlate

clock set

To set the time and the date for an ACE, use the **clock set** command in Exec mode.

clock set *hh:mm:ss DD MONTH YYYY*

Syntax Description

hh:mm:ss	Current time to which the ACE clock is being reset. Specify one or two digits for the hour, minutes, and seconds.
DD MONTH YYYY	Current date to which the ACE clock is being reset. Specify the full name of the month, one or two digits for the day, and four digits for the year. The following month names are recognized: • January • February • March • April • May • June • July • August • September • October • November • December

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

When you enter this command, the ACE displays the current configured date and time.

If you want to use the Network Time Protocol (NTP) to automatically synchronize the ACE system clock to an authoritative time server (such as a radio clock or an atomic clock), see Chapter 1, Setting Up the ACE, in the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*. In this case, the NTP time server automatically sets the ACE system clock.

If you previously configured NTP on an ACE, the ACE prevents you from using the **clock set** command and displays an error message. To manually set the ACE system clock, remove the NTP peer and NTP server from the configuration before setting the clock on an ACE.

Examples

For example, to specify a time of 1:38:30 and a date of October 7, 2008, enter:

```
host1/Admin# clock set 01:38:30 7 Oct 2008
Wed Oct 7 01:38:30 PST 2008
```

Related Commands

show clock
(config) clock timezone
(config) clock summer-time

configure

To change from the Exec mode to the configuration mode, use the **configure** command.

configure [**terminal**]

Syntax Description

terminal	(Optional) Enables you to configure the system from the terminal.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires one or more features assigned to your user role, such as the AAA, interface, or fault-tolerant features. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To return to the Exec mode from the configuration mode, use the **exit** command.

To execute an Exec mode command from any of the configuration modes, use the **do** version of the command.

Examples

To change to the configuration mode from the Exec mode, enter:

```
host1/Admin# configure
host1/Admin(config)#
```

Related Commands

exit

copy capture

To copy an existing context packet capture buffer as the source file in the ACE compact flash to another file system, use the **copy capture** command.

copy capture *capture_name* **disk0:** [*path/*]*destination_name*

Syntax Description

capture_name	Name of the packet capture buffer on the disk0: file system. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
disk0:	Specifies that the buffer is copied to the disk0: file system.
[*path/*]*destination_name*	Destination path (optional) and name for the packet capture buffer. Specify a text string from 1 to 80 alphanumeric characters. If you do not provide the optional path, the ACE copies the file to the root directory on the disk0: file system.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the config-copy feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

After you copy a capture file to a remote server, you can use the **delete disk0:***filename* command to delete the file from the ACE and free memory.

Examples

To copy the packet capture buffer to a file in disk0: called MYCAPTURE1, enter:

```
host1/Admin# copy capture CAPTURE1 disk0:MYCAPTURE1
```

Related Commands

clear capture
show capture

copy core:

To copy a core file to a remote server, use the **copy core:** command.

copy core:*filename* **disk0:**[*path/*\]*filename* | {**ftp://***server*/*path*[*/filename*] | **sftp://**[*username*@]*server*/*path*[*/filename*] | **tftp://***server*[**:***port*]/*path*[*/filename*]}

Syntax Description

filename1	Filename of the core dump residing on the ACE in flash memory. Use the **dir core:** command to view the core dump files available in the core: file system.
disk0:[*path/*\]*filename2*	Specifies that the file destination is the disk0: directory of the current context and the filename for the core. If you do not provide the optional path, the ACE copies the file to the root directory on the disk0: file system.
ftp://*server*/*path*[*/filename*]	Specifies the File Transfer Protocol (FTP) network server and optional renamed core dump.
sftp://[*username*@]*server*/*path*[*/filename*]	Specifies the Secure File Transfer Protocol (SFTP) network server and optional renamed core dump.
tftp://*server*[**:***port*]/*path*[*/filename*]	Specifies the Trivial File Transfer Protocol (TFTP) network server and optional renamed core dump.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the config-copy feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To display the list of available core files, use the **dir core:** command. Copy the complete filename (for example, 0x401_vsh_log.25256.tar.gz) into the **copy core:** command.

When you select a destination file system using **ftp:**, **sftp:**, or **tftp:**, the ACE does the following:

- Prompts you for your username and password if the destination file system requires user authentication.
- Prompts you for the server information if you do not provide the information with the command.
- Copies the file to the root directory of the destination file system if you do not provide the path information.

Examples

To copy a core file from the ACE to a remote FTP server, enter:

```
host1/Admin# copy core:ixp0_crash.txt ftp://192.168.1.2
```

```
Enter the destination filename[]? [ixp0_crash.txt]
Enter username[]? user1
Enter the file transfer mode[bin/ascii]: [bin]
Password:
Passive mode on.
Hash mark printing on (1024 bytes/hash mark).
```

Note The **bin** (binary) file transfer mode is intended for transferring compiled files (executables). The **ascii** file transfer mode is intended for transferring text files, such as config files. The default selection of **bin** should be sufficient in all cases when copying files to a remote FTP server.

Related Commands dir

copy disk0:

To copy a file from one directory in the disk0: file system of flash memory to another directory in disk0: or a network server, use the **copy disk0:** command.

copy disk0:[*path/*]*filename1* {**disk0:**[*path/*]*filename2* | **ftp://***server/path*[*/filename*] | **image:***image_filename* | **sftp://**[*username@*]*server/path*[*/filename*] | **tftp://***server*[**:***port*]*/path*[*/filename*] | **running-config** | **startup-config**}

Syntax Description

disk0:[*path/*]*filename1*	Specifies the name of the file to copy in the disk0: file system. Use the **dir disk0:** command to view the files available in disk0:. If you do not provide the optional path, the ACE copies the file from the root directory on the disk0: file system.
disk0:[*path/*]*filename2*	Specifies that the file destination is the disk0: directory of the current context and the filename for the core. If you do not provide the optional path, the ACE copies the file to the root directory on the disk0: file system.
ftp://*server/path*[*/filename*]	Specifies the File Transfer Protocol (FTP) network server and optional renamed file.
image:*image_filename*	Specifies the image: filesystem and the image filename.
sftp://[*username@*]*server/path*[*/filename*]	Specifies the Secure File Transfer Protocol (SFTP) network server and optional renamed file.
ftp://*server*[**:***port*]*/path*[*/filename*]	Specifies the Trivial File Transfer Protocol (TFTP) network server and optional renamed file.
running-config	Specifies to replace the running-configuration file that currently resides on the ACE in volatile memory.
startup-config	Specifies to replace the startup-configuration file that currently resides on the ACE in flash memory.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the config-copy feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

When you select a destination file system using **ftp:**, **sftp:**, or **tftp:**, the ACE does the following:

- Prompts you for your username and password if the destination file system requires user authentication.
- Prompts you for the server information if you do not provide the information with the command.
- Copies the file to the root directory of the destination file system if you do not provide the path information.

Examples

To copy the file called SAMPLEFILE to the MYSTORAGE directory in flash memory, enter:

```
host1/Admin# copy disk0:samplefile disk0:MYSTORAGE/SAMPLEFILE
```

Related Commands

dir

copy ftp:

To copy a file, software image, running-configuration file, or startup-configuration file from a remote File Transfer Protocol (FTP) server to a location on the ACE, use the **copy ftp:** command.

copy ftp://*server*/*path*[/*filename*] {**disk0:**[*path*/]*filename* | **image:**[*image_name*] | **running-config** | **startup-config**}

Syntax Description

ftp://*server*/*path*[/*filename*]	Specifies the FTP network server and optional file to copy.
disk0:[*path*/]*filename*	Specifies that the file destination is the disk0: directory of the current context and the filename. If you do not provide the optional path, the ACE copies the file to the root directory on the disk0: file system.
image: [*image_name*]	Specifies to copy a system software image to flash memory. Use the **boot system** command in configuration mode to specify the BOOT environment variable. The BOOT environment variable specifies a list of image files on various devices from which the ACE can boot at startup. The **image:** keyword is available only in the Admin context. The *image_name* argument is optional. If you do not enter a name, the ACE uses the source filename.
running-config	Specifies to replace the running-configuration file that currently resides on the ACE in RAM (volatile memory).
startup-config	Specifies to replace the startup-configuration file that currently resides on the ACE in flash memory (nonvolatile memory).

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the config-copy feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To copy a startup-configuration file from a remote FTP server to the ACE, enter:

```
host1/Admin# copy ftp://192.168.1.2/startup_config_Adminctx startup-config
```

Related Commands

show running-config
show startup-config

copy image:

To copy an ACE software system image from flash memory to a remote server using File Transfer Protocol (FTP), Secure File Transfer Protocol (SFTP), or Trivial File Transfer Protocol (TFTP), use the **copy image:** command.

copy image:*image_filename* {**ftp://***server*/*path*[/*filename*] |
sftp://[*username*@]*server*/*path*[/*filename*] | **tftp://***server*[**:***port*]/*path*[/*filename*]}

Syntax Description

image_filename	Name of the ACE system software image. Use the **dir image:** command or the **show version** command to view the software system images available in flash memory.
ftp://*server*/*path*[/*filename*]	Specifies the FTP network server and optional renamed image.
sftp://[*username*@]*server*/*path*[/*filename*]	Specifies the SFTP network server and optional renamed image.
tftp://*server*[**:***port*]/*path*[/*filename*]	Specifies the TFTP network server and optional renamed image.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the config-copy feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

When you select a destination file system using **ftp:**, **sftp:**, or **tftp:**, the ACE does the following:

- Prompts you for your username and password if the destination file system requires user authentication.
- Prompts you for the server information if you do not provide the information with the command.
- Copies the file to the root directory of the destination file system if you do not provide the path information.

Examples

```
host1/Admin# copy image:c4710ace-mz.A3_1_0.bin ftp://192.168.1.2
```

Related Commands

dir
show version

copy licenses

To create a backup license file for the ACE licenses in the .tar format and copy it to the disk0: file system, use the **copy licenses** command.

copy licenses disk0:[*path/*]*filename*.**tar**

Syntax Description

disk0:	Specifies that the backup license file is copied to the disk0: file system.
[*path/*]*filename*.**tar**	Specifies the destination filename for the backup licenses. The destination filename must have a .tar file extension. If you do not provide the optional path, the ACE copies the file to the root directory on the disk0: file system.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the config-copy feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To copy the installed software licenses to the disk0: file system, enter:

```
host1/Admin# copy licenses disk0:mylicenses.tar
```

Related Commands

show license
untar disk0:

copy running-config

To copy the contents of the running configuration file in RAM (volatile memory) to the startup configuration file in flash memory (nonvolatile memory) or a network server, use the **copy running-config** command.

copy running-config {**disk0:**[*path/*]*filename* | **startup-config** | **ftp://***server*/*path*[*/filename*] | **sftp://**[*username*@]*server*/*path*[*/filename*] | **tftp://***server*[**:***port*]/*path*[*/filename*]}

Syntax Description

disk0:[*path/*]*filename*	Specifies that the running configuration is copied to a file on the disk0: file system. If you do not provide the optional path, the ACE copies the file to the root directory on the disk0: file system.
startup-config	Copies the running configuration file to the startup configuration file.
ftp://*server*/*path*[*/filename*]	Specifies the File Transfer Protocol (FTP) network server and optional renamed file.
sftp://[*username*@]*server*/*path*[*/filename*]	Specifies the Secure File Transfer Protocol (SFTP) network server and optional renamed file.
tftp://*server*[**:***port*]/*path*[*/filename*]	Specifies the Trivial File Transfer Protocol (TFTP) network server and optional renamed file.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the config-copy feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

When you select a destination file system using **ftp:**, **sftp:**, or **tftp:**, the ACE does the following:

- Prompts you for your username and password if the destination file system requires user authentication.
- Prompts you for the server information if you do not provide the information with the command.
- Copies the file to the root directory of the destination file system if you do not provide the path information.

To copy the running configuration to the startup configuration, you can also use the **write memory** command.

Examples

To save the running-configuration file to the startup-configuration file in flash memory on the ACE, enter:

```
host1/Admin# copy running-config startup-config
```

Related Commands

show running-config
show startup-config
write

copy startup-config

To merge the contents of the startup configuration file into the running configuration file or copy the startup configuration file to a network server, use the **copy startup-config** command.

copy startup-config {**disk0:**[*path/*]*filename* | **running-config** | **ftp://***server/path*[*/filename*] | **sftp://**[*username*@]*server/path*[*/filename*] | **tftp://***server*[**:***port*]*/path*[*/filename*]}

Syntax Description

disk0:[*path/*]*filename*	Specifies that the startup configuration is copied to a file on the disk0: file system. If you do not provide the optional path, the ACE copies the file to the root directory on the disk0: file system.
running-config	Merges contents of the startup configuration file into the running configuration file.
ftp://*server/pat*[*/filename*]	Specifies the File Transfer Protocol (FTP) network server and optional renamed file.
sftp://[*username*@]*server/path*[*/filename*]	Specifies the Secure File Transfer Protocol (SFTP) network server and optional renamed file.
tftp://*server*[**:***port*]*/path*[*/filename*]	Specifies the Trivial File Transfer Protocol (TFTP) network server and optional renamed file.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the config-copy feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

When you select a destination file system using **ftp:**, **sftp:**, or **tftp:**, the ACE does the following:

- Prompts you for your username and password if the destination file system requires user authentication.
- Prompts you for the server information if you do not provide the information with the command.
- Copies the file to the root directory of the destination file system if you do not provide the path information.

Examples

To merge the contents of the startup-configuration file into the running-configuration file in flash memory, enter:

```
host1/Admin# copy startup-config running-config
```

Related Commands

show startup-config

copy sftp:

To copy a file, software image, running-configuration file, or startup-configuration file from a remote Secure File Transfer Protocol (SFTP) server to a location on the ACE, use the **copy sftp:** command.

copy sftp://[*username*@]*server*/*path*[/*filename*] {**disk0:**[*path*/]*filename*| **image:**[*image_name*] | **running-config** | **startup-config**}

Syntax Description

sftp://[*username*@]*server*/*path*[/*filename*]	Specifies the SFTP network server and optional renamed file.
disk0:[*path*/]*filename*	Specifies that the file destination is the disk0: directory of the current context and the filename. If you do not provide the optional path, the ACE copies the file to the root directory on the disk0: file system.
image: [*image_name*]	Specifies to copy a system software image to flash memory. Use the **boot system** command in configuration mode to specify the BOOT environment variable. The BOOT environment variable specifies a list of image files on various devices from which the ACE can boot at startup. The **image:** keyword is available only in the Admin context. The *image_name* argument is optional. If you do not enter a name, the ACE uses the source filename.
running-config	Specifies to replace the running-configuration file that currently resides on the ACE in RAM (volatile memory).
startup-config	Specifies to replace the startup-configuration file that currently resides on the ACE in flash memory (nonvolatile memory).

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the config-copy feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To copy a startup-configuration file from a remote SFTP server to the ACE, enter:

```
host1/Admin# copy sftp://192.168.1.2/startup_config_Adminctx startup-config
```

Related Commands

show running-config
show startup-config

copy tftp:

To copy a file, software image, running-configuration file, or startup-configuration file from a remote Trivial File Transfer Protocol (TFTP) server to a location on the ACE, use the **copy tftp:** command.

copy tftp://*server*[**:***port*]**/***path*[**/***filename*] {**disk0:**[*path/*]*filename* | **image:**[*image_name*] | **running-config** | **startup-config**}

Syntax Description

tftp://*server*[**:***port*]**/***path*[**/***filename*]	Specifies the TFTP network server and optional renamed file.
disk0:[*path/*]*filename*	Specifies that the file destination is the disk0: directory of the current context and the filename. If you do not provide the optional path, the ACE copies the file to the root directory on the disk0: file system.
image: [*image_name*]	Specifies to copy a system software image to flash memory. Use the **boot system** command in configuration mode to specify the BOOT environment variable. The BOOT environment variable specifies a list of image files on various devices from which the ACE can boot at startup. The **image:** keyword is available only in the Admin context. The *image_name* argument is optional. If you do not enter a name, the ACE uses the source filename.
running-config	Specifies to replace the running-configuration file that currently resides on the ACE in RAM (volatile memory).
startup-config	Specifies to replace the startup-configuration file that currently resides on the ACE in flash memory (nonvolatile memory).

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the config-copy feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To copy a startup-configuration file from a remote TFTP server to the ACE, enter:

```
host1/Admin# copy tftp://192.168.1.2/startup_config_Adminctx startup-config
```

Related Commands

show running-config
show startup-config

crypto crlparams

To configure signature verification on a Certificate Revocation List (CRL) to determine that it is from a trusted certificate authority, use the **crypto crlparams** command.

crypto crlparams *crl_name* **cacert** *ca_cert_filename*

no crypto crlparams *crl_name*

Syntax Description

crl_name
ca_cert_filename

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A3(2.2)	This command was introduced.

Usage Guidelines

This command requires the SSL feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To configure signature verification on a CRL, enter:

```
host1/Admin(config)# crypto crlparams CRL1 cacert MYCERT.PEM
```

To remove signature verification from a CRL, enter:

```
host1/Admin(config)# no crypto crlparams CRL1
```

Related Commands

(config-ssl-proxy) crl

crypto delete

To delete a certificate and key pair file from the ACE that is no longer valid, use the **crypto delete** command.

crypto delete {*filename* | **all**}

Syntax Description

filename	Name of a specific certificate or key pair file to delete. Enter an unquoted text string with no spaces and a maximum of 40 alphanumeric characters.
all	Deletes all of the certificate and key pair files.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the SSL feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To view the list of the certificate and key pair files stored on the ACE for the current context, use the **show crypto files** command.

Examples

To delete the key pair file MYRSAKEY.PEM, enter:

```
host1/Admin# crypto delete MYRSAKEY.PEM
```

Related Commands

crypto export
crypto import
show crypto

crypto export

To export a copy of a certificate or key pair file from the ACE to a remote server or the terminal screen, use the **crypto export** command.

crypto export *local_filename* {**ftp** | **sftp** | **tftp** | **terminal**} *ip_addr username remote_filename*

Syntax Description

local_filename	Name of the file stored on the ACE to export. Enter an unquoted text string with no spaces and a maximum of 40 alphanumeric characters.
ftp	Specifies the File Transfer Protocol (FTP) file transfer process.
sftp	Specifies the Secure File Transfer Protocol (SFTP) file transfer process.
tftp	Specifies the Trivial File Transfer Protocol (TFTP) file transfer process.
terminal	Displays the file content on the terminal for copy and paste purposes. Use the **terminal** keyword when you need to cut and paste certificate or private key information from the console. You can only use the terminal method to display PEM files, which are in ASCII format.
ip_addr	IP address or name of the remote server. Enter an IP address in dotted-decimal notation (for example, 172.27.16.10).
username	Username required to access the remote server. The ACE prompts you for your password when you enter the command.
remote_filename	Name to save the file to on the remote server. Enter an unquoted text string with no spaces and a maximum of 40 alphanumeric characters.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the SSL feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You cannot export a certificate or key pair file that you marked as nonexportable when you imported the file to the ACE.

The remote server variables listed after the **terminal** keyword in the "Syntax Description" are used by the ACE only when you select a transport type of **ftp**, **sftp**, or **tftp** (the variables are not used for **terminal**). We recommend using SFTP as it provides the most security.

To view the list of the certificate and key pair files stored on the ACE for the current context, use the **show crypto files** command.

Examples

To use SFTP to export the key file MYKEY.PEM from the ACE to a remote SFTP server, enter:

```
host1/Admin# crypto export MYKEY.PEM sftp 192.168.1.2 JOESMITH /USR/KEYS/MYKEY.PEM
User password: ****
Writing remote file /usr/keys/mykey.pem
host1/Admin#
```

Related Commands

crypto delete
crypto import
show crypto

crypto generate csr

To generate a Certificate Signing Request (CSR) file, use the **crypto generate csr** command.

crypto generate csr *csr_params key_filename*

Syntax Description

csr_params	CSR parameters file that contains the distinguished name attributes. The ACE applies the distinguished name attributes contained in the CSR parameters file to the CSR. To create a CSR parameters file, use the **(config) crypto csr-params** command in the configuration mode.
key_filename	RSA key pair filename that contains the key on which the CSR is built. Enter an unquoted text string with no spaces and a maximum of 40 alphanumeric characters. It is the public key that the ACE embeds in the CSR. Ensure that the RSA key pair file is loaded on the ACE for the current context. If the appropriate key pair does not exist, the ACE logs an error message.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Secure Sockets Layer (SSL) feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The **crypto generate csr** command generates the CSR in PKCS10 encoded in PEM format and outputs it to the screen. Most major certificate authorities have web-based applications that require you to cut and paste the certificate request to the screen. If necessary, you can also cut and paste the CSR to a file.

Note The ACE does not save a copy of the CSR locally.

After submitting your CSR to the CA, you will receive your signed certificate in one to seven business days. When you receive your certificate, use the **crypto import** command to import the certificate to the ACE.

Examples

To generate a CSR that is based on the CSR parameter set CSR_PARAMS_1 and the RSA key pair in the file MYRSAKEY_1.PEM, enter:

```
host1/Admin# crypto generate csr CSR_PARAMS_1 MYRSAKEY_1.PEM
```

Related Commands

crypto import
(config) crypto csr-params

crypto generate key

To generate an RSA key pair file, use the **crypto generate key** command.

crypto generate key [**non-exportable**] *bitsize filename*

Syntax Description

non-exportable	(Optional) Marks the key pair file as nonexportable, which means that you cannot export the key pair file from the ACE.
bitsize	Key pair security strength. The number of bits in the key pair file defines the size of the RSA key pair used to secure web transactions. Longer keys produce a more secure implementation by increasing the strength of the RSA security policy. Available entries (in bits) are as follows: • 512 (least security) • 768 (normal security) • 1024 (high security, level 1) • 1536 (high security, level 2) • 2048 (high security, level 3
filename	Name that you assign to the generated RSA key pair file. Enter an unquoted text string with no spaces and a maximum of 40 alphanumeric characters.The key pair filename is used only for identification purposes by the ACE.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the SSL feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To generate the RSA key pair file MYRSAKEYS.PEM with a bit size of 1536, enter:

```
host1/Admin# crypto generate key 1536 MYRSAKEYS.PEM
```

Related Commands

crypto delete
crypto export
crypto generate csr
crypto import
crypto verify
show crypto

crypto import

To import certificate or key pair files to the ACE or terminal screen from a remote server, use the **crypto import** command.

crypto import [**non-exportable**] {{**ftp** | **sftp**} [**passphrase** *passphrase*] *ip_addr username remote_filename local_filename*} | {**tftp** [**passphrase** *passphrase*] *ip_addr remote_filename local_filename*} | **terminal** *local_filename* [**passphrase** *passphrase*]

Syntax Description

non-exportable	(Optional) Specifies that the ACE marks the imported file as nonexportable, which means that you cannot export the file from the ACE.
ftp	Specifies the File Transfer Protocol (FTP) file transfer process.
sftp	Specifies the Secure File Transfer Protocol (SFTP) file transfer process.
passphrase *passphrase*	(Optional) Indicates that the file was created with a passphrase, which you must submit with the file transfer request in order to use the file. The passphrase pertains only to encrypted PEM files and PKCS files.
ip_addr	IP address or name of the remote server. Enter an IP address in dotted-decimal notation (for example, 172.27.16.10).
username	Username required to access the remote server. The ACE prompts you for your password when you enter the command.
remote_filename	Name of the certificate or key pair file that resides on the remote server to import. Enter an unquoted text string with no spaces and a maximum of 40 alphanumeric characters.
local_filename	Name to save the file to when imported to the ACE. Enter an unquoted text string with no spaces and a maximum of 40 alphanumeric characters.
tftp	Specifies the Trivial File Transfer Protocol (TFTP) file transfer process.
terminal	Allows you to import a file using cut and paste by pasting the certificate and key pair information to the terminal display. You can only use the terminal method to display PEM files, which are in ASCII format.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Secure Sockets Layer (SSL) feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Because a device uses its certificate and corresponding public key together to prove its identity during the SSL handshake, be sure to import both corresponding file types: the certificate file and its corresponding key pair file.

The remote server variables listed after the *passphrase* variable in the Syntax Description table are only used by the ACE when you select a transport type of **ftp**, **sftp**, or **tftp** (the variables are not used for **terminal**). If you select one of these transport types and do not define the remote server variables, the ACE prompts you for the variable information. We recommend using SFTP because it provides the most security.

The ACE supports the importation of PEM-encoded SSL certificates and keys with a maximum line width of 130 characters using the terminal. If an SSL certificate or key is not wrapped or it exceeds 130 characters per line, use a text editor such as the visual (vi) editor or Notepad to manually wrap the certificate or key to less than 130 characters per line. Alternatively, you can import the certificate or key by using SFTP, FTP, or TFTP with no regard to line width. Of these methods, we recommend SFTP because it is secure.

If you attempt to import a file that has the same filename of an existing local file, the ACE appliance does not overwrite the existing file. Before importing the updated file, you must either delete the local file or rename the imported file.

The ACE appliance supports 4096 certificates and 4096 keys.

To view the list of the certificate and key pair files stored on the ACE for the current context, use the **show crypto files** command.

Examples

To import the RSA key file MYRSAKEY.PEM from an SFTP server, enter:

```
host1/Admin# crypto import non-exportable sftp 1.1.1.1 JOESMITH /USR/KEYS/MYRSAKEY.PEM
MYKEY.PEM
Password: ********
Passive mode on.
Hash mark printing on (1024 bytes/hash mark).
#
Successfully imported file from remote server.
host1/Admin#
```

This example shows how to use the **terminal** keyword to allow pasting of the certificate information to the file MYCERT.PEM:

```
host1/Admin# crypto import terminal MYCERT.PEM
Enter PEM formatted data ending with a blank line or "quit" on a line by itself
--------BEGIN CERTIFICATE-----------------------
MIIC1DCCAj2gAwIBAgIDCCQAMA0GCSqGSIb3DQEBAgUAMIHEMQswCQYDVQQGEwJa
QTEVMBMGA1UECBMMV2VzdGVybiBDYXBlMRIwEAYDVQQHEwlDYXBlIFRvd24xHTAb
```

```
BgNVBAoTFFRoYXd0ZSBDb25zdWx0aW5nIGNjMSgwJgYDVQQLEx9DZXJ0aWZpY2F0
aW9uIFNlcnZpY2VzIERpdmlzaW9uMRkwFwYDVQQDExBUaGF3dGUgU2VydmVyIENB
MSYwJAYJKoZIhvcNAQkBFhdzZXJ2ZXItY2VydHNAdGhhd3RlLmNvbTAeFw0wMTA3
-----------END CERTIFICATE-----------------------
QUIT
host1/Admin#
```

Related Commands

crypto delete
crypto export
crypto verify
show crypto

crypto verify

To compare the public key in a certificate with the public key in a key pair file, and to verify that they are identical, use the **crypto verify** command.

crypto verify *key_filename cert_filename*

Syntax Description

key_filename	Name of the key pair file (stored on the ACE) that the ACE uses to verify against the specified certificate. Enter an unquoted text string with no spaces and a maximum of 40 alphanumeric characters.
cert_filename	Name of the certificate file (stored on the ACE) that the ACE uses to verify against the specified key pair. Enter an unquoted text string with no spaces and a maximum of 40 alphanumeric characters.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Secure Sockets Layer (SSL) feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

If the public key in the certificate does not match the public key in the key pair file, the ACE logs an error message.

To view the list of the certificate and key pair files stored on the ACE for the current context, use the **show crypto files** command.

Examples

To verify that the public keys in the Admin context files MYRSAKEY.PEM and MYCERT.PEM match, enter:

```
host1/Admin# crypto verify MYRSAKEY.PEM MYCERT.PEM
keypair in myrsakey.pem matches certificate in mycert.pem
```

This example shows what happens when the public keys do not match:

```
host1/Admin# crypto verify MYRSAKEY2.PEM MYCERT.PEM
Keypair in myrsakey2.pem does not match certificate in mycert.pem
host1/Admin#
```

Related Commands

crypto import
show crypto

debug

To enable the ACE debugging functions, use the **debug** command.

debug {**aaa** | **access-list** | **all** | **arpmgr** | **bpdu** | **buffer** | **cfg_cntlr** | **cfgmgr** | **fifo** | **fm** | **ha_dp_mgr** | **ha_mgr** | **hardware** | **hm** | **ifmgr** | **ip** | **ipcp** | **ldap** | **license** | **logfile** | **nat-download** | **netio** | **ntp** | **optimize** | **pfmgr** | **pktcap** | **portmgr** | **radius** | **routemgr** | **security** | **sme** | **snmp** | **ssl** | **syslogd** | **system** | **tacacs+** | **tl** | **virtualization** | **vnet**}

Syntax Description

aaa	Enables debugging for authentication, authorization, and accounting (AAA).
access-list	Enables access-list debugging.
all	Enables all debugging functions.
arpmgr	Enables Address Resolution Protocol (ARP) manager debugging.
bpdu	Enables bridge protocol data unit (BPDU) debugging.
buffer	Configures debugging of CP buffer manager.
cfg_cntlr	Enables configuration controller debugging.
cfgmgr	Enables configuration manager debugging.
fifo	Configures debugging of the packet first in, first out (FIFO) driver.
fm	Enables ACE feature manager debugging.
ha_dp_mgr	Enables HA-DP debugging.
ha_mgr	Enables HA debugging.
hardware	Debugs hardware kernel loadable module parameters.
hm	Enables HM debugging.
ifmgr	Enables interface manager debugging.
ip	Enables IP service debugging.
ipcp	Enables interprocess control protocol debugging.
ldap	Configures debugging for Lightweight Directory Access Protocol (LDAP).
license	Enables the debugging of licensing.
logfile	Directs the debug output to a log file.
nat-download	Enables Network Address Translation (NAT) download debugging.
netio	Enables the debugging of the CP network I/O.
ntp	Debugs the Network Time Protocol (NTP) module.
optimize	Sets the log level options.
pfmgr	Enables the debugging of the platform manager.
pktcap	Enables packet capture debugging.
portmgr	Debugs the port manager.
radius	Configures debugging for the Remote Authentication Dial-In User Service (RADIUS) daemon.
routemgr	Enables route manager debugging.
ipcp	Enables the debugging of the kernel IPCP component.
security	Enables the debugging for security and accounting.

sme	Enables the debugging for the System Manager Extension.
snmp	Configures Simple Network Management Protocol (SNMP) server debugging.
ssl	Enables ACE SSL manager debugging.
syslogd	Enables syslogd debugging.
system	Enables debugging of the system components.
tacacs+	Configures debugging for Terminal Access Controller Access Control System Plus (TACACS+).
tl	Configures debugging of TL driver.
virtualization	Enables virtualization debugging.
vnet	Configures debugging of virtual net-device driver.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised.

Usage Guidelines

This command is available to roles that allow debugging and to network monitor or technician users. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The ACE **debug** commands are intended for use by trained Cisco personnel only. Entering these commands may cause unexpected results. Do not attempt to use these commands without guidance from Cisco support personnel.

Examples

To enable access-list debugging, enter:

```
host1/Admin# debug access-list
```

Related Commands

clear debug-logfile
show debug

delete

To delete a specified file in an ACE file system, use the **delete** command.

delete {**core:***filename* | **disk0:**[*path/*\]*filename* | **image:***filename* | **volatile:***filename*}

Syntax Description

core:*filename*	Deletes the specified file from the core: file system.
disk0:[*path/*\]*filename*	Deletes the specified file from the disk0: file system. If you do not specify the optional path, the ACE looks for the file in the root directory of the disk0: file system.
image:*filename*	Deletes the specified file from the image: file system.
volatile:*filename*	Deletes the specified file from the volatile: file system.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

If you do not specify a filename with the file system keyword, the ACE prompts you for a filename.

To display the list of files that reside in a file system, use the **dir** command.

Examples

To delete the file 0x401_VSH_LOG.25256.TAR.GZ from the core: file system, enter:

```
host1/Admin# delete core:0x401_VSH_LOG.25256.TAR.GZ
```

Related Commands

dir

dir

To display the contents of a specified ACE file system, use the **dir** command.

dir {**core:** | **disk0:**[*path/*][*filename*] | **image:**[*filename*] | **probe:**[*filename*] | **volatile:**[*filename*]}

Syntax Description

core:	Displays the contents of the core: file system.
disk0:[*path/*]	Displays the contents of the disk0: file system. Specify the optional path to display the contents of a specific directory on the disk0: file system.
image:	Displays the contents of the image: file system.
probe:	Displays the contents of the probe: file system. This directory contains the Cisco-supplied scripts. For more information about these scripts, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.
volatile:	Displays the contents of the volatile: file system.
filename	(Optional) Specified file to display. Displays information, such as the file size and the date that it was created. You can use wildcards in the filename. A wildcard character (*) matches all patterns. Strings after a wildcard are ignored.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	The **probe:** option was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To delete a file from a file system, use the **delete** command.

To delete all core dumps, use the **clear cores** command.

Examples

To display the contents of the image: file system, enter:

```
switch/Admin# dir image:

176876624 Aug 08 2008 14:15:31 c4710ace-mz.A3_1_0.bin
176876624 Jun 9 14:15:31 2008 c4710ace-mz.A1_8_0A.bin

          Usage for image: filesystem
                 896978944 bytes total used
                  11849728 bytes free
                 908828672 bytes total
```

Related Commands

clear cores
delete
show file

exit

To exit out of Exec mode and log out the CLI session, use the **exit** command.

exit

Syntax Description

This command has no keywords or arguments.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To log out of an active CLI session, enter:

```
host1/Admin# exit
```

Related Commands

This command has no related commands.

format flash:

To erase all data stored on the Flash memory and reformat it with the third extended filesystem (ext3) as the base file system, use the **format flash:** command. All user-defined configuration information is erased and the ACE returns to the factory-default settings.

format flash:

Syntax Description

This command has no keywords or arguments.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The ACE performs the following verification sequence prior to reformatting Flash memory:

- If the system image (the current loaded image) is present in the GNU GRand Unified Bootloader (GRUB) boot loader, the ACE automatically performs a backup of that image and then performs the reformat of Flash memory.
- If the system image is not present in the Grub boot loader, the ACE prompts you for the location of an available image to backup prior to reformatting the Flash memory.
- If you choose not to backup an available image file, the ACE searches for the ACE-APPLIANCE-RECOVERY-IMAGE.bin image in the Grub partition of Flash memory. ACE-APPLIANCE-RECOVERY-IMAGE.bin is the recovery software image that the ACE uses if the disk partition in Flash memory is corrupted.
  - If ACE-APPLIANCE-RECOVERY-IMAGE.bin is present, the ACE continues with the Flash memory reformat. The CLI prompt changes to “switch(RECOVERY-IMAGE)/Admin#” as a means for you to copy the regular ACE software image.
  - If ACE-APPLIANCE-RECOVERY-IMAGE.bin is not present, the ACE stops the Flash memory reformat because there is no image to boot after format.

Before you reformat the Flash memory, you should save a copy of the following ACE operation and configuration attributes to a remote server:

- ACE software image (use the **copy image:** command)
- ACE license (use the **copy licenses** command)
- Startup configuration of each context (use the **copy startup-config** command)
- Running configuration of each context (use the **copy running-config** command)
- Core dump files of each context (use the **copy core:** command)

- Packet capture buffers of each context (use the **copy capture** command)
- Secure Sockets Layer (SSL) certificate and key pair files of each context (use the **crypto export** command)

After you reformat the Flash memory, perform the following actions:

- Copy the ACE software image to the image: file system using the **copy ftp:**, **copy tftp:**, or **copy sftp:** command
- Reinstall the ACE license using the **license** command
- Import the following configuration files into the associated context using the **copy disk0:** command:
  - Startup-configuration file
  - Running-configuration file
- Import the following SSL files into the associated context using the **crypto import** command:
  - SSL certificate files
  - SSL key pair files

Examples

For example, to erase all information in Flash memory and reformat it, enter:

```
host1/Admin# format flash:
Warning!! This will erase everything in the compact flash including startup configs for
all the contexts and reboot the system!!
Do you wish to proceed anyway? (yes/no)  [no] yes
```

If the ACE fails to extract a system image from the Grub bootloader, it prompts you to provide the location of an available system image to backup:

```
Failed to extract system image Information from Grub
backup specific imagefile? (yes/no)  [no] yes
Enter Image name: scimi-3.bin
Saving Image [scimi-3.bin]
Formatting the cf.....
Unmounting ext3 filesystems...
Unmounting FAT filesystems...
Unmounting done...

Unmounting compact flash filesystems...
format completed  successfully
Restoring Image backupimage/scimi-3.bin
kjournald starting.  Commit interval 5 seconds
REXT3 FS on hdb2, internal journal
EXT3-fs: mounted filesystem with ordered data mode.
starting graceful shutdown
switch/Admin# Unmounting ext3 filesystems...
Unmounting FAT filesystems...
Unmounting done...
```

Related Commands

copy capture
copy ftp:
copy tftp:
copy sftp:
crypto export
crypto import
dir
license

ft switchover

To purposely cause a failover to make a particular context active, use the **ft switchover** command.

ft switchover [**all** [**force**] | **force** | *group_id* [**force**]]

Syntax Description

all	(Optional) Causes a switchover of all FT groups configured in the ACE simultaneously.
force	(Optional) Causes a switchover of the Admin context if you enter the command in the Admin context and do not specify a group ID, or the specified FT group, while ignoring the state of the standby member. Use this option only when the fault-tolerant (FT) VLAN is down.
group_id	(Optional) Causes a switchover of the specified FT group. Enter the ID of an existing FT group as an integer from 1 to 255.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	Added the **all** keyword.

Usage Guidelines

This command requires the fault-tolerant feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

By using the **ft switchover** command, you direct the standby group member to statefully become the active member of the FT group, which forces a switchover.

You may need to force a switchover when you want to make a particular context the standby (for example, for maintenance or a software upgrade on the currently active context). If the standby group member can statefully become the active member of the FT group, a switchover occurs. To use this command, you must configure the **no preempt** command in FT group configuration mode.

The **ft switchover** command exhibits the following behavior, depending on whether you enter the command from the Admin context or a user context:

- Admin context—If you specify an FT group ID, then the FT group specified by the group ID switches over. If you do not specify a group ID, then the Admin context switches over.
- User context—Because you cannot specify an FT group ID in a user context, the context in which you enter the command switches over.

When you specify the **ft switchover** command, there may be brief periods of time when the configuration mode is enabled on the new active group member to allow the administrator to make configuration changes. However, these configuration changes are not synchronized with the standby group member and will exist only on the active group member. We recommend that you refrain from making any configuration changes after you enter the **ft switchover** command until the FT states stabilize to Active and Standby_hot. Once the FT group reaches the steady state of Active and Standby_hot, any configuration changes performed on the active group member will be incrementally synchronized to the standby group member, assuming that configuration synchronization is enabled.

Examples

To cause a switchover from the active appliance to the standby appliance of FT group1, enter:

```
host1/Admin# ft switchover 1
```

Related Commands

(config-ft-group) preempt

gunzip

To uncompress (unzip) LZ77 coded files residing in the disk0: file system (for example, zipped probe script files), use the **gunzip** command.

gunzip disk0:[*path/*]*filename***.gz**

Syntax Description

disk0:[*path/*]*filename***.gz**	Specifies the name of the compressed file on the disk0: file system. The filename must end with a .gz extension. If you do not specify the optional path, the ACE looks for the file in the root directory.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

This command is useful in uncompressing large files. The filename must end with a .gz extension for the file to be uncompressed using the **gunzip** command. The .gz extension indicates a file that is zipped by the gzip (GNU zip) compression utility.

To display a list of available zipped files on disk0:, use the **dir** command.

Examples To unzip a compressed series of probe script files from the file PROBE_SCRIPTS in the disk0: file system, enter:

```
host1/Admin# gunzip disk0:PROBE_SCRIPTS.gz
```

Related Commands **dir**

invoke context

To display the context running configuration information from the Admin context, use the **invoke context** command.

invoke context *context_name* **show running-config**

Syntax Description

context_name	Name of user-created context. This argument is case sensitive.

Command Modes Exec

Admin context

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples To display the running configuration for the C1 user context from the Admin context, enter:

```
host1/Admin# invoke context C1 show running-config
```

Related Commands This command has no related commands.

license

To install, update, or uninstall licenses on the ACE, use the **license** command.

license {**install disk0:**[*path*/]*filename* [*target_filename*] | **uninstall** *name* |
update disk0:[*path*/]*permanent_filename demo_filename*}

Syntax Description

install disk0:[*path/*]*filename*	Installs a demo or permanent license from the disk0: file system into flash memory on the ACE. The *filename* is the name of the license on the disk0: file system. If you do not specify the optional path, the ACE looks for the file in the root directory.
target_filename	(Optional) Target filename for the license file.
uninstall *name*	Uninstalls the specified license file. Enter the license name as an unquoted text string with no spaces.
update disk0:	Updates an installed demo license with a permanent license.
[*path/*]*permanent_filename*	Filename for the permanent license.
demo_filename	Filename for the demo license.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

After you receive a demo or permanent software license key in an e-mail from Cisco Systems, you must copy the license file to a network server and then use the **copy tftp** command in Exec mode to copy the file to the disk0: file system on the ACE.

To update an installed demo license with a permanent license, use the **license update** command. The demo license is valid for 60 days. To view the expiration of the demo license, use the **show license usage** command.

To back up license files, use the **copy licenses** command

Caution When you remove a demo or permanent virtual context license, the ACE removes all user contexts from the Admin running configuration. By removing the user contexts, their running and startup configurations are also removed from the ACE. Before removing any virtual context license, save the Admin running configuration and the user context running configurations to a remote server.

For more information about the types of ACE licenses available and how to manage the licenses on your ACE, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To install a new permanent license, enter:

```
host1/Admin# license install disk0:ACE-VIRT-020.LIC
```

To uninstall a license, enter:

```
host1/Admin# license uninstall ACE-VIRT-20.LIC
```

To update the demo license with a permanent license, enter:

```
host1/Admin# license update disk0:ACE-AP-VIRT-020.lic ACE-AP-VIRT-020-DEMO.lic
```

Related Commands

copy licenses
copy tftp:
show license

mkdir disk0:

To create a new directory in disk0:, use the **mkdir disk0:** command.

mkdir disk0:[*path/*]*directory_name*

Syntax Description

[*path/*]*directory_name*	Name that you assign to the new directory. Specify the optional path if you want to create a directory within an existing directory.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

If a directory with the same name already exists, the ACE does not create the new directory and the "Directory already exists" message appears.

Examples

To create a directory in disk0: called TEST_DIRECTORY, enter:

```
host1/Admin# mkdir disk0:TEST_DIRECTORY
```

Related Commands

dir
rmdir disk0:

move disk0:

To move a file between directories in the disk0: file system, use the **move disk0:** command.

move disk0:[*source_path/*]*filename* **disk0:**[*destination_path/*]*filename*

Syntax Description

disk0:	Indicates the disk0: file system of the current context.
source_path/	(Optional) Path of the source directory.
destination_path/	(Optional) Path of the destination directory.
filename	Name of the file to move in the disk0: file system.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

If a file with the same name already exists in the destination directory, that file is overwritten by the file that you move.

Examples

To move the file called SAMPLEFILE in the root directory of disk0: to the MYSTORAGE directory in disk0:, enter:

```
host1/Admin# move disk0:SAMPLEFILE disk0:MYSTORAGE/SAMPLEFILE
```

Related Commands

dir

ping

To verify the connectivity of a remote host or server by sending echo messages from the ACE, use the **ping** command.

ping [*target_ip* [**count** *count* | **size** *size* | **timeout** *time*]]

Syntax Description

target_ip	(Optional) IP address of the remote host to ping. Enter an IP address in dotted-decimal notation (for example, 172.27.16.10). If you do not specify the IP address of the remote host, the CLI prompts you for the information.
count *count*	(Optional) Repeat count. Enter the repeat count as an integer from 1 to 65000.
size *size*	(Optional) Datagram size. Enter the datagram size as an integer from 36 to 452.
timeout *time*	(Optional) Timeout in seconds. Enter the timeout value as an integer from 0 to 3600.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The **ping** command sends an echo request packet to an address from the current context on the ACE and then awaits a reply. The ping output can help you evaluate path-to-host reliability, delays over displaying the name of the current directory and the path, and whether the host can be reached or is functioning.

To terminate a ping session before it reaches its timeout value, press **Ctrl-C**.

Examples

To ping the FTP server with an IP address of 196.168.1.2 using the default ping session values, enter:

```
host1/Admin# ping 196.168.1.2
```

Related Commands

traceroute

reload

To reload the configuration on the ACE, use the **reload** command.

reload

Syntax Description

This command has no keywords or arguments.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The **reload** command reboots the ACE and performs a full power cycle of both the hardware and software. The reset process can take several minutes. Any open connections with the ACE are dropped after you enter the **reload** command.

Caution Configuration changes that are not written to flash memory are lost after a reload. Before rebooting, enter the **copy running-conf startup-config** command to save a copy of the running configuration to the startup configuration in flash memory. If you fail to save your running configuration changes, the ACE reverts to the last saved version of the startup configuration upon restart.

Examples

To execute a soft reboot, enter:

```
host1/Admin# reload
This command will reboot the system
Save configurations for all the contexts. Save? [yes/no]: [yes]
```

Related Commands

copy capture
show running-config
show startup-config

rmdir disk0:

To remove a directory from the disk0: file system, use the **rmdir disk0:** command.

rmdir disk0:*directory*

Syntax Description

directory	Name of the directory to remove.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To remove a directory from disk0:, the directory must be empty. To view the contents of a directory, use the **dir** command. To delete files from a directory, use the **delete** command.

Examples

To remove the directory TEST_DIRECTORY from disk0:, enter:

```
host1/Admin# rmdir disk0:TEST-DIRECTORY
```

Related Commands

delete
dir
mkdir disk0:

setup

To initiate a special setup script that guides you through the basic process of configuring an Ethernet port on the ACE as the management port to access the Device Manager GUI, use the **setup** command.

setup

Syntax Description

This command has no keywords or arguments.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The setup script is intended primarily as the means to guide you though a basic configuration of the ACE to quickly access the Device Manager. Use the **setup** command when the ACE boots without a startup-configuration file. This situation may occur when the ACE is new and the appliance was not configured upon initial startup. The setup script guides you through configuring a management VLAN on the ACE through one of its Gigabit Ethernet ports.

After you specify a gigabit Ethernet port, the port mode, and management VLAN, the setup script automatically applies the following default configuration:

- Management VLAN allocated to the specified Ethernet port.
- VLAN 1000 assigned as the management VLAN interface.
- GigabitEthernet port mode configured as VLAN access port.
- Extended IP access list that allows IP traffic originating from any other host addresses.
- Traffic classification (class map and policy map) created for management protocols HTTP, HTTPS, ICMP, SSH, Telnet, and XML-HTTPS. HTTPS is dedicated for connectivity with the Device Manager GUI.
- VLAN interface configured on the ACE and a policy map assigned to the VLAN interface.

The ACE provides a default answer in brackets [ ] for each question in the setup script. To accept a default configuration prompt, press **Enter**, and the ACE accepts the setting. To skip the remaining configuration prompts, press **Ctrl-C** any time during the configuration sequence.

When completed, the setup script prompts you to apply the configuration settings.

Examples

To run the setup script from the CLI, enter:

```
host1/Admin# setup
This script will perform the configuration necessary for a user to manage the ACE
Appliance using the ACE Device Manager.The management port is a designated Ethernet port
which has access to the same network as your management tools including the ACE Device
Manager. You will be prompted for the Port Number, IP Address, Netmask and Default Route
(optional). Enter 'ctrl-c' at any time to quit the script

Would you like to enter the basic configuration (yes/no): y

Enter the Ethernet port number to be used as the management port (1-4):? [1]: 3

Enter the management port IP Address (n.n.n.n): [192.168.1.10]: 192.168.1.10

Enter the management port Netmask(n.n.n.n): [255.255.255.0]: 255.255.255.2

Enter the default route next hop IP Address (n.n.n.n) or <enter> to skip this step:
172.16.2.1

Summary of entered values:

  Management Port: 3
  Ip address 192.168.1.10
  Netmask: 255.255.255.2
  Default Route: 172.16.2.1

Submit the configuration including security settings to the ACE Appliance?
(yes/no/details): [y]: d

Detailed summary of entered values:

interface gigabit/Ethernet 1/3
  switchport access vlan 1000
  no shut
access-list ALL extended permit ip any any class-map type management match-any
remote_access
  match protocol xml-https any
  match protocol dm-telnet any
  match protocol icmp any
  match protocol telnet any
  match protocol ssh any
  match protocol http any
  match protocol https any
  match protocol snmp any
policy-map type management first-match remote_mgmt_allow_policy
  class remote_access
    permit
interface vlan 1000
  ip address 192.168.1.10 255.255.255.0
  access-group input ALL
  service-policy input remote_mgmt_allow_policy
  no shutdown
ssh key rsa
ip route 0.0.0.0 0.0.0.0 172.16.2.1
Submit the configuration including security settings to the ACE Appliance?
(yes/no/details): [y]: y

Configuration successfully applied. You can now manage this ACE Appliance by entering the
url 'https://192.168.1.10' into a web browser to access the Device Manager GUI.
```

Related Commands

This command has no related commands.

show

To display ACE statistical and configuration information, use the **show** command.

show *keyword* [| {**begin** *pattern* | **count** | **end** | **exclude** *pattern* | **include** *pattern* | **next** | **prev**}] [**>** {*filename* | {**disk0:**| **volatile**}:[*path/*][*filename*] | **ftp://***server/path*[*/filename*] | **sftp://**[*username*@]*server/path*[*/filename*] | **tftp://***server*[**:***port*]*/path*[*/filename*]}]

Syntax Description

keyword	Keyword associated with the **show** command. See the **show** commands that follow.
|	(Optional) Enables an output modifier that filters the command output.
begin *pattern*	Begins with the line that matches the pattern that you specify.
count	Counts the number of lines in the output.
end *pattern*	Ends with the line that matches the pattern that you specify.
exclude *pattern*	Excludes the lines that match the pattern that you specify.
include *pattern*	Includes the lines that match the pattern that you specify.
next	Displays the lines next to the matching pattern that you specify.
prev	Displays the lines before the matching pattern that you specify.
>	(Optional) Enables an output modifier that redirects the command output to a file.
filename	Name of the file that the ACE saves the output to on the volatile: file system.
disk0:	Specifies that the destination is the disk0: file system on the ACE flash memory.
volatile:	Specifies that the destination is the volatile: file system on the ACE.
[*path/*][*filename*]	(Optional) Path and filename to the disk0: or volatile: file system. This path is optional because the ACE prompts you for this information if you omit it.
ftp://*server/path*[*/filename*]	Specifies the File Transfer Protocol (FTP) network server and optional filename.
sftp://[*username*@]*server/path* [*/filename*]	Specifies the Secure File Transfer Protocol (SFTP) network server and optional filename.
tftp://*server*[**:***port*]*/path*[*/filename*]	Specifies the Trivial File Transfer Protocol (TFTP) network server and optional filename.

Command Modes

Exec

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The features required in your user role to execute a specific **show** command are described in the "Usage Guidelines" section of the command. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Most commands have an associated **show** command. For example, the associated **show** command for the **interface** command in configuration mode is the **show interface** command. Use the associated **show** command to verify changes that you make to the running configuration.

The output of the **show** command may vary depending on the context that you enter the command from. For example, the **show running-config** command displays the running-configuration for the current context only.

To convert **show** command output from the ACE to XML for result monitoring by an NMS, use the **xml-show** command.

Examples

To display the current running configuration, enter:

```
host1/Admin# show running-config
```

Related Commands

xml-show

show aaa

To display AAA accounting and authentication configuration information for the current context, use the **show aaa** command.

show aaa {**accounting** | **authentication** [**login error-enable**] | **groups**} [|] [>]

Syntax Description

accounting	Displays accounting configuration information.
authentication	Displays authentication configuration information.
login error-enable	(Optional) Displays the status of the login error message configuration.
groups	Displays the configured server groups.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show aaa** command output, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

Examples

To display the accounting configuration information, enter:

```
host1/Admin# show aaa accounting
    default: local
```

Related Commands

show accounting log
(config) aaa accounting default
(config) aaa authentication login

show access-list

To display statistics associated with a specific access control list (ACL), use the **show access-list** command.

show access-list *name* [**detail**] [|] [>]

Syntax Description

name	Name of an existing ACL. Enter the name as an unquoted text string.
detail	Displays detailed information for the specified ACL.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised with the **detail** option.

Usage Guidelines

This command requires the access-list feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The ACL information that the ACE displays when you enter the **show access-list** command includes the ACL name, the number of elements in the ACL, the operating status of the ACL (ACTIVE or NOT ACTIVE), any configured remarks, the ACL entry, and the ACL hit count.

For information about the fields in the **show access-list** command output, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

Examples

To display statistical and configuration information for the ACL ACL1, enter:

```
host1/Admin# show access-list ACL1
```

Related Commands

clear access-list
show running-config
(config) access-list ethertype
(config) access-list extended
(config) access-list remark
(config) access-list resequence

show accounting log

To display AAA accounting log information, use the **show accounting log** command.

show accounting log [*size*] [|] [>]

Syntax Description

size	(Optional) Size (in bytes) of the local accounting file. Enter a value from 0 to 250000. The default is 250000 bytes.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show accounting log** command output, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

Examples

To display the contents of the accounting log file, enter:

```
host1/Admin# show accounting log
```

Related Commands

show aaa
(config) aaa accounting default

show acl-merge

To display statistics related to merged ACLs, use the **show acl-merge** command.

show acl-merge acls vlan *number* |**internal vlan 1 | 4095**} {**in | out**} [**summary**]} | {**match** {**acls** {**vlan** *number* |**internal vlan 1 | 4095**} {**in | out**} *ip_address1 ip_address2 protocol src_port dest_port*} | {**merged-list** {**acls** {**vlan** *number* |**internal vlan 1 | 4095**}{**in | out**} [**non-redundant | summary**]} [|] [**>**]

Syntax Description

acls	Displays various feature ACLs and their entries before the merge.
vlan *number*	Specifies the interface on which the ACL was applied.
internal vlan 1 | 4095	Displays the ACL merge information for internal VLAN 1 or 4095.
in | out	Specifies the direction in which the ACL was applied to network traffic: incoming or outgoing.
summary	(Optional) Displays summary information before or after the merge.
match	Displays the ACL entry that matches the specified tuple.
ip_address1	Source IP address. Enter an IP address in dotted-decimal notation (for example, 172.27.16.10).
ip_address2	Destination IP address. Enter an IP address in dotted-decimal notation (for example, 172.27.16.10).
protocol	Protocol specified in the ACL.
src_port	Source port specified in the ACL.
dest_port	Destination port specified in the ACL.
merged-list	(Optional) Displays the merged ACL.
non-redundant	(Optional) Displays only those ACL entries that have been downloaded to a network processor.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(2.3)	This command was revised to include the **internal vlan 1 | 4095** keywords.

Usage Guidelines

This command requires the acl-merge feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

This command is intended for use by trained Cisco personnel for troubleshooting purposes only.

The ACL merge list number (instance ID) is locally generated (not synchronized) on each ACE in a redundant configuration. The number assigned depends on the order in which the ACLs are applied to the VLANs. This number can be different on the two appliances. The ACL merged list could be different on the two appliances depending on when redundancy is enabled.

Examples

To display the ACL merge information for VLAN 401, enter:

```
host1/Admin# show acl-merge acls vlan 401 in summary
```

Related Commands

This command has no related commands.

show action-list

To display information about action list configuration, use the **show action-list** command in Exec mode. The **show action-list** command output displays all optimization action list configurations and default values.

show action-list *list_name* [|] [>]

Syntax Description

list_name	Identifier of an existing action list as an unquoted text string with a maximum of 64 alphanumeric characters.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(2.3)	The Description field has been added to the **show action-list** command output. This field displays the previously entered summary about the specific parameter map.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show action-list** command output, see the *Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide*.

Examples

To display configuration information for the ACT_LIST1 action list, enter:

```
host1/Admin# show action-list ACT_LIST1
```

Related Commands

show running-config
(config) action-list type modify http
(config) action-list type optimization http

show arp

To display the current active IP address-to-MAC address mapping in the Address Resolution Protocol (ARP) table, statistics, or inspection or timeout configuration, use the **show arp** command.

show arp [**inspection** | **internal event-history dbg** | **statistics** [**vlan** *vlan_number*] | **timeout**] [|] [>]

Syntax Description

inspection	(Optional) Displays the ARP inspection configuration.
internal event-history dbg	(Optional) Displays the ARP internal event history. The ACE **debug** commands are intended for use by trained Cisco personnel only. Do not attempt to use these commands without guidance from Cisco support personnel.
statistics	(Optional) Displays the ARP statistics for all VLAN interfaces.
vlan *vlan_number*	(Optional) Displays the statistics for the specified VLAN number.
timeout	(Optional) Displays the ARP timeout values.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the routing feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The **show arp** command without options displays the active IP address-to-MAC address mapping in the ARP table.

For information about the fields in the **show arp** command output, see the *Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*.

Examples

To display the current active IP address-to-MAC address mapping in the ARP table, enter:

```
host1/Admin# show arp
```

Related Commands

clear arp
(config) action-list type modify http
(config) action-list type optimization http
(config) arp

show banner motd

To display the configured banner message of the day, use the **show banner motd** command.

show banner motd [|] [>]

Syntax Description

|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To configure the banner message, use the **banner** command in the configuration mode.

For information about the fields in the **show banner motd** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display the message of the day, enter:

```
host1/Admin# show banner motd
```

Related Commands

(config) banner

show bootvar

To display the current BOOT environment variable and configuration register setting, use the **show bootvar** command. This command is available only in the Admin context.

show bootvar [|] [>]

Syntax Description

|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To set the BOOT environment variable, use the **boot system image:** command in the configuration mode.

For information about the fields in the **show bootvar** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display the current BOOT environment variable and configuration register setting, enter:

```
host1/Admin# show bootvar
```

```
BOOT variable = "disk0:c4710ace-mz.A3_1_0.bin"
Configuration register is 0x1
```

Related Commands This command has no related commands.

show buffer

To display the buffer manager module messages, use the **show buffer** command.

show buffer {**events-history** | **stats** | **usage**} [|] [>]

Syntax Description

events-history	Displays a historic log of the most recent messages generated by the buffer manager event history.
stats	Displays detailed counters for various buffer manager event occurrences.
usage	Displays the number of buffers currently being held (allocated but not freed) by each buffer module. The **usage** keyword also shows an estimate of the number of times a particular buffer module has freed the same buffer more than once (this condition indicates a software error).
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

This command is intended for use by trained Cisco personnel for troubleshooting purposes only.

Examples

To display the control plane buffer event history, enter:

```
host1/Admin# show buffer events-history
1) Event:E_DEBUG, length:72, at 477729 usecs after Sat Jan 1 00:01:29 2000
[102] headers=0xd2369000, ctrl_blocks=0xd280a040, data_blocks=0xd5403aa0
2) Event:E_DEBUG, length:50, at 477707 usecs after Sat Jan 1 00:01:29 2000
[102] total blocks=151682 (ctrl=75841, data=75841)
```

Related Commands

clear buffer stats

show capture

To display the packet information that the ACE traces as part of the packet capture function, use the **show capture** command.

show capture *buffer_name* [**detail** [**connid** *connection_id* | **range** *packet_start packet_end*] | **status**] [|] [>]

Syntax Description

buffer_name	Name of the packet capture buffer. Specify an unquoted text string with no spaces from 1 to 80 alphanumeric characters.
detail	(Optional) Displays additional protocol information for each packet.
connid *connection_id*	(Optional) Displays protocol information for a specified connection identifier.
range *packet_start packet_end*	(Optional) Displays protocol information for a range of captured packets.
status	(Optional) Displays capture status information for each packet.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For all types of received packets, the console display is in tcpdump format.

To copy the capture buffer information as a file in flash memory, use the **copy capture** command.

For information about the fields in the **show capture** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display the captured packet information contained in packet capture buffer CAPTURE1, enter:

```
switch/Admin# show capture CAPTURE1
```

Related Commands copy capture

show checkpoint

To display information relating to the configured checkpoints, use the **show checkpoint** command.

show checkpoint {**all** | **detail** *name*} [|] [>]

Syntax Description

all	Displays a list of all existing checkpoints. The show output includes checkpoint time stamps.
detail *name*	Displays the running configuration of the specified checkpoint.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show checkpoint** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display the running configuration for the checkpoint MYCHECKPOINT, enter:

```
host1/Admin# show checkpoint detail MYCHECKPOINT
```

Related Commands checkpoint

show clock

To display the current date and time settings of the system clock, use the **show clock** command.

show clock [|] [>]

Syntax Description

|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To configure the system clock setting, use the **clock** command in the configuration mode.

For information about the fields in the **show clock** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display the current clock settings, enter:

```
host1/Admin# show clock
Fri Feb 24 20:08:14 UTC 2006
```

Related Commands

(config) clock summer-time
(config) clock timezone

show conn

To display the connection statistics, use the **show conn** command.

show conn {**address** *ip_address1* [*ip_address2*] **netmask** *mask* [**detail**]} | **count** | **detail** | {**port** *number1* [*number2*] [**detail**]} | {**protocol** {**tcp** | **udp**} [**detail**]} | {**rserver** *rs_name* [*port_number*] [**serverfarm** *sfarm_name1*] [**detail**]} | {**serverfarm** *sfarm_name2* [**detail**]} [|] [>]

Syntax Description

address *ip_address1* [*ip_address2*]	Displays connection statistics for a single source or destination IP address or, optionally, for a range of source or destination IP addresses. To specify a range of IP addresses, enter an IP address for the lower limit of the range and a second IP address for the upper limit of the range. Enter one or two IP addresses in dotted-decimal notation (for example, 192.168.12.15).
netmask *mask*	Specifies the network mask for the IP address or range of IP addresses that you specify. Enter a network mask in dotted-decimal notation (for example, 255.255.255.0).
count	Displays the total current connections to the ACE. **Note** The total current connections is the number of connection objects. There are two connection objects for each flow and complete connection.
detail	Displays detailed connection information. **Note** The total current connections is the number of connection objects. There are two connection objects for each flow and complete connection.
port *number1* [*number2*]	Displays connection statistics for a single source or destination port or optionally, for a range of source or destination ports.
protocol {**tcp** | **udp**}	Displays connection statistics for TCP or UDP.
rserver *rs_name*	Displays connection statistics for the specified real server.
port_number	(Optional) Port number associated with the specified real server. Enter an integer from 1 to 65535.
serverfarm *sfarm_name1*	Displays connection statistics for the specified real server associated with this server farm.
serverfarm *sfarm_name2*	Displays connection statistics for the real servers associated with the specified server farm.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(2.2)	This **detail** option was added for a specified address, port, protocol, real server, or server farm.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show conn** command output, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

Examples

To display connection statistics for a range of IP addresses, enter:

```
host1/Admin# show conn address 192.168.12.15 192.168.12.35 netmask 255.255.255.0
```

Related Commands

clear conn

show context

To display the context configuration information, use the **show context** command.

show context [*context_name* | **Admin**] [|] [>]

Syntax Description

context_name	(Optional) Name of user-created context. The ACE displays just the specified context configuration information. The *context_name* argument is case sensitive. and is visible only from the admin context.
Admin	(Optional) Displays just the admin context configuration information. This keyword is visible only from the admin context.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The ACE displays different information for this command depending on the context that you are in when executing the command:

- Admin context—When you are in the Admin context and use the **show context** command without specifying a context, the ACE displays the configuration information for the admin context and all user-created contexts.
- user-created context—When you are in a user-created context and enter the **show context** command, the ACE displays only the configuration information of the current context.

For information about the fields in the **show context** command output, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To display the Admin context and all user-context configuration information, enter:

```
host1/Admin# show context
```

To display the configuration information for the user context CTX1, enter:

```
host1/Ctx1# show context
```

Related Commands

changeto
(config) context

show copyright

To display the software copyright information for the ACE, use the **show copyright** command.

show copyright [|] [>]

Syntax Description

|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show copyright** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples To display the ACE software copyright information, enter:

```
host1/Admin# show copyright
```

Related Commands This command has no related commands.

show crypto

To display the summary and detailed reports on files containing Secure Sockets Layer (SSL) certificates, key pairs, chain and authentication groups, and statistics, use the **show crypto** command.

show crypto {**authgroup** {*group_name*| **all**} | **cdp-errors** | **certificate** {*filename* | **all**} | **chaingroup** {*filename* | **all**} | {**crl** {*filename* [**detail**]| **all** | **best-effort**} | **csr-params** {*filename* | **all**} | **files** | **key** {*filename* | **all**} | **session**}} [|] [**>**]

Syntax Description

authgroup	Specifies the authentication group file type.
group_name	Name of the specific authentication group file.
all	Displays the summary report that lists all the files of the specified file type or certificates for each authentication group, or certificate revocation lists (CRLs) in the context.
cdp-errors	Displays the statistics for discrepancies in CRL Distribution Points (CDPs) for the certificates on the ACE; not context specific. A CDP indicates the location of the CRL in the form of a URL. CDP parsing in the certificate occurs only when best effort CRL is in use. The statistics include incomplete, malformed and missing information, and unrecognized transports.
certificate	Specifies the certificate file type.
filename	Name of a specific file. The ACE displays the detailed report for the specified file. Enter an unquoted text string with no spaces and a maximum of 40 alphanumeric characters.
chaingroup	Specifies the chaingroup file type.
crl	Specifies the certificate revocation list configured in the context.
detail	(Optional) Displays detailed statistics for the downloading of the CRL including failure counters.
best-effort	Displays summarized information for all best-effort CRLs in ACE (a maximum of 16 CRLs).
csr-params	Specifies the Certificate Signing Request (CSR) parameter set.

files	Displays the summary report listing all of the crypto files loaded on the ACE, including certificate, chaingroup, and key pair files. The summary report also shows whether the file contains a certificate, a key pair, or both.
key	Specifies the key pair file type.
session	Displays the number of cached TLS and SSL client and server session entries in the current context.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised with the **authgroup**, **csr-params**, **crl**, and **session** keywords.
A3(2.2)	The **cdp-errors** keyword and the **detail** option were added.
A3(2.3)	The **best-effort** keyword was added.

Usage Guidelines

This command requires the SSL feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

When using the **show crypto certificate** command and the certificate file contains a chain, the ACE displays only the bottom level certificate (the signers are not displayed).

For information about the fields in the **show crypto** command output, see the *Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide*.

Examples

To display the summary report that lists all of the crypto files, enter:

```
host1/Admin# show crypto files
```

Related Commands

crypto delete
crypto export
crypto import
crypto verify
(config) crypto csr-params

show debug

To display the debug flags, use the **show debug** command.

show debug {**aaa** | **access-list** | **arpmgr** | **ascii-cfg** | **bpdu** | **buffer** | **cfg_cntlr** | **cfgmgr** | **dhcp** | **fifo** | **fm** | **fs-daemon** | **ha_dp_mgr** | **ha_mgr** | **hm** | **ifmgr** | **ipcp** | **ldap** | **license** | **logfile** | **nat-download** | **netio** | **pfmgr** | **pktcap** | **radius** | **routemgr** | **security** | **sme** | **snmp** | **ssl** | **syslogd** | **system** | **tacacs+** | **tl** | **ttyd** | **virtualization** | **vnet** | **vshd**} [|] [>]

Syntax Description

aaa	Displays the 301 debug flags.
access-list	Displays the access-list debug flags.
arpmgr	Displays the Address Resolution Protocol (ARP) manager debug flags.
ascii-cfg	Displays the ASCII cfg debug flags.
bpdu	Displays the bridge protocol data unit (BPDU) debug flags.
buffer	Displays the CP buffer debug flags.
cfg_cntlr	Displays the configuration controller debug flags.
cfgmgr	Displays the configuration manager debug flags.
dhcp	Displays the Dynamic Host Configuration Protocol (DHCP) debug flags.
fifo	Displays the show packet first in, first out (FIFO) debug flags.
fm	Displays the feature manager debug flags.
fs-daemon	Displays the FS daemon debug flags.
ha_dp_mgr	Displays the high availability (HA) dataplane manager debug flags.
ha_mgr	Displays the HA manager debug flags.
hm	Displays the HM debug flags.
ifmgr	Displays the interface manager debug flags.
ipcp	Displays the kernel IP Control Protocol (IPCP) debug flags.
ldap	Displays the Lightweight Directory Access Protocol (LDAP) debug flags.
license	Displays the licensing debug flags.
logfile	Displays the contents of the logfile.
nat-download	Displays the Network Address Translation (NAT) download debug flags.
netio	Displays the CP net I/O debug flags.
pfmgr	Displays the platform manager debug flags.
pktcap	Displays the packet capture debug flags.
radius	Displays the Remote Authentication Dial-In User Service (RADIUS) debug flags.
routemgr	Displays the route manager debug flags.
security	Displays the security/accounting debug flags.
sme	Displays the System Manager Extension (SME) debug flags.
snmp	Displays the Simple Network Management Protocol (SNMP) server debug flags.
ssl	Displays the Secure Sockets Layer (SSL) manager debug flags.

syslogd	Displays the syslogd debug flags.
system	Displays the system debug flags.
tacacs+	Displays the Terminal Access Controller Access Control System Plus (TACACS+) debug flags.
tl	Displays the CP buffer debug flags.
ttyd	Displays the TTYD debug flags.
virtualization	Displays the virtualization debug flags.
vnet	Displays the virtual network (VNET) driver debug flags.
vshd	Displays the VSHD debug flags.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the debug feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The ACE **debug** commands are intended for use by trained Cisco personnel only. Entering these commands may cause unexpected results. Do not attempt to use these commands without guidance from Cisco support personnel.

Examples

To display the VSHD debug flags, enter:

```
host1/Admin# show debug vshd
```

Related Commands

debug
clear debug-logfile

show domain

To display the information about the configured domains in the ACE, use the **show domain** command.

show domain [*name*] [|] [>]

Syntax Description

name	(Optional) Name of an existing context domain. Specify a domain name to display the detailed configuration report that relates to the specified domain.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Syntax Description

This command has no keywords or arguments.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To display the complete domain configuration report that lists all of the configured domains, enter the **show domain** command without including the *name* argument.

For information about the fields in the **show domain** command output, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To display the domain configuration report for the domain D1, enter:

```
host1/Admin# show domain D1
```

Related Commands

(config) domain

show fifo

To display the packet first in, first out (FIFO) statistics for the Pkt-Fifo module, use the **show fifo** command.

show fifo {**event-history** | **registers** | **stats**} [|] [>]

Syntax Description

event-history	Displays a historic log of the most recent debug messages generated by the Pkt-Fifo module.
registers	Displays the state of all the registers associated with the transmit and receive hardware engines.
stats	Displays detailed counters for the various Pkt-Fifo module event occurrences.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

This command is intended for use by trained Cisco personnel for troubleshooting purposes only.

Examples

To display the control plane packet FIFO registers, enter:

```
host1/Admin# show fifo registers
```

Related Commands

clear fifo stats

show file

To display the contents of a specified file in a directory in persistent memory (flash memory) or volatile memory (RAM), use the **show file** command.

show file {**disk0:** | **volatile:**}[*directory/*]*filename* [**cksum** | **md5sum**] [|] [>]

Syntax Description

disk0:	Specifies the disk0 file system in persistent memory.
volatile:	Specifies the file system in volatile memory.
[*directory/*]*filename*	Path and name of the specified file.
cksum	(Optional) Displays the cyclic redundancy check (CRC) checksum for the file. The checksum values compute a CRC for each named file. Use this command to verify that the files are not corrupted. You compare the checksum output for the received file against the checksum output for the original file.
md5sum	(Optional) Displays the MD5 checksum (electronic fingerprint) for the file. MD5 is the latest implementation of the Internet standards described in RFC 1321 and is useful for data security and integrity.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show file** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display the contents of the file FILE1 stored in the directory MYFILES in disk0:, enter:

```
host1/Admin# show file disk0:MYFILES/FILE1
```

Related Commands

dir
clear cores
delete

show fragment

To display the IP fragmentation and reassembly statistics for all interfaces in the ACE or the specified interface, use the **show fragment** command.

show fragment [**vlan** *vlan_id*] [|] [>]

Syntax Description

vlan *vlan_id*	(Optional) Specifies an existing interface.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the interface feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

If you omit the **vlan** *vlan_id* optional keyword and argument, you can display statistics for all interfaces in the ACE.

For information about the fields in the **show fragment** command output, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

Examples

To display the IP fragmentation and reassembly statistics for VLAN 210, enter:

```
host1/Admin# show fragment vlan 210
```

Related Commands

show vlans

show ft

To display the fault-tolerant (ft), or redundancy, statistics per context, use the **show ft** command.

show ft {**config-error** [*context_name*]} | {**group** {**brief** | {[*group_id*]{**detail** | **status** | **summary**}}}} | {**history** {**cfg_cntlr** | **ha_dp_mgr** | **ha_mgr**}} | {**idmap**} | {**memory** [**detail**]} | {**peer** *peer_id* {**detail** | **status** | **summary**}} | {**stats** *group_id*} | {**track** *group_id* {**detail** | **status** | **summary**}} [|] [>]

Syntax Description

config-error [*context_name*]	Displays the commands that fail on the standby ACE appliance during bulk synchronization in a redundant configuration. If all commands succeed on the standby ACE appliance, the command displays the following message: `No bulk config apply errors` In the Admin context, the optional *context_name* argument is the name of a user context. If you do not enter the argument, the command uses the Admin context. In a user context, this argument is not available.
group *group_id*	Displays FT group statistics for the specified FT group. In the Admin context, this keyword displays statistics for all FT groups in the ACE. Also, in the Admin context, you can specify an FT group number to display statistics for an individual group. In a user context, this keyword displays statistics only for the FT group to which the user context belongs.
brief	Displays the group ID, local state, peer state, context name, and context ID of all the FT groups that are configured in the ACE.
detail	Displays detailed information for the specified FT group or peer.
status	Displays the current operating status for the specified FT group or peer.
summary	Displays summary information for the specified FT group or peer.
history	Displays a history of internal redundancy software statistics (Admin context only).
cfg_cntlr	Displays the configuration controller debug log.
ha_dp_mgr	Displays the high availability (HA) dataplane manager debug log.
ha_mgr	Displays the HA manager debug log.
idmap	Displays the IDMAP table for all object types. In a redundancy configuration, the IDMAP table is used to map objects between the active and the standby ACEs for use in config sync and state replication.
memory [**detail**]	Displays summary HA manager memory statistics or optional detailed HA manager memory statistics (Admin context only).
peer *peer_id*	Specifies the identifier of the remote standby member of the FT group.
stats *group_id*	Displays redundancy statistics for the specified FT group.
track *group_id*	Displays redundancy statistics related to tracked items for all FT groups.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(2.2)	The **config-error** keyword and *context_name* option were added to this command.

Usage Guidelines

This command requires the fault-tolerant feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show ft** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display the detailed statistics for FT group GROUP1, enter:

```
host1/Admin# show ft group GROUP1 detail
```

Related Commands

clear ft
(config) ft auto-sync
(config) ft group
(config) ft interface vlan
(config) ft peer
(config) ft track host
(config) ft track interface

show hardware

To display the ACE hardware details, such as the serial number and the hardware revision level, use the **show hardware** command.

show hardware [|] [>]

Syntax Description

|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show hardware** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display ACE hardware information, enter:

```
host1/Admin# show hardware
```

Related Commands

show inventory
show tech-support

show icmp statistics

To display the Internet Control Message Protocol (ICMP) statistics, use the **show icmp statistics** command.

show icmp statistics [|] [>]

Syntax Description

|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Use the **clear icmp-statistics** command to clear the ICMP statistics.

For information about the fields in the **show icmp statistics** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display ICMP statistics, enter:

```
host1/Admin# show icmp statistics
```

Related Commands

clear icmp statistics

show interface

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

show interface [**bvi** *number* | **gigabitEthernet** *slot_number/port_number* **[counters]** | **internal** {**event-history** {**dbg** | **mts**} | **iftable** [*name*] | **port-vlantable** | **vlantable** [*number*]} **port-channel** *channel_number* | **vlan** *number*] [|] [>]

Syntax Description

bvi *number*	(Optional) Displays the information for the specified Bridge Group Virtual Interface (BVI).
gigabitEthernet *slot_number/port_number*	(Optional) Displays the statistics for the specified gigabit Ethernet slot and port. • The *slot_number* represents the physical slot on the ACE containing the Ethernet ports. This selection is always 1. • The *port_number* represents the physical Ethernet port on the ACE. Valid selections are 1 through 4. This keyword is available in the Admin context only.
counters	Displays a summary of interface counters for the specified Ethernet data port related to the receive and transmit queues.
internal	(Optional) Displays the internal interface manager tables and events.
event-history	Displays event history information.
dbg	Displays debug history information.
mts	Displays message history information.
iftable	Displays the master interface table (Admin context only).
name	(Optional) Interface table name. If you specify an interface table name, the ACE displays the table information for that interface.
port-vlantable	(Optional) Displays the Ethernet port manager VLAN table.
vlantable	(Optional) Displays the VLAN table (Admin context only).
number	(Optional) VLAN number. If you specify an interface number, the ACE displays the table information for that interface.
port-channel *channel_number*	(Optional) Displays the channel number assigned to a port-channel interface. Valid values are from 1 to 255. This keyword is available in the Admin context only.
vlan *number*	(Optional) Displays the statistics for the specified VLAN.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

BVI and VLAN interface—Admin and user contexts

Ethernet data port, Ethernet management port, and port-channel interface—Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the interface feature in your user role. In addition, the Ethernet data port, Ethernet management port, and port-channel interface command functions require the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To display all of the interface statistical information, enter the **show interface** command without using any of the optional keywords.

You can configure flow control on each Ethernet port of a Catalyst 6500 series switch. However, the ACE does not support flow control. If you connect an ACE to a Catalyst 6500 series switch, the flow control functionality is disabled on the ACE. The output of the **show interface gigabitEthernet** command on the ACE displays the "input flow-control is off, output flow control is off" flow-control status line as shown in the example above regardless of the state of flow control on the Catalyst 6500 series switch port to which the ACE is connected.

The **internal** keyword and options are intended for use by trained Cisco personnel for troubleshooting purposes only.

For information about the fields in the **show interface** command output, see the *Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*.

Examples

To display all of the interface statistical information, enter:

```
host1/Admin# show interface
```

To view the configuration status for Ethernet data port 4, enter:

```
host1/Admin# show interface gigabitEthernet 1/4
```

Related Commands

clear interface

show inventory

To display the system hardware inventory, use the **show inventory** command.

show inventory [**raw**] [|] [>]

Syntax Description

raw	(Optional) Displays the hardware inventory report and information about each temperature sensor in the ACE.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Use the **show inventory** command to display information about the field-replaceable units (FRUs) in the ACE, including product IDs, serial numbers, and version IDs.

If you do not include the **raw** keyword, the ACE displays the hardware inventory report only.

For information about the fields in the **show inventory** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display the hardware inventory report, enter:

```
host1/Admin# show inventory
```

To display the hardware inventory report and information about each temperature sensor, enter:

```
host1/Admin# show inventory raw
```

Related Commands

show hardware

show ip

To display the IP statistics, use the **show ip** command.

show ip {**dhcp relay** {**conf** | **information policy** | **statistics**} | **fib** [**ixp** {**1** | **2** {**dest-ip** *ip_address*}} | **summary** | **wr dest-ip** *ip_address*] | **interface brief** {[**bvi** | **vlan**] *number*} | **route** [**summary** | **internal** {**event-history dbg** | **memory**}] | **traffic**} [|] [>]

Syntax Description

dhcp relay	Specifies the Dynamic Host Configuration Protocol (DHCP) configuration information.
conf	Displays the DHCP relay configuration information.
information policy	Displays the relay agent information and the reforwarding policy status.
statistics	Displays the DHCP relay statistics.
fib	Displays the Forwarding Information Base (FIB) table for the context. This table contains information that the forwarding processors require to make IP forwarding decisions. This table is derived from the route and ARP tables.

ixp 1 | 2 dest-ip *ip_address*	(Optional) Displays the FIB information for a destination address on the ACE IXP (network processor) 1 or 2. Enter the IP address in dotted-decimal notation (for example, 172.27.16.10).
summary	(Optional) Displays the FIB table or route summary for the current context.
wr dest-ip *ip_address*	(Optional) Displays the FIB information for the specified wire region (0 only) and destination IP address. Enter the IP address in dotted-decimal notation (for example, 172.27.16.10).
interface brief	Displays a brief configuration and status summary of all interfaces, a specified bridge group virtual interface (BVI), or a virtual LAN (VLAN), including the interface number, IP address, status, and protocol.
bvi	Displays the information for a specified BVI.
vlan	Displays the statistics for a specified VLAN number.
number	Number of the existing BVI or VLAN. For a BVI, enter an integer from 1 to 4090. For a VLAN, enter an integer from 2 to 4090.
route	Displays the route entries.
internal	(Optional) Specifies the internal route entries.
event-history dbg	Displays the event history statistics.
memory	Displays the mtrack output statistics.
traffic	Displays the IP protocol statistics.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	Added the **interface brief** and related keywords.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The **internal** and **fib** keywords and options are intended for use by trained Cisco personnel for troubleshooting purposes only.

For information about the fields in the **show ip** command output, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide* and the *Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*.

Examples

To display all IP route entries, enter:

```
host1/Admin# show ip route
```

Related Commands

clear ip

show ipcp

To display the Interprocess Communication Protocol (IPCP) statistics, use the **show ipcp** command.

show ipcp {**cde** | clients | event-history | pci | peek_poke} [|] [**>**]

Syntax Description

cde	Displays IPCP statistical information.
clients	Displays IPCP message queue information.
event-history	Displays IPCP event history information.
pci	Displays IPCP Peripheral Component Interconnect (PCI) information.
peef_poke	Displays IPCP peek poke message queue information.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

This command is intended for use by trained Cisco personnel for troubleshooting purposes only.

Examples

To display IPCP statistics for the CDE interface, enter the following command:

```
host1/Admin# show ipcp cde
```

Related Commands

This command has no related commands.

show kalap udp load

To display the latest load information for a VIP address or a domain name provided to the KAL-AP request, use the **show kalap udp load** command in Exec mode.

show kalap udp load {**all** | **domain** *domain* | **vip** *ip_address*} [|] [>]

Syntax Description

all	Displays the latest load information for all VIP addresses and domains.
domain *domain*	Displays the latest load information for the specified domain name.
vip *ip_address*	Displays the latest load information for the specified VIP address. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The output fields for the **show kalap udp load** command display the VIP address or domain name, its load value, and the time stamp.

Examples

To display the latest load information to the KAL-AP request for VIP address 10.10.10.10, enter:

```
host1/Admin# show kalap udp load vip 10.10.10.10
```

To display the latest load information to the KAL-AP request for domain KAL-AP-TAG1, enter:

```
host1/Admin# show kalap udp load domain KAL-AP-TAG1
```

Related Commands

This command has no related commands.

show ldap-server

To display the configured Lightweight Directory Access Protocol (LDAP) server and server group parameters, use the **show ldap-server** command.

show ldap-server [**groups**] [|] [>]

Syntax Description

groups	(Optional) Displays configured LDAP server group information.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show ldap-server** command output, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

Examples

To display the configured LDAP server groups, enter:

```
host1/Admin# show ldap-server groups
```

Related Commands

(config) aaa group server
(config) ldap-server host
(config) ldap-server port
(config) ldap-server timeout

show license

To display your ACE license information, use the **show license** command.

show license [**brief** | **file** *filename* | **internal event-history** | **status** | **usage**] [|] [>]

Syntax Description

brief	(Optional) Displays a filename list of currently installed licenses.
file *filename*	(Optional) Displays the file contents of the specified license.
internal event-history	(Optional) Displays a history of licensing-related events.
status	(Optional) Displays the status of licensed features.
usage	(Optional) Displays the usage table for all licenses.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.
A3(2.3)	The Count value for Web Optimization in the **show license status** command output has been modified from “cps” to “concurrent connections.”

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Entering the **show license** command without any options and arguments displays all of the installed ACE license files and their contents.

For information about the fields in the **show license** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

To manage the licenses on your ACE, use the **license** command.

Examples

To display all of the installed ACE license files and their contents, enter:

```
host1/Admin# show license
```

Related Commands

copy capture
license

show line

To display all of the configured console and virtual terminal line sessions, use the **show line** command.

show line [**console** [**connected**]] [|] [>]

Syntax Description

console	(Optional) Displays the configured console settings for the ACE.
connected	(Optional) Displays the physical connection status.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show line** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display all configured console and virtual terminal line sessions, enter:

```
host1/Admin# show line
```

Related Commands

clear line

show logging

To display the current severity level and state of all syslog messages stored in the logging buffer, or to display information related to specific syslog messages, use the **show logging** command.

show logging [**history** | **internal** {**event-history dbg** | **facility**} | **message** [*syslog_id* | **all** | **disabled**] | **persistent** | **queue** | **rate-limit** | **statistics**] [|] [>]

Syntax Description

history	(Optional) Displays the logging history file.
internal	(Optional) Displays syslog internal messages.
event-history dbg	Displays the debug history for the syslog server.
facility	Displays the registered internal facilities for the syslog server.
message	(Optional) Displays a list of syslog messages that have been modified from the default settings. These are messages that have been assigned a different severity level or messages that have been disabled.
syslog_id	(Optional) Identifier of a specific system log message to display, specified by message ID, and identifies whether the message is enabled or disabled.
all	(Optional) Displays all system log message IDs and identifies whether they are enabled or disabled.
disabled	(Optional) Displays a complete list of suppressed syslog messages.
persistent	(Optional) Displays statistics for the log messages sent to flash memory on the ACE.
queue	(Optional) Displays statistics for the internal syslog queue.
rate-limit	(Optional) Displays the current syslog rate-limit configuration.
statistics	(Optional) Displays syslog statistics.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To use the **show logging** command, you must have the ACE buffer enabled as a logging output location. By default, logging to the local buffer on the ACE is disabled. To enable system logging to a local buffer and to limit the messages sent to the buffer based on severity, use the **logging buffered** configuration command from the desired context.

The **show logging** command lists the current syslog messages and identifies which **logging** command options are enabled.

To clear the ACE buffer of the logging information currently stored, use the **clear logging** command.

For information about the fields in the **show logging** command output, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

Examples

To display a complete list of disabled syslog messages, enter:

```
host1/Admin# show logging message disabled
```

To display the contents of the logging history buffer, enter:

```
host1/Admin# show logging history
```

To display the contents of the internal facility messages buffer, enter:

```
host1/Admin# show logging internal facility
```

To display statistics for the log messages sent to flash memory on the ACE, enter:

```
host1/Admin# show logging persistent
```

To display statistics for the internal syslog queue, enter:

```
host1/Admin# show logging queue
```

To display the current syslog rate-limit configuration, enter:

```
host1/Admin# show logging rate-limit
```

To display the current syslog statistics, enter:

```
host1/Admin# show logging statistics
```

Related Commands

clear logging
(config) logging buffered

show login timeout

To display the login session idle timeout value, use the **show login timeout** command.

show login timeout [|] [>]

Syntax Description

|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To configure the login timeout value, use the **login timeout** command in configuration mode.

For information about the fields in the **show login timeout** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display the login timeout value, enter:

```
host1/Admin# show login timeout
```

Related Commands

(config) login timeout

show nat-fabric

To display the Network Address Translation (NAT) policy and pool information for the current context, use the **show nat-fabric** command.

show nat-fabric {**policies** | **src-nat** *policy_id mapped_if* | **dst-nat** *static_xlate_id* | **nat-pools** | **implicit-pat**| **global-static**} [|] [>]

Syntax Description

policies	Displays the NAT policies.
src-nat *policy_id mapped_if*	Displays the specified source NAT policy information. To obtain the values for the *policy_id* and *mapped_if* arguments, view the policy_id and mapped_if fields displayed by the **show nat-fabric policies** command.
dst-nat *static_xlate_id*	Displays the static address translation for the specified static XLATE ID. To obtain the value for the *static_xlate_id* argument, view the static_xlate_id field displayed by the **show nat-fabric policies** command.
nat-pools	Displays NAT pool information for a dynamic NAT policy.
implicit-pat	Displays the implicit PAT policies.
global-static	Displays global static NAT information when the **static** command in global configuration mode is configured.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised with the **global-static** keyword.

Usage Guidelines

This command requires the NAT feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

This command is intended for use by trained Cisco personnel for troubleshooting purposes only.

To obtain the values for the *policy_id*, *mapped_if*, and *static_xlate_id* arguments, view their respective fields displayed by the **show nat-fabric policies** command.

Examples To display the implicit PAT policies, enter:

```
host1/Admin# show nat-fabric implicit-pat
```

Related Commands This command has no related commands.

show netio

To display the control plane network I/O information, use the **show netio** command.

show netio {**clients** | **event-history** | **stats**} [|] [>]

Syntax Description

clients	Displays statistics for the applications that are transmitting and receiving packets through the Netio module.
event-history	Displays a historic log of the most recent debug network I/O messages.
stats	Displays detailed counters for various Netio event occurrences.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

This command is intended for use by trained Cisco personnel for troubleshooting purposes only.

Examples To display control plane network I/O client information, enter:

```
host1/Admin# show netio event-history
1) Event:E_DEBUG, length:73, at 921762 usecs after Sat Jan 1 00:04:55 2000
[105] ed_request_encap: Sending ARP_RESOLUTION for 75.0.0.6, in context 0
2) Event:E_DEBUG, length:78, at 921752 usecs after Sat Jan 1 00:04:55 2000
[105] ed_egress_route_lookup: Route lookup failure -96 for 75.0.0.6, context 0
```

Related Commands clear netio stats

show np

To display the hardware information stored on the two network processors (NPs), use the **show np** command.

show np *np_number* {**access-list** {**node vlan** *vlan_number* {**in** *node_address* | **out** *node_address*} | **resource** | **root vlan** *vlan_number* {**in** | **out**} | **syslog {linenotable** *table_index* [**all**] | **name_table** *table_index* [**all**] **}** | **trace vlan** *vlan_number* {**in** | **out**} **protocol** *prot_number* | **source** *source_ip source_port* | **destination** *dest_ip dest_port*} | **adjacency** [*lower_index upper_index* [**all**] | **cpu** | **internal** [*lower_index upper_index*] | **reap**] | **interface** {**icmlookup** [**all**] | **iflookup** [**all**]} | **mac-address-table** | **me-stats** *ucdump_option* | **memory** | **mtrie dest-ip** *dest_ip* | **nat** {**bitmap** *map_id* | **dst_nat** *policy_id* | **implicit-pat** | **policies** | **src-nat** *policy_id interface_id*} | **status**} [|] [**>**]

Syntax Description

np_number	Network processor number. Enter one of the following processor identifier numbers: • **0**—x86 processor • **1**—Octeon processor
access-list	Displays information related to the access list.
node	Displays the contents of the hardware access control list (ACL) node, identified by the *vlan_number*.
vlan *vlan_number*	Specifies the number of the VLAN.
in	Specifies the inbound traffic flow.
out	Specifies the outbound traffic flow.
node_address	Address of the node.
resource	Displays information about the access list resource usage.
root	Displays the hardware address of the root of the downloaded, aggregated ACL, identified by the *vlan_number*.
syslog	Displays information about the access list syslog tables.
linenotable *table_index*	Displays the access list syslog namestring table. Enter an index entry from 0 to 262143.
name_table *table_index*	Displays the access list syslog line number table. Enter an index entry from 0 to 16383.
all	Specifies if invalid entries also need to be shown
trace vlan *vlan_number*	Traces a packet through a specific access list.
protocol *prot_number*	Specifies a protocol number.
source	Specifies the source of the flow.
source_ip	Source IP address.
source_port	Source port number.
destination	Specifies the destination of a flow.
dest_ip	Destination IP address.
dest_port	Destination port number.
adjacency	(Optional) Displays information related to the adjacent nodes.
lower_index	(Optional) Lower index value. Enter a value from 1 to 32767.

upper_index	(Optional) Upper index value. Enter a value from 1 to 32767.
all	(Optional) Displays all entries, including invalid entries.
internal	(Optional) Displays the internal information for adjacency structures.
reap	(Optional) Retrieves the encap reap statistics.
cpu	Displays information about the CPU processes. This command option is available only to a user with the Admin role in any context.
interface	Displays information related to the interface tables.
icmlookup	Displays the ICM/OCM interface table from the CP (0) or the specified NP.
iflookup	Displays the fast path interface lookup table from the CP (0) or the specified NP. **Note** The **iflookup** keyword presents information from the fast path interface lookup table. If you wish to verify the configured shared VLAN host ID value, enter the **show running-config | include shared** command.
mac-address-table	Displays the MAC address table.
me-stats	Displays Micro Engine statistics for the specified network processor. This command option is available only to a user with the Admin role in any context.
ucdump_option	Options for the ucdump utility. The ucdump utility is a binary on Xscale which returns information about Micro Engine statistics. Specify **--help** as the *ucdump_option* argument to list all of the supported ucdump utility options. Enter up to 80 alphanumeric characters. **Note** The following ucdump utility options are disabled from **show np me-stats**: -C, -f, and -i.
memory	Displays information about the memory processes. This command option is available only to a user with the Admin role in any context.
mtrie dest-ip *dest_ip*	Displays Mtrie entry for the specified destination IP address.
nat	Displays information related to the network processor Network Address Translation (NAT) tables.
bitmap *map_id*	Specifies the NAT-pool bit-map table in the network processor.
dest_nat *policy_id*	Specifies the destination NAT policy.
implicit-pat	Specifies the implicit Port Address Translation (PAT) policy table.
policies	Specifies the full NAT policy table.
src-nat	Specifies the source NAT policy.
policy_id	Policy identifier number. Enter a value from 0 to 65535.
interface_id	Mapped interface identifier. Enter a value from 0 to 65535.
status	Displays status information related to the specified network processor.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command and its options require the access-list or interface feature in your user role, except for the **cpu**, **me-stats**, and **memory** options. These three options require that you have the Admin user role in any context. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

This command is intended for use by trained Cisco personnel for troubleshooting purposes only.

Examples

To display the access list information from the hardware using the network processor 0, enter:

```
host1/Admin# show np 0 access-list
```

To display Micro Engine statistics for a ucdump utility (-b, which instructs the ACE to dump fastpath buffer memory), enter:

```
host1/Admin# show np me-stats -b

Fastpath thread buffers
================================

ME:1 thread:0 addr:0x0010 particle:0x00000000 len:78 rx_seq=7
0018  0x8500004e  0x00608034  0x0000001e  0x00101e07    ...N .`.4 .... ....
001c  0x0000ffff  0xffffffff  0x00059a3b  0x9a390800    .... .... ...; .9..
0020  0x4500002c  0xa4540000  0xff11fd64  0x0c010105    E..,  .T.. ...d ....
0024  0x0c010101  0xc350c352  0x00185db6  0x000100f0    .... .P.R ..]. ....
0028  0x00000008  0x00000000  0x00000064  0x00000000    .... .... ...d ....
```

Related Commands

show processes

show ntp

To display information about the Network Time Protocol (NTP) statistics, use the **show ntp** command.

show ntp {**peer-status** | **peers** | **statistics** [**io** | **local** | **memory** | **peer** *ip_address*]} [|] [>]

Syntax Description

peer-status	Displays the status for all configured NTP servers and peers.
peers	Displays a listing of all peers.
statistics	Displays the NTP statistics.
io	(Optional) Displays information the input/output statistics.
local	(Optional) Displays the counters maintained by the local NTP.
memory	(Optional) Displays the statistical counters related to the memory code.
peer	(Optional) Displays the peer-peer statistical counters of the specified peer.
ip_address	Peer statistics for the specified IP address.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To display the status for all configured NTP servers and peers, enter:

```
host1/Admin# show peer-status
```

To display a listing of all peers, enter:

```
switch/Admin# show ntp peers
```

Related Commands

(config) ntp

show optimization-global

To display information about the global optimization statistics, use the **show optimization-global** command.

show optimization-global [|] [>]

Syntax Description

|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To display global optimization statistics, enter:

```
host1/Admin# show optimization-global
```

Related Commands

(config) optimize

show parameter-map

To display the detailed configuration information for a specified parameter map, use the **show parameter-map** command.

show parameter-map [*parammap_name*] [|] [>]

Syntax Description

parammap_name	(Optional) Name of an existing parameter map. Enter the name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(2.3)	The Description field has been added to the **show parameter-map** command output. This field displays the previously entered summary about the specific parameter map.

Usage Guidelines

This command requires the connection feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To display the configuration for the parameter map SSL_PARAMMAP, enter:

```
host1/Admin# show parameter-map SSL_PARAMMAP
```

Related Commands

show running-config

show probe

To display the probe information including script probes, use the **show probe** command.

show probe [*probe_name*] [**detail**] [|] [**>**]

Syntax Description

probe_name	(Optional) Name of an existing probe.
detail	(Optional) Displays a detailed probe report that includes configuration information and statistics for all configured probes.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the probe feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

If you enter the **show probe** command without specifying a probe name, the ACE displays a summary report that includes all configured probes.

For information about the fields in the **show probe** command output, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To display the probe summary report, enter:

```
host1/Admin# show probe
```

Related Commands

clear probe
(config) probe

show processes

To display the general information about all of the processes running on the ACE, use the **show processes** command. The **show processes** command displays summary CPU information for the Pentium processor.

show processes [**cpu** | **log** [**details** | **pid** *process_id*] | **memory**] [|] [>]

Syntax Description

cpu	(Optional) Displays information about the CPU processes for the Pentium processor.
log	(Optional) Displays information about the process logs for the Pentium processor.
details	(Optional) Displays detailed process log information for all process identifiers.
pid *process_id*	(Optional) Displays process information about a specific process identifier. Enter a value from 0 to 2147483647.
memory	(Optional) Displays information about the memory processes for the Pentium processor.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin users (users with an Admin role), across all contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The **show processes** command is available only to Admin users (users with an Admin role) across all contexts. The displayed system processes information is at the CPU system level (the total CPU usage) and is not on a per-context level.

For information about the fields in the **show processes** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display information about the memory processes for the Pentium processor, enter:

```
host1/Admin# show processes memory
```

Related Commands

clear processes log

show np
show tech-support

show radius-server

To display the configured Remote Authentication Dial-In User Service (RADIUS) server and group parameters, use the **show radius-server** command.

show radius-server [**groups** | **sorted**] [|] [>]

Syntax Description

groups	(Optional) Displays configured RADIUS server group information.
sorted	(Optional) Displays RADIUS server information sorted by name.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show radius-server** command output, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

Examples

To display configured RADIUS server parameters, enter:

```
host1/Admin# show radius-server
```

To display the configured RADIUS server groups, enter:

```
host1/Admin# show radius-server groups
```

To display the sorted RADIUS servers, enter:

```
host1/Admin# show radius-server sorted
```

Related Commands

- **(config) aaa group server**
- **(config) radius-server attribute nas-ipaddr**
- **(config) radius-server deadtime**
- **(config) radius-server host**
- **(config) radius-server key**
- **(config) radius-server retransmit**

show resource allocation

To display the allocation for each resource across all resource classes and class members, use the **show resource allocation** command.

show resource allocation [|] [>]

Syntax Description

|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

This command shows the resource allocation but does not show the actual resources being used. To display information about actual resource usage, use the **show resource usage** command.

For information about the fields in the **show resource allocation** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display the allocation for each resource, enter:

```
host1/Admin# show resource allocation
```

Related Commands

- **show resource usage**

show resource usage

To display the resource usage for each context, use the **show resource usage** command.

show resource usage [**all** | [[**context** *context_name* | **summary** | **top** *number*] [**resource** {**acc-connections** | **acl-memory** | **all** | **conc-connections** | **mgmt-connections** | **probes** | **proxy-connections** | **rate** {**bandwidth** | **connections** | **http-comp** | **inspect-conn** | **mac-miss** | **mgmt-traffic** | **ssl-connections** | **syslog**} | **regexp** | **sticky** | **syslogbuffer** | **xlates**}]]] [**counter** [**all** | **current** | **denied** | **peak** [*count_threshold*]]] [|] [**>**]

Syntax Description

all	(Optional) Displays the resource usage for each context individually. This is the default setting.
context *context_name*	(Optional) Displays the resource usage for the specified context. The *context_name* argument is case sensitive.
summary	(Optional) Displays the total resource usage for all contexts together. For example, the denied column shows the items that have been denied for each context limit.
top *number*	(Optional) Displays the greatest *n* users of a single resource arranged from the highest to the lowest percentage of resources used. You must specify a single resource type and cannot use the **resource all** keywords with this option.
resource	(Optional) Displays statistics for one of the following specified resources:
acc-connections	Displays the number of application acceleration connections.
acl-memory	Displays the ACL memory usage.
all	Displays the resource usage for all resources used by the specified context or contexts.
conc-connections	Displays the resource usage for simultaneous connections.
mgmt-connections	Displays the resource usage for management connections.
probes	Displays the resource usage for probes.
proxy-connections	Displays the resource usage for proxy connections.
rate	Displays the rate per second for the specified connections or syslog messages.
bandwidth	Displays the bandwidth in bytes per second.
connections	Displays connections per second.
http-comp	Displays the HTTP compression rate in bytes per second. To convert the value to bits per second, multiply the displayed value by 8.
inspect-conn	Displays RTSP/FTP inspection connections per second.
mac-miss	Displays MAC miss traffic that was punted to the CP packets per second.
mgmt-traffic	Displays management traffic bytes per second.
ssl-connections	Displays Secure Sockets Layer (SSL) connections.
syslog	Displays the syslog message buffer usage.
regexp	Displays resource usage for regular expressions.
sticky	Displays resource usage for sticky entries.

syslogbuffer	Displays resource usage for the syslog buffer.
xlates	Displays resource usage by Network Address Translation (NAT) and Port Address Translation (PAT) entries.
counter	(Optional) Specifies one of the following keywords as the counter name:
all	(Optional) Displays all statistics. This is the default setting.
current	(Optional) Displays the active concurrent instances or the current rate of the resource.
denied	(Optional) Displays the number of denied uses of the resource since the resource statistics were last cleared.
peak	(Optional) Displays the peak concurrent instances, or the peak rate of the resource since the statistics were last cleared, either using the **clear resource usage** command or because the device rebooted.
count_threshold	(Optional) Number above which resources are shown. Enter an integer from 0 to 4294967295. The default is 1. If the usage of the resource is below the number you set, then the resource is not shown. If you specify **all** for the counter name, then the *count_threshold* applies to the current usage. To show all resources, set the *count_threshold* to **0**.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Defaults

None

Command Modes

Exec

Admin context

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show resource usage** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display the resource usage for context C1, enter:

```
host1/Admin# show resource usage context C1 resource
```

Related Commands This command has no related commands.

show role

To display the configured user roles (predefined and user-configured roles), use the **show role** command.

show role [*role_name*] [|] [**>**]

Syntax Description

role_name	(Optional) Name of an existing role.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To configure roles, use the **role** command in configuration mode.

For information about the fields in the **show role** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display all of the available user roles, enter:

```
host1/Admin# show role
```

Related Commands

(config) role

show rserver

To display the summary or detailed statistics for a named real server or for all real servers, use the **show rserver** command.

show rserver [*rserver_name*] [**detail**] [|] [**>**]

Syntax Description

rserver_name	(Optional) Identifier of an existing real server.
detail	(Optional) Displays detailed statistics for the real server name that you enter or for all real servers. If you do not include the **detail** keyword, the summary report is displayed.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the rserver feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show rserver** command output, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

For the Total Conn-failures output field of the **show rserver detail** command, the following conditions apply:

For Layer 4 traffic with normalization on, the count increments if the three-way handshake fails to be established for either of the following reasons:

- A RST comes from the client or the server after a SYN-ACK.
- The server does not reply to a SYN. The connection times out.

For Layer 4 traffic with normalization off, the count does not increment.

For L7 traffic (normalization is always on), the count increments if the three-way handshake fails to be established for either of the following reasons:

- A RST comes from the server after the front-end connection is established
- The server does not reply to a SYN. The connection times out.

Examples

To display detailed statistics for all configured real servers, enter:

```
host1/Admin# show rserver detail
```

Related Commands

clear rserver
(config) rserver

show running-config

To display the running configuration information associated with the current context, use the **show running-config** command.

show running-config [**aaa** | **access-list** | **action-list** | **class-map** | **context** | **dhcp** | **domain** | **ft** | **interface** | **object-group** | **parameter-map** | **policy-map** | **probe** | **resource-class** | **role** | **rserver** | **serverfarm** | **sticky**] [|] [>]

Syntax Description

aaa	(Optional) Displays authentication, authorization, and accounting (AAA) information.
access-list	(Optional) Displays access control list (ACL) information.
action-list	(Optional) Displays action-list information.
class-map	(Optional) Displays the list of all class maps configured for the current context. The ACE also displays configuration information for each class map listed.
context	(Optional) Displays the list of contexts configured on the ACE. The ACE also displays the resource class (member) assigned to each context. The **context** keyword only works from within the admin context.
dhcp	(Optional) Displays Dynamic Host Configuration Protocol (DHCP) information.
domain	(Optional) Displays the list of domains configured for the current context. The ACE also displays configuration information for each domain listed.
ft	(Optional) Displays the list of redundancy or fault-tolerance (ft) configurations configured for the current context. The ACE also displays configuration information for each ft configuration listed.
interface	(Optional) Displays interface information.
object-group	(Optional) Displays object-group information.
parameter-map	(Optional) Displays parameter map information.
policy-map	(Optional) Displays policy map information.
probe	(Optional) Displays probe information.
resource-class	(Optional) Displays resource class information.
role	(Optional) Displays the list of roles configured for the current context. The ACE also displays configuration information for each role on the list.
rserver	(Optional) Displays rserver information.
serverfarm	(Optional) Displays server farm information.
sticky	(Optional) Displays sticky information.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The **show running-config** command is a context-sensitive command. The ACE creates a running configuration for each context that you create; therefore, to display the running-config file of a specific context, you must enter the **show running-config** command from within the desired context. If you need to change to another context before executing the **show running-config** command, use the **changeto** command or log directly in to the desired context.

Use the **copy capture** command to do the following:

- Save a copy of the running configuration to a file on one or more destination locations.
- Save the running configuration as the startup configuration.
- Save the startup configuration as the running configuration.

For information about the fields in the **show running-config** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display the entire running configuration, enter:

```
host1/Admin# show running-config
```

Related Commands

copy capture
show startup-config
show tech-support
write

show script

To display the statistics for a script file that is active on the ACE including exit codes and exit messages, use the **show script** command.

show script {*script_name probe_name* [*rserver_name* [*port_number*] [**serverfarm** *sfarm_name*]] | **code** *script_name*} [|] [**>**]

Syntax Description

script_name	Name of a loaded script.
probe_name	Name of a probe containing an association with the specified script.
rserver_name	(Optional) Name of a real server that contains an association with the specified probe.
port_number	(Optional) Port number on the specified real server.
serverfarm *sfarm_name*	(Optional) Specifies the server farm containing an association with the specified real server.
code *script_name*	Displays the code for the specified script.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the probe feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show script** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display the script file code for the script in the file MYSCRIPT, enter:

```
host1/Admin# show script code MYSCRIPT
```

Related Commands

(config) script file name
(config-probe-probe_type) script

show security internal event-history

To display information about the security event history, use the **show security internal event-history** command.

show security internal event-history {**errors** | **msgs**} [|] [>]

Syntax Description

errors	Displays the debug error logs of the security manager.
msgs	Displays the message logs of the security manager.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

This command is intended for use by trained Cisco personnel for troubleshooting purposes only.

Examples

To display the error logs of the security manager, enter:

```
host1/Admin# show security internal event-history errors
```

Related Commands

This command has no related commands.

show serverfarm

To display a summary or detailed statistics about a specified server farm, use the **show serverfarm** command.

show serverfarm [*name* [**retcode**]] [**detail**] [|] [**>**]

Syntax Description

name	(Optional) Detailed report for the specified server farm. If you do not specify a server farm name, the summary report is displayed.
retcode	(Optional) Displays the HTTP return codes statistics for configured real server and retcode map combinations only if the return code hit count is greater than 0. All return code hit counts are an aggregate of the counts of both network processors. Displays the HTTP return codes associated with the server farm.
detail	(Optional) Displays detailed statistics for the specified server farm. When used after the **retcode** option, the **detail** option displays return code statistics even if the value is 0.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the serverfarm feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show serverfarm** command output, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To display a summary report about the server farm, enter:

```
host1/Admin# show serverfarm
```

Related Commands

clear serverfarm
(config) serverfarm

show service-policy

To display the statistics for all policy maps or a specific policy map that is currently in service, use the **show service-policy** command. If you do not enter an option with this command, the ACE displays all enabled policy statistics.

show service-policy [*policy_name* [**class-map** *class_name*]] [**detail** | **summary**] [|] [>]

Syntax Description

policy_name	(Optional) Identifier of an existing policy map that is currently in service (applied to an interface) as an unquoted text string with a maximum of 64 alphanumeric characters. If you do not enter the name of an existing policy map, the ACE displays information and statistics for all policy maps.
class-map *class_name*	(Optional) Displays the statistics for the specified class map associated with the policy.
detail	(Optional) Displays a more detailed listing of policy map statistics and status information.
summary	(Optional) Displays a summary of policy map or class map statistics and status information.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(2.1)	The **class-map** *class_name* and **summary** options were added.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The **show service-policy** command displays the following information:

- VLAN to which the policy is applied
- Class map associated with the policy
- Status of any load-balancing operations

The ACE updates the counters that the **show service-policy** command displays after the applicable connections are closed.

For information about the fields in the **show service-policy** command output, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To display detailed statistics and current status of the service policy MGMT_POLICYMAP, enter:

```
host1/Admin# show service-policy MGMT_POLICYMAP detail
```

Related Commands

clear service-policy
show running-config
(config) service-policy

show snmp

To display the Simple Network Management Protocol (SNMP) statistics and configured SNMP information, use the **show snmp** command.

show snmp [**community** | **engineID** | **group** | **host** | **sessions** | **user**] [|] [>]

Syntax Description

community	(Optional) Displays SNMP community strings.
engineID	(Optional) Displays the identification of the local SNMP engine and all remote engines that have been configured on the ACE.
group	(Optional) Displays the names of groups on the ACE, the security model, the status of the different views, and the storage type of each group.
host	(Optional) Displays the configured SNMP notification recipient host, the User Datagram Protocol (UDP) port number, the user, and the security model.
sessions	(Optional) Displays the IP address of the targets for which traps or informs have been sent.
user	(Optional) Displays SNMPv3 user information.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

By default, this command displays the ACE contact, the ACE location, the packet traffic information, community strings, and the user information. You can instruct the ACE to display specific SNMP information by including the appropriate keyword.

For information about the fields in the **show snmp** command output, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

Examples

To display SNMP statistics and configured SNMP information, enter:

```
host1/Admin# show snmp
```

Related Commands

(config) snmp-server community
(config) snmp-server contact
(config) snmp-server enable traps
(config) snmp-server host
(config) snmp-server location
(config) snmp-server trap link ietf
(config) snmp-server trap-source vlan
(config) snmp-server user

show ssh

To display the information about the Secure Shell (SSH) keys and sessions, use the **show ssh** command.

show ssh {**key** [**dsa** | **rsa** | **rsa1**] | **maxsessions** [*context_name*] | **session-info** [*context_name*]} [|] [**>**]

Syntax Description

key	Displays the host key pair details for all SSH keys.
dsa	(Optional) Displays only the details of the DSA key pair for the SSH version 2 protocol.
rsa	(Optional) Displays only the details of the RSA key pair for the SSH version 2 protocol.
rsa1	(Optional) Displays only the details of the RSA1 key pair for the SSH version 1 protocol.
maxsessions	Displays the maximum number of SSH sessions that the ACE allows. Context administrators may also view SSH session information associated with a particular context.
context_name	(Optional) Name of an existing context that contains the SSH session information that the context administrator wants to view. Only the global administrator can view Telnet information associated with a particular context. The *context_name* argument is case sensitive and is visible only from the admin context.
session-info	Displays session information, including the session ID, the remote host IP address, and the active time.

|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

From the Admin context, this argument allows you to display only the SSH information associated with a specific user-created context.

For information about the fields in the **show ssh** command output, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

Examples

To display all of the loaded SSH keys, enter:

```
host1/Admin# show ssh key
```

To display the maximum number of SSH sessions that the ACE permits for the context C2, enter:

```
host1/Admin # show ssh maxsessions C2
Maximum Sessions Allowed is 2(SSH Server is enabled)
```

Related Commands

clear ssh
(config) class-map
(config) ssh key
(config) ssh maxsessions

show startup-config

To display information about the startup configuration that is associated with the current context, use the **show startup-config** command.

show startup-config [|] [>]

Syntax Description

|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To clear the startup configuration, use the **clear startup-config** command.

To copy the running configuration to the startup configuration, or copy the startup configuration to the running configuration, use the **copy running-config** command.

For information about the fields in the **show startup-config** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display information about the startup configuration, enter:

```
host1/Admin# show startup-config
```

Related Commands

clear startup-config
copy capture
show running-config

show stats

To display statistics about the ACE operation, use the **show stats** command.

show stats [**connection** | {**crypto {client** | **server}** [**alert** | **authentication** | **cipher** | **termination**]} | **http** | **inspect** [**ftp** | **http** | **rtsp**]| **kalap** | **loadbalance** [**radius** | **rdp** | **rtsp** | **sip**] | **optimization http** | **probe** [**type** *probe_type*] | **sticky**] [|] [>]

Syntax Description

connection	(Optional) Displays global connection statistics associated with the current context.
crypto	(Optional) Displays TLS and SSL client (**client** keyword) or server (**server** keyword) statistics for the current context.
client	Displays the complete TLS and SSL client statistics for the current context.
server	Displays the complete TLS and SSL server statistics for the current context.
alert	(Optional) Displays back-end SSL alert statistics.
authentication	(Optional) Displays the back-end SSL authentication statistics.
cipher	(Optional) Displays the back-end SSL cipher statistics.
termination	(Optional) Displays the back-end SSL termination statistics.
http	(Optional) Displays global HTTP statistics associated with the current context.
inspect [**ftp** | **http** | **rtsp**]	(Optional) Displays global FTP, HTTP, or RTSP inspect statistics associated with the current context. If you do not include any options with the inspect keyword, the ACE displays the global HTTP statistics.
kalap	(Optional) Displays global server load-balancing (GSLB) statistics associated with the current context.
loadbalance	(Optional) Displays global load-balancing statistics associated with the current context.
radius	(Optional) Displays Remote Authentication Dial-In User Service (RADIUS) load-balancing statistics associated with the current context.
rdp	(Optional) Displays Reliable Datagram Protocol (RDP) load-balancing statistics associated with the current context.
rtsp	(Optional) Displays Real-Time Streaming Protocol (RTSP) load-balancing statistics associated with the current context.
sip	(Optional) Displays Session Initiation Protocol (SIP) load-balancing statistics associated with the current context.
optimization http	(Optional) Displays HTTP optimization global statistics associated with the current context.
probe [**type** *probe_type*]	(Optional) Displays global probe statistics associated with the current context.
sticky	(Optional) Displays global sticky statistics associated with the current context.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised.
A3(2.1)	The **alert**, **authentication**, **cipher**, and **termination** options were added.
A3(2.2)	The SSL CRL download field for the **show stats client | server** command was removed. The TCP fin/rst msgs sent, Bounced fin/rst msgs sent, and SSL fin/rst msgs sent fields for the **show stats http** command was divided into the following new fields in the **show stats http command** output: • TCP fin msgs sent • TCP rst msgs sent • Bounced fin msgs sent • Bounced rst msgs sent • SSL fin msgs sent • SSL rst msgs sent

Usage Guidelines

This command requires the loadbalance, inspect, NAT, connection, or SSL feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To display the statistics for a specific probe type (for example, scripted), include the **type** *probe_type* keyword and argument.

Examples

To display all of the statistics about the ACE operation, enter:

```
host1/Admin# show stats
```

Related Commands

clear stats

show sticky cookie-insert group

To display the inserted cookie information for the specified sticky group, use the **show sticky cookie-insert group** command.

show sticky cookie-insert group *sticky_group_name*

Syntax Description

	The name of the configured sticky group
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A3(2.2)	This command was introduced.

Usage Guidelines

This command requires the sticky feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

This command displays information that correlates the inserted cookie, the sticky entry, and the final destination for the cookie insert configuration. For information about the fields in the **show sticky cookie-insert** command output, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To display the inserted cookie information for the sticky group, enter:

```
host1/Admin# show sticky cookie-insert group STICKY-TEST
```

Related Commands

(config-sticky-cookie) cookie insert

show sticky database

To display the sticky statistics, use the **show sticky database** command.

show sticky database [**static**] [**client** *ip_address* | **group** *name1* | **http-content** *value1* | **http-cookie** *value2* | **http-header** *value3* | **layer4-payload** *value4* | **rserver** *name2* [*port*] **serverfarm** *name3* | **rtsp-header** *value5* | **sip-header** *value6* | **type** {**http-cookie** | **http-header** | **ip-netmask** {**both** | **destination** | **source**} | **radius** {**calling-id** | **framed-ip** | **username**}}]

Syntax Description

static	(Optional) Displays static sticky database entries. If you do not use an optional keyword to specify the type of static sticky database entry to display, all entries are displayed.
client *ip_address*	(Optional) Displays sticky database entries for the source IP address of a client that you specify.
group *name1*	(Optional) Displays sticky database entries for the sticky group name that you specify.
http-content *value1*	(Optional) Displays sticky database entries for the HTTP content value that you specify.
http-cookie *value2*	(Optional) Displays sticky database entries for the HTTP cookie value that you specify.
http-header *value3*	(Optional) Displays sticky database entries for the HTTP header value that you specify.
layer4-payload *value4*	(Optional) Displays sticky database entries for the Layer 4 payload value that you specify.
rserver *name2*	(Optional) Displays sticky database entries for the real-server name that you specify.
port	(Optional) Real server port number.
serverfarm *name3*	Specifies a server farm associated with the real server.
rtsp-header *value5*	(Optional) Displays sticky database entries for the RTSP header value that you specify.
sip-header *value6*	(Optional) Displays sticky database entries for the SIP header value that you specify.
type	(Optional) Displays sticky database entries for one of the following sticky group types:
http-content	Specifies HTTP content sticky database entries.
http-cookie	Specifies HTTP cookie sticky database entries.
http-header	Specifies HTTP header sticky database entries.
ip-netmask	Specifies IP netmask sticky database entries.
both	Specifies both source and destination IP netmasks.
destination	Specifies the destination IP netmask.
source	Specifies the source IP netmask.
radius	Specifies RADIUS attribute sticky database entries.
calling-id	Specifies RADIUS calling-ID attribute sticky database entries.
framed-ip	Specifies RADIUS framed-IP attribute sticky database entries.
username	Specifies RADIUS username attribute sticky database entries.
rtsp-header	Specifies RTSP header sticky database entries.
sip-header	Specifies SIP header sticky database entries.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised.
A3(2.2)	When you enable cookie insertion through the **cookie insert** command in sticky-cookie configuration mode, the **show sticky database static http-cookie** command no longer displays the hash key.

Usage Guidelines

This command requires the sticky feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show sticky** command output, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To display sticky statistics for the client with a source IP address of 192.168.12.15, enter:

```
host1/Admin# show sticky database client 192.168.12.15
```

Related Commands

(config-sfarm-host-rs) cookie-string

show syn-cookie

To display SYN cookie statistics, use the **show syn-cookie** command. To display SYN cookie statistics for all VLANs that are configured in the current context, enter the command with no arguments.

show syn-cookie [**vlan** *number*]

Syntax Description

vlan *number*	Instructs the ACE to display SYN cookie statistics for the specified interface. Enter an integer from 2 to 2024.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To display SYN cookie statistics for VLAN 100, enter:

```
host1/C1# show syn-cookie vlan 100
```

Related Commands

clear syn-cookie

show system

To display the ACE system information, use the **show system** command.

show system {**cpuhog**} | {**error-id** {*hex_id* | **list**} | **internal** {**aaa** {**event-history** {**errors** | **msgs**} | **mem-stats**} | **log** {**boot** {**kickstart** | **system**} | **install** [**details**]} | **mts** {**buffers** [**age** *seconds* | **details** | **node** *name* | **order** | **sap** *number* | **summary**] | **memory** | **opcode**} | **radius event-history** {**errors** | **msgs**} | **sysmgr** {**event-history** {**errors** | **msgs**} | **service** {**all** [**detail**] | **local** [**detail**] | **name** *service_name* [**dependencies** | **policies** | **seqnotbl**] | **not-running** [**details**] | **pid** *id* [**config** | **dependencies** | **log**] | **running** [**details**] | **uuid** *hex_id* [**config** | **dependencies**]} | **startup-config** {**locks** | **state**} | **state** | **time**} | **tacacs+ event-history** {**errors** | **msgs**} | **urifs** | **vshd** {**config-intro** | **feature-list** | **license-info** | **log** {**running-config** | **tree-table**} | **subtype-table** | **tree-table**}} | **kcache** | **kmem** | **kmemtrack** | **resources** | **skbtrack** | **uptime**} [|] [>]

Syntax Description

cpuhog	Displays the largest amount of time that a driver was executing in the kernel. This keyword is intended for use by trained Cisco personnel for troubleshooting purposes only.
error-id	Displays description about errors. This keyword is available in all user contexts.
hex_id	Error ID in hexadecimal format. The range is from 0x0 to 0xffffffff.
list	Specifies all error IDs.
internal	Displays Cisco internal system-related functions. The **internal** keywords and related keywords, options, and arguments are intended for use by trained Cisco personnel for troubleshooting purposes only. This option is available in the Admin context only.
kcache	Displays Linux kernel cache statistics.
kmem	Displays Linux kernel memory statistics.
kmemtrack	Displays how the kernel memory is being currently used. This keyword is intended for use by trained Cisco personnel for troubleshooting purposes only.
resources	Displays system-related CPU and memory statistics.
skbtrack	Displays the allocation and deallocation of network buffers in the drivers. This keyword is intended for use by trained Cisco personnel for troubleshooting purposes only.
uptime	Displays how long the ACE has been up and running. This keyword is available in all user contexts.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin context

User contexts (**error-id** and **uptime** keywords only)

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show system** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display system resource information, enter:

```
host1/Admin# show system resources
```

Related Commands

This command has no related commands.

show tacacs-server

To display the configured Terminal Access Controller Access Control System Plus (TACACS+) server and server group parameters, use the **show tacacs-server** command.

show tacacs-server [**groups** | **sorted**] [|] [>]

Syntax Description

groups	(Optional) Displays configured TACACS+ server group information.
sorted	(Optional) Displays TACACS+ server information sorted by name.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show tacacs-server** command output, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

Examples

To display the configured TACACS+ server parameters, enter:

```
host1/Admin# show tacacs-server
```

To display the configured TACACS+ server groups, enter:

```
host1/Admin# show tacacs-server groups
```

To display the sorted TACACS+ servers, enter:

```
host1/Admin# show tacacs-server sorted
```

Related Commands

(config) aaa group server
(config) tacacs-server deadtime
(config) tacacs-server host
(config) tacacs-server key
(config) radius-server timeout

show tcp statistics

To display the Transmission Control Protocol (TCP) statistics, use the **show tcp statistics** command.

show tcp statistics [|] [>]

Syntax Description

|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the connection feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show tcp statistics** command output, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

Examples

To display TCP statistics, enter:

```
host1/Admin# show tcp statistics
```

Related Commands

clear tcp statistics

show tech-support

To display information that is useful to technical support when reporting a problem with your ACE, use the **show tech-support** command.

show tech-support [**details**] [|] [>]

Syntax Description

details	(Optional) Provides detailed information for each of the **show** commands described below in the "Usage Guidelines" section.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(2.2)	This command no longer displays the following: • All **show acl-merge acls vlan** command output • All **show acl-merge merge-list vlan** *number* **out** command output It also now displays a maximum of four VLANs.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The **show tech-support** command is useful when collecting a large amount of information about your ACE for troubleshooting purposes with Cisco technical support. The output of this command can be provided to technical support representatives when reporting a problem.

The **show tech-support** command displays the output of several **show** commands at once. The output from this command varies depending on your configuration. The default output of the **show tech-support** command includes the output of the following commands:

- **show hardware**—See the **show hardware** command.
- **show interface**—See the **show interface** command.
- **show process**—See the **show processes** command.
- **show running-config**—See the **show running-config** command.
- **show version**—See the **show version** command.

Explicitly set the terminal length command to 0 (zero) to disable autoscrolling and enable manual scrolling. Use the **show terminal** command to view the configured terminal size. After obtaining the output of this command, reset your terminal length as required.

You can save the output of this command to a file by appending > *filename* to the **show tech-support** command. If you save this file, verify that you have sufficient space to do so as each of these files may take about 1.8 MB.

For information about the fields in the **show tech-support** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display the summary version of the technical support report, enter:

```
host1/Admin# show tech-support
```

Related Commands

show fifo
show hardware
show interface
show processes
show running-config
show terminal
show version

show telnet

To display the information about the Telnet session, use the **show telnet** command.

show telnet [**maxsessions**] [*context_name*] [|] [**>**]

Syntax Description

maxsessions	(Optional) Displays the maximum number of enabled Telnet sessions.
context_name	(Optional) Name of an existing context. Use the *context_name* argument to display Telnet information that pertains only to the specified context. The *context_name* argument is case sensitive.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

If you do not include the optional **maxsessions** keyword, the ACE displays the following Telnet information:

- Session ID—Unique session identifier for the Telnet session
- Remote host—IP address and port of the remote Telnet client
- Active time—Time since the Telnet connection request was received by the ACE

For information about the fields in the **show telnet** command output, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

Examples

To display the current Telnet information, enter:

```
host1/Admin# show telnet
```

Related Commands

clear telnet
telnet
(config) class-map

show terminal

To display the console terminal settings, use the **show terminal** command.

show terminal [**internal info**] [|] [>]

Syntax Description

internal info	(Optional) Displays terminal internal information.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show terminal** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display the console terminal settings, enter:

```
host1/Admin# show terminal
```

Related Commands

terminal

show udp statistics

To display the User Datagram Protocol (UDP) statistics, use the **show udp statistics** command.

show udp statistics [|] [>]

Syntax Description

|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the connection feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show udp statistics** command output, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

Examples

To display UDP statistics, enter:

```
host1/Admin# show udp statistics
```

Related Commands

clear udp statistics

show user-account

To display user account information, use the **show user-account** command.

show user-account [*user_name*] [|] [**>**]

Syntax Description

user_name	(Optional) Name of user.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To display the user account information for all users, do not specify a user with the optional *user_name* argument.

For information about the fields in the **show user-account** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display the account information for all users, enter:

```
host1/Admin# show user-account
```

Related Commands

show users
(config) username

show users

To display the information for users that are currently logged in to the ACE, use the **show users** command.

show users [*user_name*] [|] [>]

Syntax Description

user_name	(Optional) Name of user.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To display the information for all users that are currently logged in to the ACE, do not specify a user with the optional *user_name* argument.

For information about the fields in the **show users** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display information for all users that are currently logged in to the ACE, enter:

```
host1/Admin# show users
```

Related Commands

clear user
show user-account
(config) username

show version

To display the version information of system software that is loaded in flash memory and currently running on the ACE, use the **show version** command.

show version[|] [>]

Syntax Description

|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The **show version** command also displays information related to the following ACE hardware components:

- CPU—Number of CPUs and type and model
- Memory—Total and shared volatile memory
- Flash memory—Total and used flash memory

Use the **show version** command to verify the software version on the ACE before and after an upgrade.

For information about the fields in the **show version** command output, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To display the software version information, enter:

```
host1/Admin# show version
```

Related Commands

show tech-support

show vlans

To display the VLANs on the ACE, use the **show vlans** command.

show vlans [|] [>]

Syntax Description

|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the interface feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show vlans** command output, see the *Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*.

Examples

To display the VLANs on the ACE, enter:

```
host1/Admin# show vlans
```

Related Commands

This command has no related commands.

show vnet

To display information about the virtual network (VNET) device, use the **show vnet** command.

show vnet {**event-history** | **stats**} [|] [>]

Syntax Description

event-history	Displays a historic log of the most recent debug VNET messages.
stats	Displays detailed counters for various VNET events.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

This command is intended for use by trained Cisco personnel for troubleshooting purposes only.

Examples

To display VNET device statistics for the control plane, enter:

```
host1/Admin# show vnet stats
```

Related Commands

clear vnet stats

show xlate

To display information about the IP and port translation (XLATE), use the **show xlate** command.

show xlate [**global** {*ip_address1* [*ip_address2* [**netmask** *mask1*]]}] [**local** {*ip_address3* [*ip_address4* [**netmask** *mask2*]]}] [**gport** *port1* [*port2*]] [**lport** *port1* [*port2*]] [|] [**>**]

Syntax Description

global *ip_address1* *ip_address2*	(Optional) Displays information for a global IP address or a range of global IP addresses to which the ACE translates source addresses for static and dynamic NAT. For a single global IP address, enter the address in dotted-decimal notation (for example, 192.168.12.15). To specify a range of IP addresses, enter a second IP address.
netmask *mask*	(Optional) Specifies a subnet mask for the specified IP addresses.
local *ip_address3* *ip_address4*	(Optional) Displays information for a local IP address or a range of local IP addresses. For a single local IP address, enter the address in dotted-decimal notation (for example, 192.168.12.15). To specify a range of local IP addresses, enter a second IP address.
gport *port1* *port2*	(Optional) Displays information for a global port or a range of global ports to which the ACE translates source ports for static port redirection and dynamic PAT. Enter a port number as an integer from 0 to 65535. To specify a range of port numbers, enter a second port number.
lport *port1* *port2*	(Optional) Displays information for a local port or a range of local ports. Enter a port number as an integer from 0 to 65535. To specify a range of port numbers, enter a second port number.
|	(Optional) Pipe character (|) for enabling an output modifier that filters the command output. For a complete description of the options available for filtering the command output, see the **show** command.
>	(Optional) Greater-than character (>) for enabling an output modifier that redirects the command output to a file. For a complete description of the options available for redirecting the command output, see the **show** command.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the NAT feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the fields in the **show xlate** command output, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

Examples

To display IP and XLATE information, enter:

```
host1/Admin# show xlate global 172.27.16.3 172.27.16.10 netmask 255.255.255.0 gport 100
200
```

Related Commands

clear xlate

ssh

To initiate a Secure Shell (SSH) session with another device, use the **ssh** command.

ssh {*hostname* | *user@hostname*}

Syntax Description

hostname	Name or IP address of the host to access. If no username is specified, the default is "admin." Enter up to 64 alphanumeric characters.
user	Username on a host.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To initiate an SSH session with the host 196.168.12.10, enter:

```
host1/Admin# ssh 196.168.12.10
```

To initiate an SSH session with USER1 on HOST1, enter:

```
host1/Admin# ssh USER1@HOST1
```

Related Commands

clear ssh
show ssh
(config) class-map
(config) login timeout
(config) ssh key
(config) ssh maxsessions

system internal

To generate a debug snapshot of a service, use the **system internal** command.

system internal snapshot service {*name*}

Syntax Description

snapshot service	Specifies debug snapshots of a service.
name	Name of a system service for which you want to take a snapshot. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Exec

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin role in the Admin context. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

This command is intended for use by trained Cisco personnel for troubleshooting purposes only.

Examples

To take a snapshot of a service, enter:

```
host1/Admin# system internal snapshot service
```

Related Commands

This command has no related commands.

tac-pac

To save Technical Assistance Center (TAC) information to a local or remote location, use the **tac-pac** command.

tac-pac [**ftp://***server*/*path*[/*filename*] | **scp://***server*/*path*[/*filename*] | **sftp://**[*username*@]*server*/*path*[/*filename*] | **tftp://***server*[**:***port*]/*path*[/*filename*] | **disk0:**[*path*/]*filename*]

Syntax Description

ftp:	(Optional) Specifies the File Transfer Protocol network server as the destination.
scp:	(Optional) Specifies the Secure Copy network server as the destination.
sftp:	(Optional) Specifies the Secure File Transfer Protocol network server as the destination.
tftp:	(Optional) Specifies the Trivial File Transfer Protocol network server as the destination.
disk0:	(Optional) Specifies the disk0: file system in flash memory on the ACE as the destination.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The TAC information that the ACE saves when using the **tac-pac** command is the same information that you can display using the **show tech-support** command.

If you do not specify a directory on a file system, the default is the root directory.

The output of the **show tech-support** command is in gzip format. We recommend that you include the .gz extension in the filename so that it can be easily unzipped from the destination filesystem.

Examples

To save TAC information and send the output of the **show tech-support** command to a remote FTP server, enter:

```
host1/Admin# tac-pac ftp://192.168.1.2/tac-output_10-7-07.gz
```

Related Commands

This command has no related commands.

telnet

To initiate a Telnet session with another network device, use the **telnet** command.

telnet *ip_address* [*port*]

Syntax Description

ip_address	IP address of the network host. Enter an IP address in dotted-decimal notation (for example, 172.16.1.10).
port	(Optional) Port number on network host. The range is from 0 to 2147483647.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To open a Telnet session with another network device, enter:

```
host1/Admin# telnet 192.126.2.1
```

Related Commands

clear telnet
show telnet
(config) class-map
(config) login timeout

terminal

To configure the terminal display settings, use the **terminal** command.

terminal {**length** *lines* | **monitor** | **no** | **session-timeout** *minutes* | **terminal-type** *text* | **width** *characters*}

Syntax Description

length *lines*	Sets the number of lines displayed on the current terminal screen. This command is specific to the console port only. Telnet and Secure Shell (SSH) sessions set the length automatically. Valid entries are from 0 to 511. The default is 24 lines. A value of 0 instructs the ACE to scroll continuously (no pausing) and overrides the **terminal width** command.
monitor	Displays the syslog output on the terminal for the current terminal and session. To enable the various levels of syslog messages to the terminal, use the **logging monitor** command in configuration command mode.
no	Negates a command or sets it back to its default value.
session-timeout *minutes*	Specifies the session timeout value in minutes to configure the automatic logout time for the current terminal session on the ACE. When you exceed the time limit configured by this command, the ACE closes the session and exits. The range is 0 to 525600. The default is 5 minutes. You can set the **terminal session-timeout** value to 0 to disable this feature so that the terminal remains active until you choose to exit the ACE. The ACE does not save this change in the configuration file.
terminal-type *text*	Specifies the name and type of the terminal used to access the ACE. If a Telnet or SSH session specifies an unknown terminal type, the ACE uses the VT100 terminal by default. Specify a text string from 1 to 80 alphanumeric characters.
width *characters*	Sets the number of characters displayed on the current terminal screen. This command is specific to only the console port. Telnet and SSH sessions set the width automatically. Valid entries are from 24 to 512. The default is 80 columns.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Use the **show terminal** command to display the current terminal settings.

All terminal parameter-setting commands are set locally and do not remain in effect after you end a session. You must perform this task at the Exec prompt at each session to see the debugging messages.

Examples

To specify the VT100 terminal, set the number of screen lines to 35, and set the number of characters to 250, enter:

```
host1/Admin# terminal terminal-type vt220
host1/Admin# terminal length 35
host1/Admin# terminal width 250
```

To specify a terminal timeout of 600 minutes for the current session, enter

```
host1/Admin# terminal session-timeout 600
```

To set the width to 100 columns, enter:

```
host1/Admin# terminal width 100
```

To set the width to its default of 80 columns, enter:

```
host1/Admin# terminal no width
```

To start the current terminal monitoring session, enter:

```
host1/Admin# terminal monitor
```

To stop the current terminal monitoring session, enter:

```
host1/Admin# terminal no monitor
```

Related Commands

show terminal
(config) login timeout

traceroute

To trace the route that an IP packet takes to a network host from the ACE, use the **traceroute** command.

traceroute [*ip_address* [**size** *packet*]]

Syntax Description

ip_address	(Optional) IP address of the network host. Enter an IP address in dotted-decimal notation (for example, 172.27.16.10).
size *packet*	(Optional) Specifies the packet size. Enter a number from 40 to 452. The default is 40.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

This command traces the route that an IP packet follows to an Internet host by launching User Datagram Protocol (UDP) probe packets with a small time to live (TTL), and then listening for an Internet Control Message Protocol (ICMP) "time exceeded" reply from a gateway.

Examples

To display the route that a packet takes from the ACE to a network host with the IP address 196.126.1.2, enter:

```
host1/Admin# traceroute 196.126.1.2
```

Related Commands

ping

undebug all

To disable all debugging, use the **undebug all** command.

undebug all

Syntax Description

This command has no keywords or arguments.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command is available to all user roles that allow debugging and is not available to network monitor or technician users. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The ACE **debug** commands are intended for use by trained Cisco personnel only. Entering these commands may cause unexpected results. Do not attempt to use these commands without guidance from Cisco support personnel.

Examples

To disable all debugging, enter:

```
host1/Admin# undebug all
```

Related Commands debug

untar disk0:

To untar a single file with a .tar extension in the disk0: file system, use the **untar** command.

untar disk0:[*path*/]*filename*

Syntax Description

[*path*/]*filename*	Name of the .tar file on the disk0: file system. The filename must end with a .tar extension.

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The **copy licenses disk0:** command creates backup .tar license files on the ACE. If a license becomes corrupted or lost, or you accidently remove the license on the ACE, you can untar the license and reinstall it.

You must use the **untar** command in the Admin context to untar a backup tar license file.

Examples

To untar the mylicense.tar file on disk0, enter:

```
host1/Admin# untar disk0:mylicenses.tar
```

Related Commands

copy licenses
gunzip

write

To manage persistent and nonpersistent configuration information, use the **write** command.

write {**erase** | **memory** [**all**] | **terminal**}

Syntax Description

erase	Erases the entire startup configuration with the exception of any configuration that affects the loader functionality. The startup configuration then reverts back to the factory-default values. The running configuration is not affected.
memory	Writes the running configuration to the startup configuration.
all	(Optional) Writes configurations for all existing contexts. This keyword is available only in the Admin context.
terminal	Writes the running configuration to the terminal.

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The different versions of this command require the following user role or feature in your user role:

- **write erase**—Admin user
- **write memory**—config-copy feature
- **write all**—Admin user

The **write erase** command does not remove license files or crypto files (certs and keys) from the ACE. To remove license files, see the **license uninstall** command. To remove crypto files, see the **crypto delete** command.

If you intend to use the **write memory** command to save the contents of the running-configuration file for the current context to the startup-configuration file, you must also specify this command in the Admin context. Saving changes to the Admin context startup-configuration file is important because the Admin context startup-configuration file contains all configurations that are used to create each user context.

To write the running configuration to the startup configuration, you can also use the **copy running-config startup-config** command. To erase the startup configuration, you can also use the **clear startup-config** command. To display the running configuration, use the **show running-config** command.

Examples

To write running configuration to the startup configuration, enter:

```
host1/Admin# write memory
```

Related Commands

clear startup-config
show running-config

xml-show

To enable the display of raw XML request **show** command output in XML format, use the **xml-show** command.

xml show {**off** | **on** | **status**}

Syntax Description

off	Displays CLI **show** command output in regular CLI display output, not in XML format.
on	Displays CLI **show** command output in XML format unless a specific **show** command is not implemented to display its output in XML format.
status	Displays the current setting of the **xml-show** command (**on** or **off**).

Command Modes

Exec

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

By default, XML responses will automatically appear in XML format if the corresponding CLI **show** command output supports the XML format. However, if you are running commands on the CLI console or you are running raw XML responses from NMS, the XML responses appear in regular CLI display format.

You can enable the display of raw XML request **show** command output in XML format by performing one of the following actions:

- Specifying the **xml-show on** command in Exec mode from the CLI, or
- Including the **xml-show on** command in the raw XML request itself (CLI commands included in an XML wrapper).

Specification of the **xml-show on** command is not required if you are running true XML.

For details on the **show** command output supported in XML format, consult the ACE DTD file, ace_appliance.dtd, that is included as part of the software image (see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*). The ACE DTD File contains the information on the XML attributes for those **show** output commands that support XML format.

The **off** and **on** keywords affect only the current CLI session in use; they are session-based functions.

Examples To enable the display of raw XML request **show** command output in XML format from the CLI, enter:

```
host1/Admin# xml-show on
```

Related Commands This command has no related commands.

Configuration Mode Commands

Configuration mode commands allow you to configure global ACE parameters that affect the following contexts:

- All contexts, when configured in the Admin context
- A single user context, when configured in that context

Configuration mode also allows you to access all the ACE subordinate configuration modes. These modes provide parameters to configure the major features of the ACE, including access control lists (ACLs), application protocol inspection, fragmentation and reassembly, interfaces, Network Address Translation (NAT), persistence (stickiness), protocols, redundancy, routing, scripts, Secure Sockets Layer (SSL), server load balancing (SLB), TCP/IP normalization, users, and virtualization.

To access configuration mode, use the **config** command. The CLI prompt changes to (config).

See the individual command descriptions of all the configuration mode commands on the following pages.

Command Modes

Exec mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires one or more features assigned to your user role that allow configuration, such as AAA, interface, or fault-tolerant. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To access configuration mode, enter:

```
host1/Admin# config
host1/Admin(config)#
```

Related Commands

show running-config
show startup-config

(config) aaa accounting default

To configure the default accounting method, use the **aaa accounting default** command. You specify either a previously created AAA server group that identifies separate groups of Terminal Access Controller Access Control System Plus (TACACS+) or Remote Authentication Dial-In User Service (RADIUS) servers or the local database on the ACE. Use the **no** form of this command to remove the accounting method.

aaa accounting default {**group** *group_name*} {**local**} {**none**}

no aaa accounting default {**group** *group_name*} {**local**} {**none**}

Syntax Description

group *group_name*	Associates the accounting method with a TACACS+ or RADIUS server defined previously through the **aaa group server** command. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
local	Specifies to use the local database on the ACE as the accounting method.
none	Specifies that the ACE does not perform password verification, which disables password verification. If you configure this option, users can log in without providing a valid password. **Note** Only users with an Admin role can configure the **none** keyword.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To enable user accounting to be performed using remote TACACS+ servers, followed by local login as the fallback method, enter:

```
host1/Admin(config)# aaa accounting default group TacServer local
```

Related Commands

show aaa
show accounting log
(config) aaa authentication login
(config) aaa group server

(config) aaa authentication login

To configure the authentication method used for login to the ACE CLI, use the **aaa authentication login** command. Use the **no** form of this command to disable the authentication method.

aaa authentication login {{**console** | **default**} {{**group** *group_name*} {**local**} {**none**}}} | **error-enable**

no aaa authentication login {{**console** | **default**} {{**group** *group_name*} {**local**} {**none**}}} | **error-enable**

Syntax Description

console	Specifies the console port login authentication method, identified by the specified server group.
default	Specifies the default login authentication method (by console or by Telnet or Secure Shell [SSH] session) that is identified by the specified server group.
group *group_name*	Associates the login authentication process with a Terminal Access Controller Access Control System Plus (TACACS+), Remote Authentication Dial-In User Service (RADIUS), or Lightweight Directory Access Protocol (LDAP) server defined through the **aaa group server** command. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
local	Specifies to use the local database on the ACE as the login authentication method. If the server does not respond, then the local database is used as the fallback authentication method.
none	Specifies that the ACE does not perform password verification. If you configure this option, users can log in to the ACE without providing a valid password. **Note** Only users with an Admin role can configure the **none** keyword.
error-enable	Enables the display of the login error message when the remote AAA servers fail to respond.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Use the **error-enable** option cautiously. If you specify **none**, any user will be able to access the ACE at any time.

To view the current display status, use the **show aaa authentication login error-enable** command. When a user attempts to log in, and the remote AAA servers do not respond to the authentication request, the ACE processes the login sequence by switching to local user database.

Examples

To enable console authentication using the TACSERVER server group, followed by local login as the fallback method, enter:

```
host1/Admin(config)# aaa authentication login console group TACSERVER local
```

Password verification remains enabled for login authentication.

To turn off password validation, enter:

```
host1/Admin(config)# aaa authentication login console group TACSERVER local none
```

Related Commands

show aaa
(config) aaa accounting default
(config) aaa group server

(config) aaa group server

To configure independent server groups of Terminal Access Controller Access Control System Plus (TACACS+), Remote Authentication Dial-In User Service (RADIUS), or Lightweight Directory Access Protocol (LDAP) servers, use the **aaa group server** command. Use the **no** form of this command to remove a server group.

aaa group server {**ldap** | **radius** | **tacacs+**} *group_name*

no aaa group server {**ldap** | **radius** | **tacacs+**} *group_name*

Syntax Description

ldap	Specifies an LDAP directory server group. For information about the commands in the LDAP server configuration mode, see the "LDAP Configuration Mode Commands" section.
radius	Specifies a RADIUS server group. For information about the commands in the RADIUS server configuration mode, see the "RADIUS Configuration Mode Commands" section.
tacacs+	Specifies a TACACS+ server group. For information about the commands in the TACACS+ server configuration mode, see the "TACACS+ Configuration Mode Commands" section.
group_name	Name for the LDAP, RADIUS, or TACACS+ server group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

A server group is a list of server hosts of a particular type. The ACE allows you to configure multiple TACACS+, RADIUS, and LDAP servers as a named server group. You group the different AAA server hosts into distinct lists. The ACE searches for the server hosts in the order in which you specify them within a group. You can configure a maximum of 10 server groups for each context in the ACE.

You can configure server groups at any time, but they take effect only when you apply them to the AAA service using the **aaa authentication login** or the **aaa accounting default** commands.

To create a AAA server group and access one of the three AAA server group configuration modes, enter the **aaa group server ldap**, **aaa group server radius**, or **aaa group server tacacs+** command in configuration mode. The CLI prompt changes to (config-ldap), (config-radius), or (config-tacacs+). In this mode, you specify the IP address of one or more previously configured servers that you want added to or removed from the server group.

Examples

To create a RADIUS server group and add a previously configured RADIUS server, enter:

```
(config)# aaa group server radius RAD_Server_Group1
host1/Admin(config-radius)# server 192.168.252.1
host1/Admin(config-radius)# server 192.168.252.2
host1/Admin(config-radius)# server 192.168.252.3
```

Related Commands

show aaa
show running-config
(config) aaa accounting default
(config) aaa authentication login

(config) access-group

To apply an access control list (ACL) to the inbound direction on all VLAN interfaces in a context and make the ACL active, use the **access-group** command. Use the **no** form of this command to remove an ACL from all interfaces in a context.

access-group input *acl_name*

no access-group input *acl_name*

Syntax Description

input	Specifies the inbound direction of all interfaces in a context on which you want to apply the ACL
acl_name	Identifier of an existing ACL that you want to apply to an interface

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the access-list feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You must apply an ACL to an interface to allow the passing of traffic on that interface. This command enables you to apply an ACL to all interfaces in a context in the inbound direction only and to allow traffic on all interfaces simultaneously. The following considerations apply:

- You can use the **access-group** command in configuration mode only if there are no interfaces in the context to which you have applied an ACL previously using the **(config-if) access-group** command in interface configuration mode.
- If you have applied an ACL globally to all interfaces in a context, you cannot apply an ACL to an individual interface using the **(config-if) access-group** command in interface configuration mode.
- You can apply one Layer 2 ACL and one Layer 3 ACL globally to all interfaces in a context.
- You can apply both a Layer 3 and a Layer 2 ACL to all Layer 2 bridge-group virtual interfaces (BVIs) in a context.
- You can apply only a Layer 3 ACL to all Layer 3 virtual LANs (VLANs) in a context.

For complete details on ACLs, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

Examples

To apply an ACL named INBOUND to the inbound direction of all interfaces in the Admin context, enter:

```
host1/Admin(config)# access-group input INBOUND
```

To remove an ACL from all interfaces in the Admin context, enter:

```
host1/Admin(config)# no access-group input INBOUND
```

Related Commands

(config-if) access-group
show access-list

(config) access-list ethertype

To configure an EtherType access control list (ACL), use the **access-list ethertype** command. Use the **no** form of this command to remove the ACL from the configuration.

access-list *name* **ethertype** {**deny** | **permit**} {**any** | **bpdu** | **ipv6** | **mpls**}

no access-list *name* **ethertype** {**deny** | **permit**} {**any** | **bpdu** | **ipv6** | **mpls**}

Syntax Description

name	Unique identifier of the ACL. Enter an unquoted text string with a maximum of 64 alphanumeric characters.
ethertype	Specifies a subprotocol of type: **any**, **bpdu**, **ipv6**, or **mpls**.
deny	Blocks connections on the assigned interface.
permit	Allows connections on the assigned interface.
any	Specifies any EtherType.
bpdu	Specifies bridge protocol data units.
ipv6	Specifies Internet Protocol version 6.
mpls	Specifies Multiprotocol Label Switching.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the access-list feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can configure an ACL that controls traffic based on its EtherType. An EtherType is a subprotocol identifier. EtherType ACLs support Ethernet V2 frames. EtherType ACLs do not support 802.3-formatted frames because they use a length field instead of a type field. Bridge protocol data units (BPDUs) are exceptions because they are SNAP-encapsulated, and the ACE is designed to specifically handle BPDUs.

You can configure an EtherType ACL only on a Layer 2 interface in the inbound direction.

When you specify the **mpls** keyword in an EtherType ACL, the ACE denies or permits both MPLS-unicast and MPLS-multicast traffic.

Examples

To configure an ACL that controls traffic based on its EtherType, enter:

```
(config)#  access-list INBOUND ethertype permit mpls
```

Related Commands

clear access-list
show access-list

(config) access-list extended

To create an extended ACL, use the **access-list extended** command. The two major types of extended ACLs are as follows:

- Non-ICMP ACLs
- ICMP ACLs

Use the **no** form of this command to delete the ACL.

For a non-ICMP extended ACL, the syntax is as follows:

access-list *name* [**line** *number*] **extended** {**deny** | **permit**}
{*protocol* {**any** | **host** *src_ip_address* | *src_ip_address netmask* | **object-group** *net_obj_grp_name*} [*operator port1* [*port2*]] {**any** | **host** *dest_ip_address* | *dest_ip_address netmask* | **object-group** *net_obj_grp_name*} [*operator port3* [*port4*]]}
|{**object-group** *service_obj_grp_name*} {**any** | **host** *src_ip_address* | *src_ip_address netmask* | **object-group** *net_obj_grp_name*} {**any** | **host** *dest_ip_address* | *dest_ip_address netmask* | **object-group** *net_obj_grp_name*}

no access-list *name* [**line** *number*] **extended** {**deny** | **permit**}
{*protocol* {**any** | **host** *src_ip_address* | *src_ip_address netmask* | **object-group** *net_obj_grp_name*} [*operator port1* [*port2*]] {**any** | **host** *dest_ip_address* | *dest_ip_address netmask* | **object-group** *net_obj_grp_name*} [*operator port3* [*port4*]]}
|{**object-group** *service_obj_grp_name*} {**any** | **host** *src_ip_address* | *src_ip_address netmask* | **object-group** *net_obj_grp_name*} {**any** | **host** *dest_ip_address* | *dest_ip_address netmask* | **object-group** *net_obj_grp_name*}

For an ICMP-extended ACL, the syntax is as follows:

access-list *name* [**line** *number*] **extended** {**deny** | **permit**}
{**icmp** {**any** | **host** *src_ip_address* | *src_ip_address netmask* | **object_group** *net_obj_grp_name*} {**any** | **host** *dest_ip_address* | *dest_ip_address netmask* | **object_group** *network_grp_name*} [*icmp_type* [**code** *operator code1* [*code2*]]]}
|{**object-group** *service_obj_grp_name*} {**any** | **host** *src_ip_address* | *src_ip_address netmask* | **object-group** *net_obj_grp_name*} {**any** | **host** *dest_ip_address* | *dest_ip_address netmask* | **object-group** *net_obj_grp_name*}

no access-list *name* [**line** *number*] **extended** {**deny** | **permit**}
{**icmp** {**any** | **host** *src_ip_address* | *src_ip_address netmask* | **object_group** *net_obj_grp_name*} {**any** | **host** *dest_ip_address* | *dest_ip_address netmask* | **object_group** *network_obj_grp_name*} [*icmp_type* [**code** *operator code1* [*code2*]]]}
|{**object-group** *service_obj_grp_name*} {**any** | **host** *src_ip_address* | *src_ip_address netmask* | **object-group** *net_obj_grp_name*} {**any** | **host** *dest_ip_address* | *dest_ip_address netmask* | **object-group** *net_obj_grp_name*}

Syntax Description

name	Unique identifier of the ACL. Enter an unquoted text string with a maximum of 64 alphanumeric characters.
line *number*	(Optional) Specifies the line number position where you want the entry that you are configuring to appear in the ACL. The position of an entry affects the lookup order of the entries in an ACL. If you do not configure the line number of an entry, the ACE applies a default increment and a line number to the entry and appends it at the end of the ACL.

extended	Specifies an extended ACL. Extended ACLs allow you to specify the destination IP address and subnet mask and other parameters not available with a standard ACL.
deny	Blocks connections on the assigned interface.
permit	Allows connections on the assigned interface.
protocol	Name or number of an IP protocol. Enter a protocol name or an integer from 0 to 255 that represents an IP protocol number from the following: • **ah**—(51) Authentication Header • **eigrp**—(88) Enhanced IGRP • **esp**—(50) Encapsulated Security Payload • **gre**—(47) Generic Routing Encapsulation • **icmp**—(1) Internet Control Message Protocol (See Table 2-1 for optional ICMP messaging types) • **igmp**—(2) Internet Group Management Protocol • **ip**—(0) Internet Protocol • **ip-in-ip**—(4) IP-in-IP Layer 3 tunneling protocol • **ospf**—(89) Open Shortest Path First • **pim**—(103) Protocol Independent Multicast • **tcp**—(6) Transmission Control Protocol • **udp**—(17) User Datagram Protocol
any	Specifies the network traffic from any source.
host *src_ip_address*	Specifies the IP address of the host from which network traffic originates. Use this keyword and argument to specify the network traffic from a single IP address.
src_ip_address netmask	Traffic from a source defined by the IP address and the network mask. Use these arguments to specify the network traffic from a range of source IP addresses.
object-group *network_obj_grp_name*	Specifies the identifier of an existing source network object group. To use object groups in an ACL, replace the normal network (*source_address, mask*, and so on), service (*protocol operator port*) or ICMP type (*icmp_type*) arguments with an **object-group** *name*.
operator	(Optional) Operand used to compare source and destination port numbers for TCP, TCP-UDP, and UDP protocols. The operators are as follows: • **eq**—Equal to. • **gt**—Greater than. • **lt**—Less than. • **neq**—Not equal to. • **range**—An inclusive range of port values. If you entered the **range** operator, enter a second port number value to define the upper limit of the range.
port1 [*port2*]	TCP or UDP source port name or number from which you permit or deny services access. Enter an integer from 0 to 65535. To enter an inclusive range of ports, enter two port numbers. *Port2* must be greater than or equal to *port1*. See Table 2-2 for a list of well-known TCP port names and numbers and Table 2-3 for a list of well-known UDP port names and numbers.

dest_ip_address netmask	Specifies the IP address of the network or host to which the packet is being sent and the network mask bits that are to be applied to the destination IP address. Use these arguments to specify a range of destination IP addresses.
any	Specifies the network traffic going to any destination.
host *destination_address*	Specifies the IP address and subnet mask of the destination of the packets in a flow. Use this keyword and argument to specify the network traffic destined to a single IP address.
operator	(Optional) Operand used to compare source and destination port numbers for TCP, TCP-UDP, and UDP protocols. The operators are as follows: • **lt**—Less than. • **gt**—Greater than. • **eq**—Equal to. • **neq**—Not equal to. • **range**—An inclusive range of port values. If you enter this operator, enter a second port number value to define the upper limit of the range.
port3 [*port4*]	TCP or UDP destination port name or number to which you permit or deny access to services. To enter an optional inclusive range of ports, enter two port numbers. *Port4* must be greater than or equal to *port3*. See Table 2-2 for a list of well-known ports.
icmp_type	(Optional) Type of ICMP messaging. Enter either an integer that corresponds to the ICMP code number or one of the ICMP types as described in Table 2-1.
code	(Optional) Specifies that a numeric operator and ICMP code follows.
operator	An operator that the ACE applies to the ICMP code number that follows. Enter one of the following operators: • **lt**—Less than. • **gt**—Greater than. • **eq**—Equal to. • **neq**—Not equal to. • **range**—An inclusive range of ICMP code values. When you use this operator, specify two code numbers to define the range.
code1, code2	ICMP code number that corresponds to an ICMP type. See Table 2-2. If you entered the **range** operator, enter a second ICMP code value to define the upper limit of the range.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised with the **object-group** keyword and associated keywords and arguments.

Usage Guidelines

This command requires the access-list feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The ACE does not explicitly support standard ACLs. To configure a standard ACL, specify the destination addresses as "any" and do not specify ports in an extended in an extended ACL.

For TCP and UDP connections, you do not need to also apply an ACL on the destination interface to allow returning traffic, because the ACE allows all returning traffic for established connections.

You can apply only one extended ACL to each direction (inbound or outbound) of an interface. You can also apply the same ACL on multiple interfaces.You can apply EtherType ACLs only in the inbound direction and only on Layer 2 interfaces.

If you create an ICMP extended ACL, you can optionally specify the type of ICMP messaging. Enter either an integer that corresponds to the ICMP code number or one of the ICMP messaging types as described in Table 2-1.

Table 2-1 ICMP Types

ICMP Code Number	ICMP Type
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
30	traceroute
31	conversion-error
32	mobile-redirect

Table 2-2 Well-Known TCP Port Numbers and Key Words

Keyword	Port Number	Description
aol	5190	America-Online
bgp	179	Border Gateway Protocol

Table 2-2 Well-Known TCP Port Numbers and Key Words (continued)

Keyword	Port Number	Description
chargen	19	Character Generator
citrix-ica	1494	Citrix Independent Computing Architecture protocol
cmd	514	Same as exec, with automatic authentication
ctiqbe	2748	Computer Telephony Interface Quick Buffer Encoding
daytime	13	Daytime
discard	9	Discard
domain	53	Domain Name System
echo	7	Echo
exec	512	Exec (RSH)
finger	79	Finger
ftp	21	File Transfer Protocol
ftp-data	20	FTP data connections
gopher	70	Gopher
hostname	101	NIC hostname server
http	80	Hyper Text Transfer Protocol
https	443	HTTP over TLS/SSL
ident	113	Ident Protocol
imap4	143	Internet Message Access Protocol, version 4
irc	194	Internet Relay Chat
kerberos	88	Kerberos
klogin	543	Kerberos Login
kshell	544	Kerberos Shell
ldap	389	Lightweight Directory Access Protocol
ldaps	636	LDAP over TLS/SSL
login	513	Login (rlogin)
lotusnotes	1352	IBM Lotus Notes
lpd	515	Printer Service
matip-a	350	Mapping of Airline Traffic over Internet Protocol (MATIP) Type A
netbios-ssn	139	NetBIOS Session Service
nntp	119	Network News Transport Protocol
pcanywhere-data	5631	PC Anywhere data
pim-auto-rp	496	PIM Auto-RP

Table 2-2 Well-Known TCP Port Numbers and Key Words (continued)

Keyword	Port Number	Description
pop2	109	Post Office Protocol v2
pop3	110	Post Office Protocol v3
pptp	1723	Point-to-Point Tunneling Protocol, RFC 2637
rtsp	554	Real Time Streaming Protocol
sip	5060	Session Initiation Protocol
skinny	2000	Cisco Skinny Client Control Protocol (SCCP)
smtp	25	Simple Mail Transfer Protocol
sqlnet	1521	Structured Query Language Network
ssh	22	Secure Shell
sunrpc	111	Sun Remote Procedure Call
tacacs	49	Terminal Access Controller Access Control System
talk	517	Talk
telnet	23	Telnet
time	37	Time
uucp	540	UNIX-to-UNIX Copy Program
whois	43	Nicname
www	80	World Wide Web (HTTP)

Table 2-3 Well-Known UDP Key Words and Port Numbers

Keyword	Port Number	Description
biff	512	Mail notification
bootpc	68	Bootstrap Protocol client
bootps	67	Bootstrap Protocol server
discard	9	Discard
dnsix	195	DNSIX Security protocol auditing (dn6-nlm-aud)
domain	53	Domain Name System
echo	7	Echo
isakmp	500	Internet Security Association Key Management Protocol
kerberos	88	Kerberos
mobile-ip	434	Mobile IP registration
nameserver	42	Host Name Server
netbios-dgm	138	NetBIOS datagram service

Table 2-3 Well-Known UDP Key Words and Port Numbers (continued)

Keyword	Port Number	Description
netbios-ns	137	NetBIOS name service
netbios-ssn	139	NetBIOS Session Service
ntp	123	Network Time Protocol
pcanywhere-status	5632	PC Anywhere status
radius	1812	Remote Authentication Dial-in User Service
radius-acct	1813	RADIUS Accounting
rip	520	Routing Information Protocol
snmp	161	Simple Network Management Protocol
snmptrap	162	SNMP Traps
sunrpc	111	Sun Remote Procedure Call
syslog	514	System Logger
tacacs	49	Terminal Access Controller Access Control System
talk	517	Talk
tftp	69	Trivial File Transfer Protocol
time	37	Time
who	513	Who service (rwho)
wsp	9200	Connectionless Wireless Session Protocol
wsp-wtls	9202	Secure Connectionless WSP
wsp-wtp	9201	Connection-based WSP
wsp-wtp-wtls	9203	Secure Connection-based WSP
xdmcp	177	X Display Manager Control Protocol

Examples

To configure a TCP extended ACL, enter:

```
host1/Admin(config)# access-list INBOUND line 10 extended permit tcp 192.168.12.0
255.255.255.0 gt 1024 172.27.16.0 255.255.255.0 lt 4000
```

To remove an entry from an extended ACL, enter:

```
host1/Admin(config)# no access-list INBOUND line 10
```

To allow an external host with IP address 192.168.12.5 to be able to ping a host behind the ACE with an IP address of 10.0.0.5, enter:

```
(config)#  access-list INBOUND extended permit icmp host 192.168.12.5 host 10.0.0.5 echo
code eq 0
```

To remove an entry from an ICMP ACL, enter:

```
(config)#  no access-list INBOUND extended permit icmp host 192.168.12.5 echo
```

To use object groups for all available parameters, enter:

```
ISM/Admin(config)# access-list acl_name extended {deny | permit} object-group
service_grp_name object-group network_grp_name object-group network_grp_name
```

Related Commands

clear access-list
show access-list

(config) access-list remark

You can add comments about an access control list (ACL) to clarify the function of the ACL. To add a comment to an ACL, use the **access-list remark** command. You can enter only one comment per ACL and the comment appears at the top of the ACL. Use the **no** form of this command to remove an ACL remark.

access-list *name* **remark** *text*

no access-list *name* **remark** *text*

Syntax Description

name	Unique identifier of the ACL. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
line *number*	(Optional) Specifies the line number position where you want the comments to appear in the ACL. If you do not specify a line number, the ACE applies a default increment and a line number to the remark and appends it at the end of the ACL.
remark *text*	Specifies any comments that you want to include about the ACL. Comments appear at the top of the ACL. Enter an unquoted text string with a maximum of 100 alphanumeric characters. You can enter leading spaces at the beginning of the text. Trailing spaces are ignored.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the access-list feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

If you delete an ACL using the **no access-list** *name* command, then the remarks are also removed.

Examples

To add an entry comment to an ACL, enter:

```
host1/Admin(config)# access-list INBOUND remark This is a remark
```

To remove entry comments from an ACL, enter:

```
(config)#  no access-list INBOUND line 200 remark
```

Related Commands

clear access-list
show access-list

(config) access-list resequence

To resequence the entries in an extended access control list (ACL) with a specific starting number and interval, use the **access-list resequence** command. Use the **no** form of this command to reset the number assigned to an ACL entry to the default of 10.

access-list *name* **resequence** *number1 number2*

no access-list *name* **resequence** *number1 number2*

Syntax Description

name	Unique identifier of the ACL. Enter an unquoted text string with a maximum of 64 alphanumeric characters.
resequence	Specifies the renumbering of the entries in an ACL.
number1	Number assigned to the first entry in the ACL. Enter any integer. The default is 10.
number2	Number added to each entry in the ACL after the first entry. Enter any integer. The default is 10.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the access-list feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The ability to resequence entries in an ACL is supported only for extended ACLs.

Examples

For example, to assign the number 5 to the first entry in the access list INBOUND and then number each succeeding entry by adding 15 to the preceding entry line number, enter:

```
host1/Admin(config)# access-list INBOUND resequence 5 15
```

Related Commands

clear access-list
show access-list

(config) action-list type modify http

Action list modify configuration mode commands allow you to configure ACE action lists. An action list is a named group of actions that you associate with a Layer 7 HTTP class map in a Layer 7 HTTP policy map. You can create an action list to modify an HTTP header or to rewrite an HTTP redirect URL for SSL. For information about the commands in action list modify configuration mode, see the "Action List Modify Configuration Mode Commands" section.

To create an action list, use the **action-list type modify http** command. The CLI prompt changes to (config-actlist-modify). Use the **no** form of this command to remove the action list from the configuration.

action-list type modify http *name*

no action-list type modify http *name*

Syntax Description

name	Unique name for the action list. Enter an unquoted text string with a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To create an action list, enter:

```
host1/Admin(config)# action-list type modify http HTTP_MODIFY_ACTLIST
host1/Admin(config-actlist-modify)#
```

To remove the action list from the configuration, enter:

```
host1/Admin(config)# no action-list type modify http HTTP_MODIFY_ACTLIST
```

Related Commands

show running-config
show stats

(config) action-list type optimization http

Action list optimization configuration mode commands allow you to configure ACE action lists. An action list is a named group of actions that you associate with a Layer 7 HTTP optimization policy map. The **action-list type** command allows you to configure a series of application acceleration and optimization statements. After you enter this command, the system enters the action list optimization configuration mode.

For information about the commands in action list optimization configuration mode, see the "Action List Optimization Configuration Mode Commands" section.

To create an optimization action map for performing application acceleration and optimization, use the **action-list type** command in global configuration mode. The CLI prompt changes to (config-actlist-optm). Use the **no** form of this command to remove an action list from the ACE.

action-list type optimization http *list_name*

no action-list type optimization http *list_name*

Syntax Description

optimization http	Specifies an optimization HTTP action list. After you create the optimization HTTP type action list, you configure application acceleration and optimization functions in the action list optimization configuration mode. For information about the commands in action list optimization configuration mode, see the "Action List Optimization Configuration Mode Commands" section.
list_name	Name assigned to the action list. Enter a unique name as an unquoted text string with a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

After you configure the action list, you associate it with a specific statement in a Layer 7 HTTP optimization policy map. The Layer 7 optimization HTTP policy map activates an optimization HTTP action list that allows you to configure the specified optimization actions.

For information about the commands in action list optimization configuration mode, see the "Action List Optimization Configuration Mode Commands" section. For details about configuring the commands in the action list optimization configuration mode, see the *Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide*.

Examples

To create an optimization HTTP action list, enter:

```
host1/Admin(config)# action-list type optimization http ACT_LIST1
host1/Admin(config-actlist-optm)#
```

To remove the action list from the configuration, enter:

```
host1/Admin(config)# no action-list type optimization http ACT_LIST1
```

Related Commands

show action-list

show running-config

(config) parameter-map type

(config) policy-map

(config) arp

To configure the Address Resolution Protocol (ARP) on the ACE to manage and map IP to Media Access Control (MAC) information to forward and transmit packets, use the **arp** command. Use the **no** form of this command to remove the ARP entry or reset a default value.

arp {*ip_address mac_address* | **interval** *seconds* | **inspection enable** [**flood** | **no flood**] | **learned-interval** *seconds* | **learned-mode enable** | **rate** *seconds* | **ratelimit** *pps* | **retries** *number* | **sync disable** | **sync-interval** *seconds*}

no arp {*ip_address mac_address* | **interval** | **inspection enable** | **learned-interval** | **learned-mode enable** | **rate** | **ratelimit** | **retries** | **sync disable** | **sync-interval**}

Syntax Description

ip_address mac_address	Static ARP entry in the ARP table that allows ARP responses from an IP address to a MAC address. Enter the IP address in dotted-decimal notation (for example, 172.16.56.76). Enter the MAC address in dotted-hexadecimal notation (for example, 00.60.97.d5.26.ab).
interval *seconds*	Specifies the interval in seconds that the ACE sends ARP requests to the configured hosts. Enter a number from 15 to 31526000. The default is 300.
inspection enable	Enables ARP inspection, preventing malicious users from impersonating other hosts or routers, known as ARP spoofing. The default is disabled.
flood	(Optional) Enables ARP forwarding of nonmatching ARP packets. The ACE forwards all ARP packets to all interfaces in the bridge group. This is the default setting.
no flood	(Optional) Disables ARP forwarding for the interface and drops non-matching ARP packets.
learned-interval *seconds*	Sets the interval in seconds when the ACE sends ARP requests for learned hosts. Enter a number from 60 to 31536000. The default is 14400.
learned-mode enable	Enables the ACE to learn MAC addresses if the command has been disabled. By default, for bridged traffic, the ACE learns MAC addresses from all traffic. For routed traffic, the ACE learns MAC addresses only from ARP response packets or from packets that are destined to the ACE (for example, a ping to a VIP or a ping to a VLAN interface).
rate *seconds*	Specifies the time interval in seconds between ARP retry attempts to hosts. Enter a number from 1 to 60. The default is 10.
ratelimit *pps*	Specifies the rate limit in packets per second for gratuitous ARPs sent by the ACE. Enter a number from 100 to 8192. The default is 512. Note that this keyword applies to the entire appliance.
retries *number*	Specifies the number of ARP attempts before the ACE flags the host as down. Enter a number from 2 to 15. The default is 3.
sync disable	Disables the replication of ARP entries. By default, ARP entry replication is enabled.
sync-interval *seconds*	Specifies the time interval between ARP sync messages for learned hosts. Enter an integer from 1 to 3600 seconds (1 hour). The default is 5 seconds.

Command Modes

Configuration mode

Admin and user contexts. The **ratelimit** keyword is available in the Admin context only.

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the interface feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

- If the IP address, source ifID, and MAC address match a static ARP entry, the inspection succeeds and the ACE allows the packet to pass.
- If the IP address and interface of the incoming ARP packet match a static ARP entry, but the MAC address of the packet does not match the MAC address that you configured in that static ARP entry, ARP inspection fails and the ACE drops the packet.
- If the ARP packet does not match any static entries in the ARP table or there are no static entries in the table, then you can set the ACE to either forward the packet out all interfaces (**flood**) or to drop the packet (**no-flood**). In this case, the source IP address to MAC address mapping is new to the ACE. If you enter the **flood** option, the ACE creates a new ARP entry and marks it as LEARNED. If you enter the **no-flood** option, the ACE drops the ARP packet.

The ARP rate limit applies to all gratuitous ARPs sent for local addresses on new configurations, appliance reboot, and on MAC address changes.

When you change the ARP request internal for learned hosts and configured hosts, the new timeout does not take effect until the existing time is reached. If you want the new timeout to take effect immediately, enter the **clear arp** command to apply the new ARP interval (see the **clear arp** command).

For more information, see the *Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*

Examples

To allow ARP responses from the router at 10.1.1.1 with the MAC address 00.02.9a.3b.94.d9, enter:

```
host1/contexta(config)# arp 10.1.1.1 00.02.9a.3b.94.d9
```

To remove a static ARP entry, enter:

```
host1/contexta(config)# no arp 10.1.1.1 00.02.9a.3b.94.d9
```

To enable ARP inspection and to drop all nonmatching ARP packets, enter:

```
host1/contexta(config)# arp inspection enable no-flood
```

To configure the retry attempt interval of 15 seconds, enter:

```
host1/contexta(config)# arp rate 15
```

To reset the retry attempt interval to the default of 10 seconds, enter:

```
host1/contexta(config)# no arp rate
```

To disable the replication of ARP entries, enter:

```
host1/contexta(config)# sync disable
```

Related Commands clear arp
show arp

(config) banner

Use the **banner** command to specify a message to display as the message-of-the-day banner when a user connects to the ACE CLI. Use the **no** form of this command to delete or replace a banner or a line in a multiline banner.

banner motd *text*

no banner motd *text*

Syntax Description

motd	Configures the system to display as the message-of-the-day banner when a user connects to the ACE.
text	Line of message text to be displayed as the message-of-the-day banner. The *text* string consists of all characters that follow the first space until the end of the line (carriage return or line feed). The # character functions as the delimiting character for each line. For the banner text, spaces are allowed but tabs cannot be entered at the CLI. Multiple lines in a message-of-the-day banner are handled by entering a new **banner** command for each line that you wish to add. The banner message is a maximum of 80 alphanumeric characters per line, up to a maximum of 3000 characters (3000 bytes) total for a message-of-the-day banner. This maximum value includes all line feeds and the last delimiting character in the message.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To replace a banner or a line in a multiline banner, use the **no banner motd** command before adding the new lines.

To add multiple lines in a message-of-the-day banner, precede each line by the **banner motd** command. The ACE appends each line to the end of the existing banner. If the text is empty, the ACE adds a carriage return (CR) to the banner.

You can include tokens in the form $(token) in the message text. Tokens will be replaced with the corresponding configuration variable, as follows:

- $(hostname)—Displays the hostname for the ACE during run time.
- $(line)—Displays the tty (teletypewriter) line or name (for example, /dev/console, /dev/pts/0, or 1).

To use the $(hostname) in single line banner motd input, include double quotation marks (“) around the $(hostname) so that the $ is interpreted to a special character for the beginning of a variable in the single line. An example is as follows:

```
switch/Admin(config)# banner motd #Welcome to "$(hostname)"...#
```

Do not use the double quotation mark (“) or the percent sign (%) as a delimiting character in a single line message string. Do not use the delimiting character in the message string.

For multiline input, double quotation marks (“) are not required for the token because the input mode is different from the signal line mode. The ACE treats the double quotation mark (“) as a regular character when you operate in multiline mode.

Examples

To add a message-of-the-day banner, enter:

```
host1/Admin(config)# banner motd #Welcome to the "$(hostname)".
host1/Admin(config)# banner motd Contact me at admin@admin.com for any
host1/Admin(config)# banner motd issues.#
```

Related Commands

show banner motd

(config) boot system image:

To set the BOOT environment variable, use the **boot system image:** command. Use the **no** form of this command to remove the name of the system image file.

boot system image:*filename*

no boot system image:*filename*

Syntax Description

filename	Name of the system image file.

Command Modes

Configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can add several images to the BOOT environment variable to provide a fail-safe boot configuration. If the first file fails to boot the ACE, subsequent images that are specified in the BOOT environment variable are tried until the ACE boots or there are no additional images to attempt to boot. If there is no valid image to boot, the ACE enters ROM-monitor mode where you can manually specify an image to boot.

The ACE stores and executes images in the order in which you added them to the BOOT environment variable. If you want to change the order in which images are tried at startup, you can either prepend and clear images from the BOOT environment variable to attain the desired order or you can clear the entire BOOT environment variable and then redefine the list in the desired order.

If the file does not exist (for example, if you entered the wrong filename), then the filename is appended to the boot string, and this message displays:

```
Warning: File not found but still added in the bootstring.
```

If the file does exist, but is not a valid image, the file is not added to the bootstring, and this message displays:

```
Warning: file found but it is not a valid boot image.
```

Examples

To set the BOOT environment variable, enter:

```
host1/Admin(config)# boot system image:ace-t1k9-mzg.3.1.0.bin
```

Related Commands

show bootvar
(config) config-register

(config) class-map

To create a Layer 3 and Layer 4 or a Layer 7 class map, use the **class-map** command. Use the **no** form of the command to remove a class map from the ACE.

class-map [**match-all** | **match-any**] *map_name*

class-map type {**ftp inspect match-any** | **generic** {**match-all** | **match-any**}} *map_name*

class-map type {**http** {**inspect** | **loadbalance**} | **management** | **radius loadbalance** | **rtsp loadbalance** | **sip** {**inspect** | **loadbalance**}} [**match-all** | **match-any**] *map_name*

no class-map [**match-all** | **match-any**] *map_name*

no class-map type {**ftp inspect match-any** | **generic** {**match-all** | **match-any**}} *map_name*

no class-map type {**http** {**inspect** | **loadbalance**} | **management** | **radius loadbalance** | **rtsp loadbalance** | **sip** {**inspect** | **loadbalance**}} [**match-all** | **match-any**] *map_name*

Syntax Description

match-all	Determines how the ACE evaluates Layer 3 and Layer 4 network traffic when multiple match criteria exist in a class map. The class map is considered a match if all the match criteria listed in the class map match the network traffic class in the class map (typically, **match** commands of different types). The default setting is to meet all of the match criteria (**match-all**) in a class map.
match-any	Determines how the ACE evaluates Layer 3 and Layer 4 network traffic when multiple match criteria exist in a class map. The class map is considered a match if only one of the match criteria listed in the class map matches the network traffic class in the class map (typically, **match** commands of the same type). The default setting is to meet all of the match criteria (**match-all**) in a class map.
map_name	Name assigned to the class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. For a Layer 3 and Layer 4 class map, you enter the class map configuration mode and the prompt changes to (config-cmap).
type	Specifies the class map type that is to be defined. When you specify a class map type, you enter its corresponding class map configuration mode (for example, HTTP inspection configuration mode).
ftp inspect	Specifies a Layer 7 class map for the inspection of File Transfer Protocol (FTP) request commands. For information about commands in FTP inspection configuration mode, see the "Class Map FTP Inspection Configuration Mode Commands" section.
generic	Specifies a Layer 7 class map for generic TCP or UDP data parsing. For information about commands in class map generic configuration mode, see the "Class Map Generic Configuration Mode Commands" section.
http inspect | **loadbalance**	Specifies a Layer 7 class map for HTTP server load balancing (**loadbalance** keyword) or a Layer 7 class map for the HTTP deep packet application protocol inspection (**inspect** keyword) of traffic through the ACE. For information about commands in class map HTTP inspection configuration mode, see the "Class Map HTTP Inspection Configuration Mode Commands" section. For information about commands in class map HTTP server load-balancing configuration mode, see the "Class Map HTTP Load Balancing Configuration Mode Commands" section.

management	Specifies a Layer 3 and Layer 4 class map to classify the IP network management protocols received by the ACE. For information about commands in class map management configuration mode, see the "Class Map Management Configuration Mode Commands" section.
radius loadbalance	Specifies a Layer 7 class map for RADIUS server load balancing of traffic through the ACE. For information about commands in RADIUS server load-balancing configuration mode, see the "Class Map RADIUS Load Balancing Configuration Mode Commands" section.
rtsp loadbalance	Specifies a Layer 7 class map for RTSP server load balancing of traffic through the ACE. For information about commands in RTSP server load-balancing configuration mode, see the "Class Map RTSP Load Balancing Configuration Mode Commands" section.
sip inspect | loadbalance	Specifies a Layer 7 class map for SIP server load balancing (**loadbalance** keyword) or a Layer 7 class map for the SIP deep packet application protocol inspection (**inspect** keyword) of traffic through the ACE. For information about commands in class map SIP inspection configuration mode, see the "Class Map SIP Inspection Configuration Mode Commands" section. For information about commands in class map SIP server load-balancing configuration mode, see the "Class Map SIP Load Balancing Configuration Mode Commands" section.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised.

Usage Guidelines

This command requires the inspect, loadbalance, NAT, connection, SSL, or vip feature in your user role, depending on the type of class map that you want to configure. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Use the **class map** configuration mode commands to create class maps that classify inbound network traffic destined to, or passing through, the ACE based on a series of flow match criteria specified in the class map. The CLI prompt changes correspondingly to the selected class map configuration mode, for example, (config-cmap), (config-cmap-ftp-insp), (config-cmap-http-lb), or (config-cmap-mgmt).

A Layer 3 and Layer 4 class map contains match criteria that classifies the following:

- Network traffic that can pass through the ACE based on source or destination IP address, source or destination port, or IP protocol and port
- Network management traffic that can be received by the ACE based on the HTTP, HTTPS, ICMP, SNMP, SSH, or Telnet protocols

A Layer 7 class map contains match criteria that classifies specific Layer 7 protocol information. The match criteria enables the ACE to do the following:

- Perform server load balancing based on the HTTP cookie, the HTTP header, the HTTP URL, protocol header fields, or source IP addresses
- Perform deep packet inspection of the HTTP protocol
- Perform FTP request command filtering

The ACE supports a system-wide maximum of 8192 class maps.

For details about creating a class map, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

When multiple match criteria exist in the traffic class, you can identify evaluation instructions using the **match-any** or **match-all** keywords. If you specify **match-any**, the traffic that is evaluated must match one of the specified criteria (typically, **match** commands of the same type). If you specify **match-all**, the traffic that is evaluated must match all of the specified criteria (typically, **match** commands of different types).

Examples

To create a Layer 3 and Layer 4 class map named L4VIP_CLASS that specifies the network traffic that can pass through the ACE for server load balancing, enter:

```
host1/Admin(config)# class-map match-all L4VIP_CLASS
host1/Admin(config-cmap)#
```

To create a Layer 3 and Layer 4 class map named MGMT-ACCESS_CLASS that classifies the network management protocols that can be received by the ACE, enter:

```
host1/Admin(config)# class-map type management match-any MGMT-ACCESS_CLASS
host1/Admin(config-cmap-mgmt)#
```

To create a Layer 7 class map named L7SLB_CLASS that performs HTTP server load balancing, enter:

```
host1/Admin(config)# class-map type http loadbalance match-any L7SLB_CLASS
host1/Admin(config-cmap-http-lb)#
```

To create a Layer 7 class map named HTTP_INSPECT_L7CLASS that performs HTTP deep packet inspection, enter:

```
(config)# class-map type http inspect match-any HTTP_INSPECT_L7CLASS
host1/Admin(config-cmap-http-insp)#
```

To create a Layer 7 class map named FTP_INSPECT_L7CLASS that performs FTP command inspection, enter:

```
host1/Admin(config)# class-map type ftp inspect match-any FTP_INSPECT_L7CLASS
host1/Admin(config-cmap-ftp-insp)#
```

Related Commands

show startup-config
(config) policy-map
(config) service-policy

(config) clock timezone

To set the time zone, use the **clock timezone** command. Use the **no** form of this command to configure independent server groups of Terminal Access Controller Access Control System Plus (TACACS+), Remote Authentication Dial-In User Service (RADIUS), or Lightweight Directory Access Protocol (LDAP) servers.

clock timezone {*zone_name* {**+** | **–**} *hours minutes*} | {**standard** *time_zone*}

no clock timezone

Syntax Description

zone_name	8-letter name of the time zone (for example, PDT) to be displayed when the time zone is in effect. See Table 2-4 in the "Usage Guidelines" section for a list of the common time zone acronyms used for this argument.
hours	Hours offset from Coordinated Universal Time (UTC).
minutes	Minutes offset from UTC. Range is from 0 to 59 minutes.
standard *time_zone*	Sets the time to a standard time zone that include an applicable UTC hours offset. Enter one of the following well-known time zones: • **ACST**—Australian Central Standard Time as UTC + 9.5 hours • **AKST**—Alaska Standard Time as UTC –9 hours • **AST**—Atlantic Standard Time as UTC –4 hours • **BST**—British Summer Time as UTC + 1 hour • **CEST**—Central Europe Summer Time as UTC + 2 hours • **CET**—Central Europe Time as UTC + 1 hour • **CST**—Central Standard Time as UTC –6 hours • **EEST**—Eastern Europe Summer Time as UTC + 3 hours • **EET**—Eastern Europe Time as UTC + 2 hours • **EST**—Eastern Standard Time as UTC –5 hours • **GMT**—Greenwich Mean Time as UTC • **HST**—Hawaiian Standard Time as UTC –10 hours • **IST**—Irish Summer Time as UTC + 1 hour • **MSD**—Moscow Summer Time as UTC + 4 hours • **MSK**—Moscow Time as UTC + 3 hours • **MST**—Mountain Standard Time as UTC –7 hours • **PST**—Pacific Standard Time as UTC –8 hours • **WEST**—Western Europe Summer Time as UTC + 1 hour • **WST**—Western Standard Time as UTC + 8 hours

Command Modes

Configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	The **ACST** keyword was introduced. It replaced the **CST** keyword, as UTC +9.5 hours.

Usage Guidelines

The ACE keeps time internally in Universal Time Coordinated (UTC) offset, so this command is used only for display purposes and when the time is set manually.

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Table 2-4 lists common time zone acronyms used for the *zone_name* argument.

Table 2-4 Time Zone Acronyms

Acronym	Time Zone Name and UTC Offset
Europe	
BST	British Summer Time as UTC + 1 hour
CET	Central Europe Time as UTC + 1 hour
CEST	Central Europe Summer Time as UTC + 2 hours
EET	Eastern Europe Time as UTC + 2 hours
EEST	Eastern Europe Summer Time as UTC + 3 hours
GMT	Greenwich Mean Time as UTC
IST	Irish Summer Time as UTC + 1 hour
MSK	Moscow Time as UTC + 3 hours
MSD	Moscow Summer Time as UTC + 4 hours
WET	Western Europe Time as UTC
WEST	Western Europe Summer Time as UTC + 1 hour
United States and Canada	
AST	Atlantic Standard Time as UTC –4 hours
ADT	Atlantic Daylight Time as UTC –3 hours
CT	Central Time, either as CST or CDT, depending on the place and time of the year
CST	Central Standard Time as UTC –6 hours
CDT	Central Daylight Saving Time as UTC –5 hours
ET	Eastern Time, either as EST or EDT, depending on the place and time of the year
EST	Eastern Standard Time as UTC –5 hours
EDT	Eastern Daylight Saving Time as UTC –4 hours
MT	Mountain Time, either as MST or MDT, depending on the place and time of the year
MDT	Mountain Daylight Saving Time as UTC –6 hours

Table 2-4 Time Zone Acronyms (continued)

Acronym	Time Zone Name and UTC Offset
MST	Mountain Standard Time as UTC –7 hours
PT	Pacific Time, either as PST or PDT, depending on the place and time of the year
PDT	Pacific Daylight Saving Time as UTC –7 hours
PST	Pacific Standard Time as UTC –8 hours
AKST	Alaska Standard Time as UTC –9 hours
AKDT	Alaska Standard Daylight Saving Time as UTC –8 hours
HST	Hawaiian Standard Time as UTC –10 hours
Australia	
CST	Central Standard Time as UTC + 9.5 hours
EST	Eastern Standard/Summer Time as UTC + 10 hours (+11 hours during summer time)
WST	Western Standard Time as UTC + 8 hours

Examples

To set the time zone to PST and to set an UTC offset of –8 hours, enter:

```
host1/Admin(config)# clock timezone PST -8 0
```

To remove the clock time-zone setting, enter:

```
host1/Admin(config)# no clock timezone PST -8 0
```

Related Commands

clock set
show clock
(config) clock summer-time

(config) clock summer-time

To configure the ACE to change the time automatically to summer time (daylight saving time), use the **clock summer-time** command. Use the **no** form of this command to remove the clock summer-time setting.

clock summer-time {*daylight_timezone_name start_week start_day start_month start_time end_week end_day end_month end_time daylight_offset* | **standard** *time_zone*}

no clock summer-time

Syntax Description

daylight_timezone_name	8-letter name of the time zone (for example, PDT) to be displayed when summer time is in effect. For a list of the common time zone acronyms used for this argument, see the "Usage Guidelines" section for the **(config) clock timezone** command.
start_week	Start week for summer time, ranging from 1 through 5.
start_day	Start day for summer time, ranging from Sunday through Saturday.
start_month	Start month for summer time, ranging from January through December.
start_time	Start time (military time) in hours and minutes.
end_week	End week for summer time, ranging from 1 through 5.
end_day	End day for summer time, ranging from Sunday through Saturday.
end_month	End month for summer time, ranging from January through December.
end_time	End time (military format) in hours and minutes.
daylight_offset	Number of minutes to add during summer time. Valid entries are from 1 to 1440. The default is 60.
standard *time_zone*	Sets the daylight time to a standard time zone that includes an applicable daylight time start and end range along with a daylight offset. Enter one of the following well-known time zones: • **ADT**—Atlantic Daylight Time: 2 a.m. first Sunday in April—2 a.m. last Sunday in October, + 60 minutes • **AKDT**—Alaska Standard Daylight Time: 2 a.m. first Sunday in April—2 a.m. last Sunday in October, + 60 minutes • **CDT**—Central Daylight Time: 2 a.m. first Sunday in April—2 a.m. last Sunday in October, + 60 minutes • **EDT**—Eastern Daylight Time: 2 a.m. first Sunday in April—2 a.m. last Sunday in October, + 60 minutes • **MDT**—Mountain Daylight Time: 2 a.m. first Sunday in April—2 a.m. last Sunday in October, + 60 minutes • **PDT**—Pacific Daylight Time: 2 a.m. first Sunday in April—2 a.m. last Sunday in October, + 60 minutes

Command Modes

Configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The first part of the command specifies when summer time begins, and the second part of the command specifies when summer time ends. All times are relative to the local time zone; the start time is relative to standard time and the end time is relative to summer time. If the starting month is after the ending month, the ACE assumes that you are located in the southern hemisphere.

Examples

To specify that summer time begins on the first Sunday in April at 02:00 and ends on the last Sunday in October at 02:00, with a daylight offset of 60 minutes, enter:

```
host1/Admin(config)# clock summer-time Pacific 1 Sun Apr 02:00 5 Sun Oct 02:00 60
```

To remove the clock summer-time setting, enter:

```
host1/Admin(config)# no clock summer-time
```

Related Commands

show clock
(config) clock timezone

(config) config-register

To change the configuration register settings, use the **config-register** configuration command. Use the **no** form of this command to reset the config-register setting.

config-register *value*

no config-register *value*

Syntax Description

value	Configuration register value that you want to use the next time that you restart the ACE. The supported *value* entries are as follows: • **0x0**—Upon reboot, the ACE boots to the GNU GRand Unified Bootloader (GRUB). From the GRUB boot loader, you specify the system boot image to use to boot the ACE. Upon startup, the ACE loads the startup-configuration file stored in Flash memory (nonvolatile memory) to the running-configuration file stored in RAM (volatile memory). • **0x1**—Upon reboot, the ACE boots the system image identified in the BOOT environment variable (see **(config) boot system image:**). The BOOT environment variable specifies a list of image files on various devices from which the ACE can boot at startup. If the ACE encounters an error or if the image is not valid, it will try the second image (if one is specified). Upon startup, the ACE loads the startup-configuration file stored in Flash memory (nonvolatile memory) to the running-configuration file stored in RAM (volatile memory).

Command Modes

Configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can modify the boot method that the ACE uses at the next startup by setting the boot field in the software configuration register. The configuration register identifies how the ACE should boot.

The **config-register** command affects only the configuration register bits that control the boot field and leaves the remaining bits unaltered.

Examples

To set the boot field in the configuration register to boot the system image identified in the BOOT environment variable upon reboot and to load the startup-configuration file stored in Flash memory, enter:

```
host1/Admin(config)# config-register 0x1
```

Related Commands

(config) boot system image:

(config) context

To create a context, use the **context** command. The CLI prompt changes to (config-context). A context provides a user view into the ACE and determines the resources available to a user. Use the **no** form of this command to remove a context.

context *name*

no context *name*

Syntax Description

name	Name that designates a context. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. Do not configure a context name that contains opening braces, closing braces, white spaces, or any of the following symbols: ` $ % & * ( ) \ | ; ' " < > / ?

Command Modes

Configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.
A3(2.3)	This command no longer supports you from configuring a context name that contains opening braces, closing braces, white spaces, or any of the following symbols: ` $ % & * ( ) \ | ; ' " < > / ?

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

By default, the ACE allows you to create and use five user-configured contexts plus the default Admin context. To use a maximum of 251 contexts (Admin context plus 250 user contexts), you must purchase an additional license from Cisco Systems.

Examples

To create a context called C1, enter:

```
host1/Admin(config)# context C1
host1/Admin(config-context)#
```

To remove the context from the configuration, enter:

```
host1/Admin(config)# no context C1
```

Related Commands

changeto
show context
show user-account
show users

(config) crypto authgroup

To create a certificate authentication group, use the **crypto authgroup** command. Once you create an authentication group, the CLI enters into the authentication group configuration mode, where you add the required certificate files to the group. Use the **no** form of this command to delete an existing authentication group.

crypto authgroup *group_name*

no crypto authgroup *group_name*

Syntax Description

group_name	Name that you assign to the authentication group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Secure Sockets Layer (SSL) feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

By creating an authentication group, you can implement a group of certificates that are trusted as certificate signers on the ACE. After creating the authentication group and assigning its certificates, you can configure client authentication on an SSL-proxy service by assigning the authentication group to the service. You include an authentication group in the handshake process by configuring the SSL proxy-service with the authentication group (see the **(config) ssl-proxy service** command).

Examples

To create the authentication group AUTH-CERT1, enter:

```
host1/Admin(config)# crypto authgroup AUTH-CERT
```

Related Commands

(config) ssl-proxy service

(config) crypto chaingroup

To create a certificate chain group, use the **crypto chaingroup** command. Once you create a chain group, the CLI enters into the chaingroup configuration mode, where you add the required certificate files to the group. Use the **no** form of this command to delete an existing chain group.

crypto chaingroup *group_name*

no crypto chaingroup *group_name*

Syntax Description

group_name	Name that you assign to the chain group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Secure Sockets Layer (SSL) feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

A chain group specifies the certificate chains that the ACE sends to its peer during the handshake process. A certificate chain is a hierarchal list of certificates that includes the subject's certificate, the root CA certificate, and any intermediate CA certificates. You include a chain group in the handshake process by configuring the SSL proxy service with the chain group (see the **(config) ssl-proxy service** command).

Each context on the ACE can contain up to eight chain groups.

Examples

To create the chain group MYCHAINGROUP, enter:

```
host1/Admin(config)# crypto chaingroup MYCHAINGROUP
```

Related Commands

(config) ssl-proxy service

(config) crypto crl

To download a certificate revocation list (CRL) to the ACE, use the **crypto crl** command. Use the **no** form of this command to remove a CRL.

crypto crl *crl_name url*

no crypto crl *crl_name*

Syntax Description

crl_name	Name that you assign to the CRL. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
url	URL where the ACE retrieves the CRL. Enter the URL full path including the CRL filename in an unquoted alphanumeric string with a maximum of 255 characters. Start the URL with the http:// prefix. Only HTTP URLs are supported.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command requires the Secure Sockets Layer (SSL) feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can use a CRL downloaded to the ACE for client or server authentication on an SSL proxy service. After you download the CRL, you can assign it to an SSL proxy service for either client or server authentication (see (config-ssl-proxy) crl for more information).

Examples

To download a CRL that you want to name CRL1 from http://crl.verisign.com/class1.crl, enter:

```
host1/Admin(config)# crypto crl CRL1 http://crl.verisign.com/class1.crl
```

To remove the CRL, enter:

```
host1/Admin(config)# no crypto crl CRL1
```

Related Commands

(config) ssl-proxy service

(config) crypto csr-params

To create a Certificate Signing Request (CSR) parameter set to define a set of distinguished name attributes, use the **crypto csr-params** command. Use the **no** form of this command to remove an existing CSR parameter set.

crypto csr-params *csr_param_name*

no crypto csr-params *csr_param_name*

Syntax Description

csr_param_name	Name that designates a CSR parameter set. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the SSL feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

A CSR parameter set defines the distinguished name attributes that the ACE applies to the CSR during the CSR-generating process. The distinguished name attributes provide the CA with the information that it needs to authenticate your site. Creating a CSR parameter set allows you to generate multiple CSRs with the same distinguished name attributes. You can create up to eight CSR parameter sets per context.

When you use the **crypto csr-params** command to specify a CSR parameter set, the prompt changes to the csr-params configuration mode (for more information on this mode and commands, see the "CSR Parameters Configuration Mode Commands" section), where you define each of the distinguished name attributes. The ACE requires that you define the following attributes:

Country name

- State or province
- Common name
- Serial number

If you do not configure the required attributes, the ACE displays an error message when you attempt to generate a CSR using the incomplete CSR parameter set.

Examples

To create the CSR parameter set CSR_PARAMS_1, enter:

```
host1/Admin(config)# crypto csr-params CSR_PARAMS_1
host1/Admin(config-csr-params)
```

Related Commands

crypto generate csr
show crypto

(config) domain

To create a domain, use the **domain** command. The CLI prompt changes to (config-domain). See the "Domain Configuration Mode Commands" section for details. Use the **no** form of this command to remove a domain from the configuration.

domain *name*

no domain *name*

Syntax Description

name	Name for the domain. Enter an unquoted text string with no spaces and a maximum of 76 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can configure a maximum of 63 domains in each context.

A domain does not restrict the context configuration that you can display using the **show running-config** command. You can still display the running configuration for the entire context. However, you can restrict your access to the configurable objects within a context by adding to the domain only a limited subset of all the objects available to a context. To limit a user's ability to manipulate the objects in a domain, you can assign a role to that user. For more information about domains and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can configure KAL-AP TAGs as domains. For the domain load calculation, the ACE considers the Layer 3 class map, server farm, and real server objects. All other objects under the domain are ignored during the calculation.

Examples

To create a domain named D1, enter:

```
host1/Admin(config)# domain D1
host1/Admin(config-domain)#
```

Related Commands

(config) context
show user-account
show users

(config) end

To exit from configuration mode and return to Exec mode, use the **end** command.

end

Syntax Description

This command has no keywords or arguments.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can also press **Ctrl-Z** or enter the **exit** command to exit configuration mode.

Examples

To exit from configuration mode and return to Exec mode, enter:

```
host1/Admin(config)# end
host1/Admin#
```

Related Commands

This command has no related commands.

(config) exit

To exit from the current configuration mode and return to the previous mode, use the **exit** command.

exit

Syntax Description

This command has no keywords or arguments.

Command Modes

All configuration modes

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

In configuration mode, the **exit** command transitions to the Exec mode.

In all other configuration modes, the **exit** command transitions to the previous configuration mode.

You can also press **Ctrl-Z**, enter the **(config) end** command, or enter the **exit** command to exit configuration mode.

Examples

To exit from configuration mode and return to Exec mode, enter:

```
host1/Admin(config)# exit
host1/Admin#
```

To exit from interface configuration mode and return to configuration mode, enter:

```
host1/Admin(config-if)# exit
host1/Admin(config)#
```

Related Commands

This command has no related commands.

(config) ft auto-sync

To enable automatic synchronization of the running-configuration and the startup-configuration files in a redundancy configuration, use the **ft auto-sync** command. Use the **no** form of this command to disable the automatic synchronization of the running-configuration or the startup-configuration file.

ft auto-sync {**running-config** | **startup-config**}

no ft auto-sync {**running-config** | **startup-config**}

Syntax Description

running-config	Enables autosynchronization of the running-configuration file. The default is enabled.
startup-config	Enables autosynchronization of the startup-configuration file. The default is enabled.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the fault-tolerant feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

By default, the ACE automatically updates the running configuration on the standby context of an FT group with any changes that occur to the running configuration of the active context. If you disable the **ft auto-sync** command, you need to update the configuration of the standby context manually. For more information about configuration synchronization and configuring redundancy, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Caution Toggling **ft auto-sync running-config** in the Admin context may have undesirable side effects if the same command is also disabled in an active user context. If the **ft auto-sync running-config** command is disabled in the active Admin context and in an active user context, and you subsequently enable the **ft auto-sync running-config** command in the active Admin context first, the entire configuration of the standby user context will be lost. Always enter the **ft auto-sync running-config** command in the active user context first, and then enable the command in the active Admin context.

The ACE does not copy or write changes in the running-configuration file to the startup-configuration file unless you enter the **copy running-config startup-config** command or the **write memory** command for the current context. To write the contents of the running-configuration file to the startup-configuration file for all contexts, use the **write memory all** command. At this time, if the **ft auto-sync startup-config** command is enabled, the ACE syncs the startup-configuration file on the active ACE to the standby ACE.

The ACE does not synchronize the SSL certificates and key pairs that are present in the active context with the standby context of an FT group. If the ACE performs a configuration synchronization and does not find the necessary certs and keys in the standby context, config sync fails and the standby context enters the STANDBY_COLD state.

Caution Do not enter the **no inservice** command followed by the **inservice** command on the active context of an FT group when the standby context is in the STANDBY_COLD state. Doing so may cause the standby context running-configuration file to overwrite the active context running-configuration file.

To copy the certs and keys to the standby context, you must export the certs and keys from the active context to an FTP or TFTP server using the **crypto export** command, and then import the certs and keys to the standby context using the **crypto import** command. For more information about importing and exporting certs and keys, see the *Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide*.

To return the standby context to the STANDBY_HOT state in this case, ensure that you have imported the necessary SSL certs and keys to the standby context, and then perform a bulk sync of the active context configuration by entering the following commands in configuration mode in the active context of the FT group:

1. **no ft auto-sync running-config**
2. **ft auto-sync running-config**

Examples

To enable autosynchronization of the running-configuration file in the C1 context, enter:

```
host1/C1(config)# ft auto-sync running-config
```

Related Commands

(config) ft group
(config) ft interface vlan
(config) ft peer
(config) ft track host
(config) ft track interface

(config) ft group

To create a fault-tolerant (FT) group for redundancy, use the **ft group** command. After you enter this command, the system enters the FT group configuration mode. Use the **no** form of this command to remove an FT group from the configuration.

ft group *group_id*

no ft group *group_id*

Syntax Description

group-id	Unique identifier of the FT group. Enter an integer from 1 to 255.

Command Modes

Configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You must configure the same group ID on both peer appliances.

On each ACE, you can create multiple FT groups, up to a maximum of 256 groups. Each group consists of a maximum of two members (contexts): one active context on one appliance and one standby context on the peer appliance.

For information about the commands in FT group configuration mode, see the "FT Group Configuration Mode Commands" section.

Examples

To configure an FT group, enter:

```
host1/Admin(config)# ft group 1
host1/Admin(config-ft-group)#
```

To remove the group from the configuration, enter:

```
host1/Admin(config)# no ft group 1
```

Related Commands

(config) ft auto-sync
(config) ft interface vlan
(config) ft peer
(config) ft track host
(config) ft track interface

(config) ft interface vlan

To create a dedicated fault-tolerant (FT) VLAN over which two redundant peers communicate, use the **ft interface vlan** command. After you enter this command, the system enters the FT interface configuration mode. Use the **no** form of this command to remove an FT VLAN from the configuration.

ft interface vlan *vlan_id*

no ft interface vlan *vlan_id*

Syntax Description

vlan_id	Unique identifier for the FT VLAN. Enter an integer from 2 to 4094.

Command Modes

Configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Peer ACEs communicate with each other over a dedicated FT VLAN. These redundant peers use the FT VLAN to transmit and receive heartbeat packets and state and configuration replication packets. You must configure the same VLAN on each peer appliance. You cannot use this VLAN for normal network traffic.

To configure one of the Ethernet ports or a port-channel interface on the ACE for fault tolerance using a dedicated FT VLAN for communication between the members of an FT group, use the **ft-port vlan** command in interface configuration mode. See the **(config-if) ft-port vlan** command for more information.

On both peer ACE appliances, you must configure the same Ethernet port or port-channel interface as the FT VLAN port. For example:

- If you configure ACE appliance 1 to use Ethernet port 4 as the FT VLAN port, then be sure to configure ACE appliance 2 to use Ethernet port 4 as the FT VLAN port.
- If you configure ACE appliance 1 to use port-channel interface255 as the FT VLAN port, then be sure to configure ACE appliance 2 to use port-channel interface 255 as the FT VLAN.

To remove an FT VLAN, first remove it from the FT peer using the **no ft-interface vlan** command in FT peer configuration mode. See the **(config-ft-peer) ft-interface vlan** command for more information.

Examples

To configure an FT VLAN, enter:

```
host1/Admin(config)# ft interface vlan 200
host1/Admin(config-ft-intf)#
```

To remove the FT VLAN from the redundancy configuration, enter:

```
host1/Admin(config)# no ft interface vlan 200
```

Related Commands

(config) ft auto-sync
(config) ft group
(config) ft peer
(config) ft track host
(config) ft track interface
(config-if) ft-port vlan

(config) ft peer

On both peer ACEs, configure an FT peer definition. To create an FT peer, use the **ft peer** command. After you enter this command, the system enters the FT peer configuration mode. You can configure a maximum of two ACEs as redundancy peers. Use the **no** form of this command to remove the FT peer from the configuration.

ft peer *peer_id*

no ft peer *peer_id*

Syntax Description

peer_id	Unique identifier of the FT peer. Enter 1.

Command Modes

Configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Each ACE appliance can have one FT peer. FT peers are redundant ACE appliances that communicate with each other over a dedicated FT VLAN.

Before you can remove an FT peer from the configuration, remove the peer from the FT group using the **no peer** command in FT group configuration mode.

For information about the commands in FT peer configuration mode, see the "FT Peer Configuration Mode Commands" section.

Examples

To configure an FT peer, enter:

```
host1/Admin(config)# ft peer 1
host1/Admin(config-ft-peer)#
```

Related Commands

(config) ft auto-sync
(config) ft group
(config) ft interface vlan
(config) ft track host
(config) ft track interface

(config) ft track host

To create a tracking and failure detection process for a gateway or host, use the **ft track host** command. After you enter this command, the system enters FT track host configuration mode. Use the **no** form of this command to remove the gateway-tracking process.

ft track host *name*

no ft track host *name*

Syntax Description

name	Unique identifier of the tracking process for a gateway or host. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the fault-tolerant (FT) feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about commands in FT track host configuration mode, see the "FT Track Host Configuration Mode Commands" section.

For details about configuring redundant ACE appliances, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To create a tracking process for a gateway, enter:

```
host1/Admin(config)# ft track host TRACK_GATEWAY1
host1/Admin(config-ft-track-host)#
```

To remove the gateway-tracking process, enter:

```
host1/Admin(config)# no ft track host TRACK_GATEWAY1
```

Related Commands

(config) ft track interface

(config) ft track interface

To create a tracking and failure detection process for a critical interface, use the **ft track interface** command. After you enter this command, the system enters FT track interface configuration mode. Use the **no** form of this command to stop tracking for an interface.

ft track interface *name*

no ft track interface *name*

Syntax Description

name	Unique identifier of the tracking process for a critical interface. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the fault-tolerant (FT) feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You cannot delete an interface if the ACE is using the interface for tracking. Also, you cannot configure the FT VLAN for tracking.

For information about commands in FT track interface configuration mode, see the "FT Track Interface Configuration Mode Commands" section.

For details about configuring redundant ACE appliances, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To configure a tracking and failure detection process for an interface, enter:

```
host1/Admin(config)# ft track interface TRACK_VLAN100
```

To remove the interface-tracking process, enter:

```
host1/Admin(config)# no ft track interface TRACK_VLAN100
```

Related Commands

(config) ft auto-sync
(config) ft group
(config) ft interface vlan
(config) ft peer
(config) ft track host

(config) hostname

To specify a hostname for the ACE, use the **hostname** command. The hostname is used for the command line prompts and default configuration filenames. If you establish sessions to multiple devices, the hostname helps you track where you enter commands. Use the **no** form of this command to reset the hostname to the default of switch.

hostname *name*

no hostname *name*

Syntax Description

name	New hostname for the ACE. Enter a case-sensitive text string that contains from 1 to 32 alphanumeric characters.

Command Modes

Configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

By default, the hostname for the ACE is switch.

Examples

To change the hostname of the ACE from switch to ACE_1, enter:

```
switch/Admin(config)# hostname ACE_1
ACE_1/Admin(config)#
```

Related Commands

(config) peer hostname

(config) interface

To configure a bridge-group virtual interface (BVI), Ethernet port, port-channel interface, or VLAN interface, use the **interface** command. The CLI prompt changes to (config-if). Use the **no** form of this command to remove the interface.

interface {**bvi** *group_number* | **gigabitEthernet** *slot_number/port_number* | **port-channel** *channel_number* | **vlan** *number*}

no interface {**bvi** *group_number* | **gigabitEthernet** *slot_number/port_number* | **port-channel** *channel_number* | **vlan** *number*}

Syntax Description

bvi *group_number*	Creates a BVI for a bridge group and accesses interface configuration mode commands for the BVI. The *group_number* argument is the bridge-group number configured on a VLAN interface.
gigabitEthernet *slot_number/ port_number*	Specifies one of the four Ethernet ports on the rear panel of the ACE as follows: • *slot_number*—The physical slot on the ACE containing the Ethernet ports. This selection is always 1, the location of the daughter card in the ACE. The daughter card includes the four Layer 2 Ethernet ports to perform Layer 2 switching. • *port_number*—The physical Ethernet port on the ACE. Valid selections are 1 through 4, which specifies one of the four Ethernet ports (1, 2, 3, or 4) associated with the slot 1 (daughter card) selection.
port-channel *channel_number*	Specifies the channel number assigned to this port-channel interface. Valid values are from 1 to 255.
vlan *number*	Assigns the VLAN to the context and accesses interface configuration mode commands for the VLAN. The *number* argument is the number for a VLAN assigned to the ACE.

Command Modes

Configuration mode

BVI and VLAN—Admin and user contexts

Ethernet port and port-channel interface—Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the interface feature in your user role. In addition, the Ethernet port and port-channel interface command functions require the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The four Ethernet ports provide physical Ethernet ports to connect servers, PCs, routers, and other devices to the ACE. You can configure the four Ethernet ports to provide an interface for connecting to 10-Mbps, 100-Mbps, or 1000-Mbps networks. Each Layer 2 Ethernet port supports autonegotiate, full-duplex, or half-duplex operation on an Ethernet LAN and can carry traffic within a designated VLAN.

You can group physical ports together on the ACE to form a logical Layer 2 interface called the EtherChannel (or port channel). You must configure all the ports that belong to the same port channel with the same values (such as port parameters, VLAN membership, and trunk configuration). Only one port channel in a channel group is allowed, and a physical port can belong to only to a single port-channel interface.

To enable the bridge-group VLANs, you must configure a bridge-group virtual interface (BVI) that represents a corresponding bridge group. You should configure an IP address in the same subnet on the BVI. This address is used for management traffic and as a source IP address for traffic from the ACE, similar to ARP requests.

You can configure one or more VLAN interfaces in any user context before you assign those VLAN interfaces to the associated user contexts through the **(config-context) allocate-interface** command in the Admin context.

The ACE supports a maximum of 4000 VLAN interfaces with a maximum of 1024 shared VLANs.

The ACE requires a route back to the client before it can forward a request to a server. If the route back is not present, the ACE cannot establish a flow and drops the client request. Make sure that you configure the appropriate routing to the client network on the ACE VLAN where the client traffic enters the ACE appliance.

For information about commands in interface configuration mode, see the "Interface Configuration Mode Commands" section. For details about configuring a BVI interface, Ethernet port, port-channel interface, or VLAN interface, see the *Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*.

Examples

To configure Ethernet port 3 and access interface configuration mode, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/3
host1/Admin(config-if)#
```

To create a port-channel interface with a channel number of 255, enter:

```
host1/Admin(config)# interface port-channel 255
```

```
host1/Admin(config-if)#
```

To assign VLAN interface 200 to the Admin context and access interface configuration mode, enter:

```
host1/Admin(config)# interface vlan 200
host1/Admin(config-if)#
```

To remove a VLAN, enter:

```
host1/Admin(config)# no interface vlan 200
```

To create a BVI for bridge group 15, enter:

```
host1/Admin(config)# interface bvi 15
host1/Admin(config-if)#
```

To delete a BVI for bridge group 15, enter:

```
host1/Admin(config)# no interface bvi 15
```

Related Commands

clear interface
show interface

(config) ip dhcp relay

To configure a Dynamic Host Configuration Protocol (DHCP) relay agent on the ACE, use the **ip dhcp relay** command. When you configure the ACE as a DHCP relay agent, it is responsible for forwarding the requests and responses negotiated between the DHCP clients and the server. You must configure a DHCP server when you enable the DHCP relay. Use the **no** form of this command to disable a DHCP relay agent setting.

ip dhcp relay {**enable** | **information policy** {**keep** | **replace**} | **server** *ip_address*}

no ip dhcp relay {**enable** | **information policy** {**keep** | **replace**} | **server** *ip_address*}

Syntax Description

enable	Accepts DHCP requests from clients on the associated context or interface and enables the DHCP relay agent. The DHCP relay starts forwarding packets to the DHCP server address specified in the **ip dhcp relay server** command for the associated interface or context.
information policy	Configures a relay agent information reforwarding policy on the DHCP server to identify what the DHCP server should do if a forwarded message already contains relay information.
keep	Indicates that existing information is left unchanged on the DHCP relay agent. This is the default setting.
replace	Indicates that existing information is overwritten on the DHCP relay agent.
server	Specifies the IP address of a DHCP server to which the DHCP relay agent forwards client requests.
ip_address	IP address of the DHCP server. Enter the address in dotted-decimal IP notation (for example, 192.168.11.1).

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the DHCP feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The DHCP relay agent can be configured at both the context and interface level of the ACE. Note the following configuration considerations:

- If you configure the DHCP relay agent at the context level, the configuration is applicable to all interfaces associated with the context.
- If you configure the DHCP relay agent at the interface level, the configuration is applicable to that particular interface only; the remaining interfaces fallback to the context level configuration.

Examples

To set the IP address of a DHCP server at the context level, enter:

```
host1/Admin# changeto C1
host1/C1# config
Enter configuration commands, one per line. End with CNTL/Z
host1/C1(config)# ip dhcp relay enable
host1/C1(config)# ip dhcp relay server 192.168.20.1
```

To specify the DHCP relay at the interface level, enter:

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip dhcp relay enable
host1/Admin(config-if)# ip dhcp relay server 192.168.20.1
```

To remove the IP address of the DHCP server, enter:

```
host1/Admin(config-if)# no ip dhcp relay server 192.168.20.1
```

Related Commands

clear ip
show ip

(config) ip domain-list

To configure a domain name search list, use the **ip domain-list** command. The domain name list can contain a maximum of three domain names. Use the **no** form of this command to remove a domain name from the list.

ip domain-list *name*

no ip domain-list *name*

Syntax Description

name	Domain name. Enter an unquoted text string with no spaces and a maximum of 85 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the domain name feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can configure a Domain Name System (DNS) client on the ACE to communicate with a DNS server to provide hostname-to-IP-address translation for hostnames in CRLs for the client authentication feature. For unqualified hostnames (hostnames that do not contain a domain name), you can configure a default domain name or a list of domain names that the ACE can use to:

- Complete the hostname
- Attempt a hostname-to-IP-address resolution with a DNS server

If you configure both a domain name list and a default domain name, the ACE uses only the domain name list and not the single default name. After you have enabled domain name lookups and configured a domain name list, the ACE uses each domain name in turn until it can resolve a single domain name into an IP address.

Examples

For example, to configure a domain name list, enter:

```
host1/Admin(config)# ip domain-list cisco.com
host1/Admin(config)# ip domain-list foo.com
host1/Admin(config)# ip domain-list xyz.com
```

To remove a domain name from the list, enter:

```
host1/Admin(config)# no ip domain-list xyz.com
```

Related Commands

show running-config

(config) ip domain-lookup

(config) ip domain-name

(config) ip domain-lookup

To enable the ACE to perform a domain lookup (host-to-address translation) with a DNS server, use the **ip domain-lookup** command. By default, this command is disabled. Use the **no** form of this command to return the state of domain lookups to the default value of disabled.

ip domain-lookup

no ip domain-lookup

Syntax Description

This command has no keywords or arguments.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Domain Name feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can configure a Domain Name System (DNS) client on the ACE to communicate with a DNS server to provide hostname-to-IP-address translation for hostnames in CRLs for the client authentication feature.

Before you configure a DNS client on the ACE, ensure that one or more DNS name servers are properly configured and are reachable. Otherwise, translation requests (domain lookups) from the DNS client will be discarded. You can configure a maximum of three name servers. The ACE attempts to resolve the hostnames with the configured name servers in order until the translation succeeds. If the translation fails, the ACE reports an error.

For unqualified hostnames (hostnames that do not contain a domain name), you can configure a default domain name or a list of domain names that the ACE can use to do the following:

- Complete the hostname
- Attempt a hostname-to-IP-address resolution with a DNS server

Examples

For example, to enable domain lookups, enter:

```
host1/Admin(config)# ip domain-lookup
```

To return the state of domain lookups to the default value of disabled, enter:

```
host1/Admin(config)# no ip domain-lookup
```

Related Commands

show running-config

(config) ip domain-list

(config) ip domain-name

(config) ip name-server

(config) ip domain-name

To configure a default domain name, use the **ip domain-name** command. The domain name list can contain a maximum of three domain names. Use the **no** form of this command to remove a domain name from the list.

ip domain-list *name*

no ip domain-list *name*

Syntax Description

name	Default domain name. Enter an unquoted text string with no spaces and a maximum of 85 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the domain name feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The DNS client feature allows you to configure a default domain name that the ACE uses to complete unqualified hostnames. An unqualified hostname does not contain a domain name (any name without a dot). When domain lookups are enabled and a default domain name is configured, the ACE appends a dot (.) and the configured default domain name to the unqualified host name and attempts a domain lookup.

Examples

For example, to specify a default domain name of cisco.com, enter:

```
host1/Admin(config)# ip domain-name cisco.com
```

In the above example, the ACE appends cisco.com to any unqualified host name in a CRL before the ACE attempts to resolve the host name to an IP address using a DNS name server.

To remove the default domain from the configuration, enter:

```
host1/Admin(config)# no ip domain-name cisco.com
```

Related Commands

show running-config
(config) ip domain-list
(config) ip domain-lookup

(config) ip name-server

To configure a DNS name server on the ACE, use the **ip name-server** command. You can configure a maximum of three DNS name servers. Use the **no** form of this command to remove a name server from the list.

ip name-server *ip_address*

no ip name-server *ip_address*

Syntax Description

ip_address	IP address of a name server. Enter the address in dotted decimal notation (for example, 192.168.12.15). You can enter up to three name server IP addresses in one command line.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the domain name feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To translate a hostname to an IP address, you must configure one or more (maximum of three) existing DNS name servers on the ACE. Ping the IP address of each name server before you configure it to ensure that the server is reachable.

Examples

For example, to configure three name servers for the DNS client feature, enter:

```
host1/Admin(config)# ip name-server 192.168.12.15 192.168.12.16 192.168.12.17
```

To remove a name server from the list, enter:

```
host1/Admin(config)# no ip name-server 192.168.12.15
```

Related Commands

show running-config
(config) ip domain-lookup

(config) ip route

To configure a default or static IP route, use the **ip route** command. Use the **no** form of this command to remove a default or static IP route from the configuration.

ip route *dest_ip_prefix netmask gateway_ip_address*

no ip route *dest_ip_prefix netmask gateway_ip_address*

Syntax Description

dest_ip_prefix	IP address for the route. The address that you specify for the static route is the address that is in the packet before entering the ACE and performing network address translation.
netmask	Subnet mask for the route.
gateway_ip_address	IP address of the gateway router (the next-hop address for this route). The gateway address must be in the same network as specified in the **ip address** command for a VLAN interface.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the routing feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The default route identifies the router IP address to which the ACE sends all IP packets for which it does not have a route.

Admin and user contexts do not support dynamic routing. You must use static routes for any networks to which the ACE is not directly connected; for example, use a static route when there is a router between a network and the ACE.

The ACE supports up to eight equal cost routes on the same interface for load balancing.

Routes that identify a specific destination address take precedence over the default route.

See the *Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide* for more information about configuring default or static routes.

Examples

To configure a default route, set the IP address and the subnet mask for the route to 0.0.0.0. For example, if the ACE receives traffic that it does not have a route, it sends the traffic out the interface to the router at 192.168.4.8. Enter:

```
host1/Admin(config)# ip route 0.0.0.0 0.0.0.0 192.168.4.8
```

Related Commands

(config-if) ip address

(config) kalap udp

To configure secure KAL-AP on the ACE, use the **kalap udp** command to access KAL-AP UDP configuration mode. The CLI prompt changes to (config-kalap-udp). Use the **no** form of this command to return to configuration mode (or use the **exit** command).

kalap udp

no kalap udp

Syntax Description

This command has no keywords or arguments.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command requires the probe feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The ACE supports secure KAL-AP for MD5 encryption of data between the ACE and the Global Site Selector (GSS). For encryption, you must configure a shared secret as a key for authentication between the GSS and the ACE context. For information about the commands in KAL-AP UDP configuration mode, see the "KAL-AP UDP Configuration Mode Commands" section.

Examples

To enter KAL-AP UDP configuration mode, enter:

```
host1/Admin(config)# kalap udp
host1/Admin(config-kalap-udp)#
```

Related Commands

show kalap udp load
show running-config
(config-kalap-udp) ip address

(config) ldap-server host

To specify the Lightweight Directory Access Protocol (LDAP) server IP address, the destination port, and other options, use the **ldap-server host** command. You can enter multiple **ldap-server host** commands to configure multiple LDAP servers. Use the **no** form of this command to revert to a default LDAP server authentication setting.

ldap-server host *ip_address* [**port** *port_number*] [**timeout** *seconds*] [**rootDN** *"DN_string"* [**password** *bind_password*]]

no ldap-server host *ip_address* [**port** *port_number*] [**timeout** *seconds*] [**rootDN** *"DN_string"* [**password** *bind_password*]]

Syntax Description

ip_address	IP address for the LDAP server. Enter the address in dotted-decimal IP notation (for example, 192.168.11.1).
port *port_number*	(Optional) Specifies the TCP destination port for communicating authentication requests to the LDAP directory server. The *port_number* argument specifies the LDAP + port number. Enter an integer from 1 to 65535.
timeout *seconds*	(Optional) Specifies the time in seconds to wait for a response from the LDAP server before the ACE can declare a timeout failure with the LDAP server. Use this option to change the time interval that the ACE waits for the LDAP server to reply to an authentication request. Enter an integer from 1 to 60. The default is 5 seconds.
rootDN *"DN_string"*	(Optional) Defines the distinguished name (DN) for a user who is unrestricted by access controls or administrative limit parameters to perform operations on the LDAP server directory. The rootDN user can be thought of as the root user for the LDAP server database. Enter a quoted string with a maximum of 63 alphanumeric characters. The default is an empty string.
password *bind_password*	(Optional) Defines the bind password (rootpw) applied to the rootDN of the LDAP server directory. Enter an unquoted string with a maximum of 63 alphanumeric characters. The default is an empty string.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

By default, the LDAP server port is 389. If your LDAP server uses a port other than 389, use the **port** keyword to configure an appropriate port before starting the LDAP service. The **ldap-server port** command overrides the global setting for the specified server.

By default, the ACE waits 5 seconds for the LDAP server to reply to an authentication request before the ACE declares a timeout failure and attempts to contact the next server in the group. The **ldap-server timeout** command overrides the global setting for the specified server.

Examples

To configure LDAP server authentication parameters, enter:

```
host1/Admin(config)# ldap-server host 192.168.2.3 port 2003
host1/Admin(config)# ldap-server host 192.168.2.3 timeout 60
host1/Admin(config)# ldap-server host 192.168.2.3 rootDN "cn=manager,dc=cisco,dc=com"
password lab
```

To remove the LDAP server authentication setting, enter:

```
host1/Admin(config)# no ldap-server host 192.168.2.3 timeout 60
```

Related Commands

show aaa
(config) aaa group server
(config) ldap-server port
(config) ldap-server timeout

(config) ldap-server port

To globally configure a TCP port (if your LDAP server uses a port other than the default port 389) before you start the LDAP service, use the **ldap-server port** command. This global port setting will be applied to those LDAP servers for which a TCP port value is not individually configured by the **ldap-server host** command. Use the **no** form of this command to revert to the default of TCP port 389.

ldap-server port *port_number*

no ldap-server port *port_number*

Syntax Description

port_number	Destination port to the LDAP server. Enter an integer from 1 to 65535. The default is TCP port 389.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To override the global TCP port setting (specified by the **ldap-server port** command) for a specific server, use the **ldap-server host port** command.

Examples

To globally configure the TCP port, enter:

```
host1/Admin(config)# ldap-server port 2003
```

To revert to the default of TCP port 389, enter:

```
host1/Admin(config)# no ldap-server port 2003
```

Related Commands

show aaa
(config) aaa group server
(config) ldap-server host
(config) ldap-server timeout

(config) ldap-server timeout

To globally change the time interval that the ACE waits for the LDAP server to reply to a response before it declares a timeout failure, use the **ldap-server timeout** command. By default, the ACE waits 5 seconds to receive a response from an LDAP server before it declares a timeout failure and attempts to contact the next server in the group. The ACE applies this global timeout value to those LDAP servers for which a timeout value is not individually configured by the **ldap-server host** command. Use the **no** form of this command to revert to the default of 5 seconds between transmission attempts.

ldap-server timeout *seconds*

no ldap-server timeout *seconds*

Syntax Description

seconds	Timeout value in seconds. Enter an integer from 1 to 60. The default is 5 seconds.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To override the global TCP timeout setting (specified by the **ldap-server timeout** command) for a specific server, use the **ldap-server host timeout** command.

Examples

To globally configure the timeout value to 30 seconds, enter:

```
host1/Admin(config)# ldap-server timeout 30
```

To change to the default of 5 seconds between transmission attempts, enter:

```
host1/Admin(config)# no ldap-server timeout 30
```

Related Commands

show aaa
(config) aaa group server
(config) ldap-server host
(config) ldap-server port

(config) line vty

To configure the virtual terminal line settings, use the **line vty** configuration mode command. When you enter this command, the prompt changes (config-line) and you enter the line configuration mode. Use the **no** form of this command to reset the line configuration mode parameter to its default setting.

line vty

no line vty

Syntax Description

This command has no keywords or arguments.

Command Modes

Configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the commands in line configuration mode, see the "Line Configuration Mode Commands" section.

Examples

To enter the line configuration mode, enter:

```
host1/Admin(config)# line vty
host1/Admin(config-line)#
```

Related Commands

clear line
show line

(config) login timeout

To modify the length of time that a user can be idle before the ACE terminates the console, Telnet, or Secure Shell (SSH) session, use the **login timeout** command. By default, the inactivity timeout value is 5 minutes. Use the **no** form of this command to restore the default timeout value of 5 minutes.

login timeout *minutes*

no login timeout

Syntax Description

minutes	Length of time in minutes. Enter a value from 0 to 60 minutes. A value of 0 instructs the ACE never to time out. The default is 5 minutes.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To specify a timeout period of 10 minutes, enter:

```
host1/Admin(config)# login timeout 10
```

To restore the default timeout value of 5 minutes, enter.

```
host1/Admin(config)# no login timeout
```

Related Commands

telnet
(config-cmap-mgmt) match protocol

(config) logging buffered

To enable system logging to a local buffer and to limit the messages sent to the buffer based on severity, use the **logging buffered** command. By default, logging to the local buffer on the ACE is disabled. New messages are appended to the end of the buffer. The first message displayed is the oldest message in the buffer. When the log buffer fills, the ACE deletes the oldest message to make space for new messages. Use the **no** form of this command to disable message logging.

logging buffered *severity_level*

no logging buffered

Syntax Description

severity_level	Maximum level for system log messages sent to the buffer. The severity level that you specify indicates that you want syslog messages at that level and below. Allowable entries are as follows: • **0**—emergencies (system unusable messages) • **1**—alerts (take immediate action) • **2**—critical (critical condition) • **3**—errors (error message) • **4**—warnings (warning message) • **5**—notifications (normal but significant condition) • **6**—informational (information message) • **7**—debugging (debug messages)

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To set the logging buffer level to 3 for logging error messages, enter:

```
host1/Admin(config)# logging buffered 3
```

To disable message logging, enter:

```
host1/Admin(config)# no logging buffered
```

Related Commands

(config) logging enable

(config) logging console

To enable the logging of syslog messages during console sessions and to limit the display of messages based on severity, use the **logging console** command. By default, the ACE does not display syslog messages during console sessions. Use the **no** form of this command to disable logging to the console.

logging console *severity_level*

no logging console

Syntax Description

severity_level	Maximum level for system log messages sent to the console. The severity level that you specify indicates that you want to log messages at that level and below. Allowable entries are as follows: • **0**—emergencies (system unusable messages) • **1**—alerts (take immediate action) • **2**—critical (critical condition) • **3**—errors (error message) • **4**—warnings (warning message) • **5**—notifications (normal but significant condition) • **6**—informational (information message) • **7**—debugging (debug messages)

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Logging to the console can degrade system performance. Use the **logging console** command only when you are testing and debugging problems, or when there is minimal load on the network. We recommend that you use the lowest severity level possible because logging at a high rate may affect ACE performance. Do not use this command when the network is busy.

Examples

To enable system logging to the console for messages with severity levels of 2, 1, and 0:

```
host1/Admin(config)# logging console 2
```

Related Commands

(config) logging enable

(config) logging device-id

To specify that the device ID of the ACE is included in the syslog message, use the **logging device-id** command. If enabled, the ACE displays the device ID in all non-EMBLEM-formatted syslog messages. The device ID specification does not affect the syslog message text that is in the EMBLEM format. Use the **no** form of this command to disable device ID logging for the ACE in the syslog message.

logging device-id {**context-name** | **hostname** | **ipaddress** *interface_name* | **string** *text*}

no logging device-id

Syntax Description

context-name	Specifies the name of the current context as the device ID to uniquely identify the syslog messages sent from the ACE.
hostname	Specifies the hostname of the ACE as the device ID to uniquely identify the syslog messages sent from the ACE.
ipaddress *interface_name*	Specifies the IP address of the interface as the device ID to uniquely identify the syslog messages sent from the ACE. You can specify the IP address of a VLAN interface or BVI as the device ID. If you use the **ipaddress** keyword, syslog messages sent to an external server contain the IP address of the interface specified, regardless of which interface the ACE uses to send the log data to the external server. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
string *text*	Specifies a text string to uniquely identify the syslog messages sent from the ACE. The maximum length is 64 alphanumeric characters without spaces. You cannot use the following characters: & (ampersand), ‘ (single quotation mark), “ (double quotation marks), < (less than), > (greater than), or ? (question mark).

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The device ID part of the syslog message is viewed through the syslog server only and not directly on the ACE. The device ID does not appear in EMBLEM-formatted messages, Simple Network Management Protocol (SNMP) traps, or on the ACE console, management session, or buffer.

Examples

To instruct the ACE to use the hostname of the ACE to uniquely identify the syslog messages, enter:

```
host1/Admin(config)# logging device-id hostname
```

To disable the use of the hostname of the ACE, enter:

```
host1/Admin(config)# no logging device-id
```

Related Commands (config) logging enable

(config) logging enable

To enable message logging, use the **logging enable** command. Message logging is disabled by default. You must enable logging if you want to send messages to one or more output locations. Use the **no** form of this command to stop message logging to all output locations.

logging enable

no logging enable

Syntax Description

This command has no keywords or arguments.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Message logging is disabled by default. When enabled, log messages are sent to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages. You must set a logging output location to view any logs.

Examples

To enable message logging to all output locations, enter:

```
host1/Admin(config)# logging enable
```

To stop message logging to all output locations, enter:

```
host1/Admin(config)# no logging enable
```

Related Commands

This command has no related commands.

(config) logging facility

To change the logging facility to a value other than the default of 20 (LOCAL4), use the **logging facility** command. Most UNIX systems expect the messages to use facility 20. The ACE allows you to change the syslog facility type to identify the behavior of the syslog daemon (syslogd) on the host. Use the **no** form of this command to set the syslog facility to its default of 20.

logging facility *number*

no logging facility *number*

Syntax Description

number	Syslog facility. Enter an integer from 16 (LOCAL0) to 23 (LOCAL7). The default is 20 (LOCAL4).

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The syslog daemon uses the specified syslog facility to determine how to process messages. Each logging facility configures how the syslog daemon on the host handles a message. Syslog servers file messages based on the facility number in the message. For more information on the syslog daemon and facility levels, see your syslog daemon documentation.

Examples

To set the syslog facility as 16 (LOCAL0) in syslog messages, enter:

```
host1/Admin(config)# logging facility 16
```

To change the syslog facility back to the default of LOCAL4, enter:

```
host1/Admin(config)# no logging facility 16
```

Related Commands

(config) logging enable

(config) logging fastpath

To enable the logging of connection setup and teardown messages through the fastpath, use the **logging fastpath** command. By default, the ACE logs connection setup and teardown syslog messages through the control plane. Use the **no** form of this command to disable the logging of connection setup and teardown syslog messages.

logging fastpath

no logging fastpath

Syntax Description

This command has no keywords or arguments.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Because of the large number of syslog messages that are generated by connection setup and teardown, you can instruct the ACE to send these syslogs through the fast path instead of the control plane. The fast path supports a much higher rate of syslogs than the control plane does. When you instruct the ACE to send these syslogs through the fast path, the message formatting changes (different message spacing) and the syslog IDs change from 106023, 302022, 302023, 302024, and 302025 to 106028, 302028, 302029, 302030, and 302031, respectively.

Examples

To configure the ACE to log connection setup and teardown syslog messages, enter:

```
host1/Admin(config)# logging fastpath
```

To disable the ACE from logging connection setup and teardown syslog messages, enter:

```
host1/Admin(config)# no logging fastpath
```

Related Commands

(config) logging enable

(config) logging history

To set the Simple Network Management Protocol (SNMP) message severity level when sending log messages to a network management system (NMS), use the **logging history** command. Use the **no** form of this command to disable logging of informational system messages to an NMS.

logging history *severity_level*

no logging history

Syntax Description

severity_level	Maximum level system log messages sent as traps to the NMS. The severity level that you specify indicates that you want to log messages at that level and below. Allowable entries are as follows: • **0**—emergencies (system unusable messages) • **1**—alerts (take immediate action) • **2**—critical (critical condition) • **3**—errors (error message) • **4**—warnings (warning message) • **5**—notifications (normal but significant condition) • **6**—informational (information message) • **7**—debugging (debug messages)

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To enable or disable all SNMP syslog message logging, use the **logging history** command without the *severity_level* argument.

We recommend that you use the debugging (7) level during initial setup and during testing. After setup, set the level from debugging (7) to a lower value for use in your network.

Examples

To send informational system message logs to an SNMP NMS, enter:

```
host1/Admin(config)# logging history 6
```

To disable logging to an SNMP NMS, enter:

```
host1/Admin(config)# no logging history
```

Related Commands (config) logging enable

(config) logging host

To specify a host (the syslog server) that receives the syslog messages sent by the ACE, use the **logging host** command. You can use multiple **logging host** commands to specify additional servers to receive the syslog messages. Use the **no** form of this command to disable logging to a syslog server. By default, logging to a syslog server on a host is disabled on the ACE.

logging host *ip_address* [**tcp** | **udp** [*/port#*] | [**default-udp**] | [**format emblem**]]

no logging host *ip_address*

Syntax Description

ip_address	IP address of the host to be used as the syslog server.
tcp	(Optional) Specifies to use TCP to send messages to the syslog server. A server can only be specified to receive either UDP or TCP, not both.
udp	(Optional) Specifies to use UDP to send messages to the syslog server. A server can only be specified to receive either UDP or TCP, not both.
/port#	(Optional) Port that the syslog server listens to for syslog messages. Enter an integer from 1025 to 65535. The default protocol and port are UDP/514. The default TCP port, if specified, is 1470.
default-udp	(Optional) Instructs the ACE to default to UDP if the TCP transport fails to communicate with the syslog server.
format emblem	(Optional) Enables EMBLEM-format logging for each syslog server. The Cisco Resource Management Environment (RME) is a network management application that collects syslogs. RME can process syslog messages only if they are in EMBLEM format.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

If you choose to send log messages to a host, the ACE sends those messages using either UDP or TCP. The host must run a program (known as a server) called syslogd, a daemon that accepts messages from other applications and the network, and writes them out to system wide log files. UNIX provides the syslog server as part of its operating system. If you are running Microsoft Windows, you must obtain a syslog server for the Windows operating system.

If you use TCP as the logging transport protocol, the ACE denies new network access sessions if the ACE is unable to reach the syslog server, if the syslog server is misconfigured, if the TCP queue is full, or if the disk is full.

The **format emblem** keywords allow you to enable EMBLEM-format logging for each syslog server. EMBLEM-format logging is available for either TCP or UDP syslog messages. If you enable EMBLEM-format logging for a particular syslog host, then the messages are sent to that host. If you also enable the **logging timestamp** command, the messages are sent to the syslog server with a time stamp.

For example, the EMBLEM format for a message with a time stamp appears as follows:

```
ipaddress or dns name [Dummy Value/Counter]: [mmm dd hh:mm:ss TimeZone]:
%FACILITY-[SUBFACILITY-]SEVERITY-MNEMONIC: [vtl-ctx: context id] Message-text
```

Examples

To send log messages to a syslog server, enter:

```
host1/Admin(config)# logging host 192.168.10.1 tcp/1025 format emblem default-udp
```

To disable logging to a syslog server, enter:

```
host1/Admin(config)# no logging host 192.168.10.1
```

Related Commands

(config) logging enable
(config) logging timestamp

(config) logging message

To control the display of a specific system logging message or to change the severity level associated with the specified system logging message, use the **logging message** command. Use the **no** form of this command to disable logging of the specified syslog message.

logging message *syslog_id* [**level** *severity_level*]

no logging message *syslog_id*

Syntax Description

syslog_id	Specific message that you want to disable or to enable.
level *severity_level*	(Optional) Changes the severity level associated with a specific system log message. For example, the %<ACE>-4-411001 message listed in the syslog has the default assigned severity level of 4 (warning message). You can change the assigned default severity level to a different level. Allowable entries are as follows: • **0**—emergencies (system unusable messages) • **1**—alerts (take immediate action) • **2**—critical (critical condition) • **3**—errors (error message) • **4**—warnings (warning message) • **5**—notifications (normal but significant condition) • **6**—informational (information message) • **7**—debugging (debug messages)

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can use the **show logging** command to determine the level currently assigned to a message and whether the message is enabled.

For information on syslog messages and their IDs, see the *Cisco 4700 Series Application Control Engine Appliance Command Reference*.

Examples

To disable the %<ACE>-6-615004 syslog message (VLAN available for configuring an interface), enter:

```
host1/Admin(config)# no logging message 615004
```

To resume logging of the disabled syslog message, enter:

```
host1/Admin(config)# logging message 615004 level 6
```

To change the severity level of the 615004 syslog message from the default of 6 (informational) to a severity level of 5 (notification), enter:

```
(config)# logging message 615004 level 5
```

To return the severity level of the 615004 syslog message to the default of 6, enter:

```
host1/Admin(config)# no logging message 615004
```

Related Commands

(config) logging enable

(config) logging monitor

To display syslog messages as they occur when accessing the ACE through a Secure Shell (SSH) or a Telnet session, use the **logging monitor** command. You can limit the display of messages based on severity. By default, logging to a remote connection using the SSH or Telnet is disabled on the ACE. Use the **no** form of this command to disable system message logging to the current Telnet or SSH session.

logging monitor *severity_level*

no logging monitor

Syntax Description

severity_level	Maximum level for system log messages displayed during the current SSH or Telnet session. The severity level that you specify indicates that you want to log messages at that level and below. Allowable entries are as follows: • **0**—emergencies (system unusable messages) • **1**—alerts (take immediate action) • **2**—critical (critical condition) • **3**—errors (error message) • **4**—warnings (warning message) • **5**—notifications (normal but significant condition) • **6**—informational (information message) • **7**—debugging (debug messages)

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Note Before you can use this command, you must enable remote access on the ACE and establish a remote connection using the SSH or Telnet protocols from a PC.

To display logs during the SSH or Telnet session, use the **terminal monitor** Exec mode command. This command enables syslog messages for all sessions in the current context. The **logging monitor** command sets the logging preferences for all SSH and Telnet sessions, while the **terminal monitor** command controls logging for each individual Telnet session. However, in each session, the **terminal monitor** command controls whether syslog messages appear on the terminal during the session.

Examples

To send informational system message logs to the current Telnet or SSH session, enter:

```
host1/Admin# terminal monitor
host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
host1/Admin(config)# logging monitor 6
```

To disable system message logging to the current Telnet or SSH session, enter:

```
host1/Admin(config)# no logging monitor
```

Related Commands

(config) logging enable

(config) logging persistent

To send specific log messages to compact flash on the ACE, use the **logging persistent** command. By default, logging to compact flash is disabled on the ACE. The ACE allows you to specify the system message logs that you want to keep after a system reboot by saving them to compact flash. Use the **no** form of this command to disable logging to compact flash.

logging persistent *severity_level*

no logging persistent

Syntax Description

severity_level	Maximum level for system log messages sent to compact flash. The severity level that you specify indicates that you want to log messages at that level and below. Allowable entries are as follows: • **0**—emergencies (system unusable messages) • **1**—alerts (take immediate action) • **2**—critical (critical condition) • **3**—errors (error message) • **4**—warnings (warning message) • **5**—notifications (normal but significant condition) • **6**—informational (information message) • **7**—debugging (debug messages)

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

We recommend that you use a lower severity level, such as severity level 3, because logging at a high rate to flash memory on the ACE might affect performance.

Examples

To send informational system message logs to flash memory on the ACE, enter:

```
host1/Admin(config)# logging persistent 6
```

To disable logging to flash memory on the ACE, enter:

```
host1/Admin(config)# no logging persistent
```

Related Commands

(config) logging enable

(config) logging queue

To change the number of syslog messages that can appear in the message queue, use the **logging queue** command. By default, the ACE can hold 80 syslog messages in the message queue while awaiting processing. Use the **no** form of this command to reset the logging queue size to the default of 100 messages.

logging queue *queue_size*

no logging queue *queue_size*

Syntax Description

queue_size	Queue size for storing syslog messages. Enter an integer from 1 to 8192. The default is 80 messages.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Set the queue size before the ACE processes syslog messages. When traffic is heavy, messages might get discarded.

Examples

To set the size of the syslog message queue to 1000, enter:

```
host1/Admin(config)# logging queue 1000
```

To reset the logging queue size to the default of 80 messages, enter:

```
host1/Admin(config)# no logging queue 0
```

Related Commands

(config) logging enable

(config) logging rate-limit

To limit the rate at which the ACE generates messages in the syslog, use the **logging rate-limit** command. You can limit the number of syslog messages generated by the ACE for specific messages. Use the **no** form of this command to disable rate limiting for message logging in the syslog.

logging rate-limit {*num* {*interval* | **level** *severity_level* | **message** *syslog_id*} | **unlimited** {**level** *severity_level* | **message** *syslog_id*}}

no logging rate-limit {*num* {*interval* | **level** *severity_level* | **message** *syslog_id*} | **unlimited** {**level** *severity_level* | **message** *syslog_id*}}

Syntax Description

num	Number at which the syslog is to be rate limited.
interval	Time interval in seconds over which the system message logs should be limited. The default time interval is 1 second.
level *severity_level*	Specifies the syslog level that you want to rate limit. Allowable entries are as follows: • **0**—emergencies (system unusable messages) • **1**—alerts (take immediate action) • **2**—critical (critical condition) • **3**—errors (error message) • **4**—warnings (warning message) • **5**—notifications (normal but significant condition) • **6**—informational (information message) • **7**—debugging (debug messages)
message *syslog_id*	Identifies the ID of the specific message you want to suppress reporting.
unlimited	Disables rate limiting for messages in the syslog.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Disabled rate limiting is the default setting. In this case, the **logging rate-limit unlimited** command will not be displayed in the ACE running-configuration file.

The severity level you enter indicates that you want all syslog messages at the specified level to be rate-limited. For example, if you specify a severity level of 7, the ACE applies a rate limit only to level 7 (debugging messages). If you want to apply a logging rate limit on a different severity level, you must configure the **logging rate-limit level** command for that level as well.

If you configure rate limiting for syslogs 302028 through 302031 (connection setup and teardown syslogs that are formatted in the data plane), the ACE always rate-limits these syslogs at level 6. Even if you change the logging level to a different value using the **logging message** command and the new logging level appears on the syslog server or other destination, the ACE will continue to rate-limit these syslogs at level 6.

For information on syslog messages and their IDs, see the *Cisco 4700 Series Application Control Engine Appliance Command Reference*.

Examples

To limit the syslog rate to a 60-second time interval for informational messages (level 6), enter:

```
host1/Admin(config)# logging rate-limit 42 60 level 6
```

To suppress reporting of system message 302022, enter:

```
host1/Admin(config)# logging rate-limit 42 60 302022
```

To disable rate limiting, enter:

```
host1/Admin(config)# no logging rate-limit 42 60 level 6
```

Related Commands

(config) logging enable

(config) logging standby

To enable logging on the standby ACE in a redundant configuration, use the **logging standby** command. When enabled, the standby ACE syslog messages remain synchronized should a failover occur. When enabled, this command causes twice the message traffic on the syslog server. Use the **no** form of this command to disable logging on the standby ACE.

logging standby

no logging standby

Syntax Description

This command has no keywords or arguments.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

This command is disabled by default.

Examples

To enable logging on the failover standby ACE:

```
host1/Admin(config)# logging standby
```

To disable logging on the standby ACE, enter:

```
host1/Admin(config)# no logging standby
```

Related Commands

(config) logging enable

(config) logging timestamp

To specify that syslog messages should include the date and time that the message was generated, use the **logging timestamp** command. By default, the ACE does not include the date and time in syslog messages. Use the **no** form of this command to specify that the ACE not include the date and time when logging syslog messages.

logging timestamp

no logging timestamp

Syntax Description

This command has no keywords or arguments.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

This command is disabled by default.

Examples

To enable the time stamp on system logging messages, enter:

```
host1/Admin(config)# logging timestamp
```

To disable the time stamp from syslog messages, enter:

```
host1/Admin(config)# no logging timestamp
```

Related Commands

(config) logging enable

(config) logging trap

To identify which messages are sent to a syslog server, use the **logging trap** command. This command limits the logging messages sent to a syslog server based on severity. Use the **no** form of this command to return the trap level to the default (information messages).

logging trap *severity_level*

no logging trap

Syntax Description

severity_level	Maximum level for system log messages. The severity level that you specify indicates that you want to log messages at that level and below. Allowable entries are as follows: • **0**—emergencies (system unusable messages) • **1**—alerts (take immediate action) • **2**—critical (critical condition) • **3**—errors (error message) • **4**—warnings (warning message) • **5**—notifications (normal but significant condition) • **6**—informational (information message) • **7**—debugging (debug messages)

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To send logging messages to a syslog server, use the **logging host** command to specify the name or IP address of the host to be used as the syslog server.

Examples

To send informational system message logs to the syslog server, enter:

```
host1/Admin(config)# logging trap 6
```

To disable sending message logs to the syslog server, enter:

```
host1/Admin(config)# no logging trap 6
```

Related Commands

(config) logging enable
(config) logging host

(config) object-group

To create an object group, use the **object-group** command. Object groups allow you to streamline the creation of multiple ACL entries in an ACL. Use the **no** form of this command to remove the object group from the configuration.

object-group [**network** | **service**] *name*

no object-group [**network** | **service**] *name*

Syntax Description

network	Specifies a group of hosts or subnet IP addresses.
service	Specifies a group of TCP or UDP port specifications.
name	Unique identifier for the object group. Enter the object group name as an unquoted, alphanumeric string from 1 to 64 characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

You can create either network or service object groups. After you create these groups, you can use a single ACL entry to allow trusted hosts to make specific service requests to a group of public servers.

If you add new members to an existing object group that is already in use by an entry in a large ACL, recommitting the ACL can take a long time, depending on the size of the ACL and the object group. In some cases, making this change can cause the ACE to devote over an hour to committing the ACL, during which time you cannot access the terminal. We recommend that you first remove the ACL entry that refers to the object group, make your change, and then add the ACL entry back into the ACL.

Examples

To create a network object group, enter:

```
host1/Admin(config)# object-group network NET_OBJ_GROUP1
```

Related Commands

(config-objgrp-netw) ip_address netmask

(config-objgrp-netw) host

(config) ntp

To configure the ACE system clock to synchronize a peer (or to be synchronized by a peer) or to be synchronized by a time server, use the **ntp** command. Use the **no** form of the command to remove an NTP peer or server from the configuration.

ntp {**peer** *ip_address1* [**prefer**] | **server** *ip_address2* [**prefer**]}

no ntp {**peer** *ip_address1* [**prefer**] | **server** *ip_address2* [**prefer**]}

Syntax Description

peer	Configures the ACE system clock to synchronize a peer or to be synchronized by a peer. You can specify multiple associations.
ip_address1	IP address of the peer providing or being provided by the clock synchronization.
prefer	(Optional) Makes this peer the preferred peer that provides synchronization. Using the **prefer** keyword reduces switching back and forth between peers.
server	Configures the ACE system clock to be synchronized by a time server. You can specify multiple associations.
ip_address2	IP address of the time server that provides the clock synchronization.
prefer	(Optional) Makes this server the preferred server that provides synchronization. Use the **prefer** keyword to set this NTP server as the preferred server if multiple servers have similar accuracy. NTP uses an algorithm to determine which server is the most accurate and synchronizes to that one. If servers have similar accuracy, then the **prefer** keyword specifies which of those servers to use.

Command Modes

Configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

An NTP association can be a peer association, which means that the ACE is willing to synchronize to the other system or to allow the other system to synchronize to the ACE. An NTP association can also be a server association, which means that only this system will synchronize to the other system, not the other way around. You can identify multiple servers; the ACE uses the most accurate server.

To send logging messages to a syslog server, use the **logging host** command to specify the name or IP address of the host to be used as the syslog server.

Examples

To specify multiple NTP server IP addresses and identify a preferred server, enter:

```
host1/Admin(config)# ntp server 192.168.10.10 prefer
host1/Admin(config)# ntp server 192.168.4.143
host1/Admin(config)# ntp server 192.168.5.10
```

To form a peer association with a preferred peer, enter:

```
host1/Admin(config)# ntp peer 192.168.10.0 prefer
```

To remove an NTP peer or server from the configuration, enter:

```
host1/Admin(config)# no ntp peer 192.168.10.0
```

Related Commands

clear ntp statistics
show clock

(config) optimize

To configure the global optimization settings on the ACE, enter the **optimize** command. The CLI prompt changes to (config-optimize). To remove an optimize mode selection, use the **no** form of the command.

optimize

no optimize

Syntax Description

This command has no keywords or arguments.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about commands in optimize configuration mode, see the "Optimize Configuration Mode Commands" section. For details about configuring the commands in the optimize configuration mode, see the *Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide*.

Examples

To access the optimize configuration mode, enter:

```
host1/Admin(config)# optimize
host1/Admin(config-optimize)#
```

Related Commands

show optimization-global

(config) parameter-map type

To create a connection-, HTTP-, optimization HTTP-, or SSL-type parameter map, use the **parameter-map type** command. Use the **no** form of this command to remove a parameter map from the ACE.

parameter-map type {**connection** | **generic** | **http** | **optimization http** | **rtsp** | **sip** | **skinny** | **ssl**} *name*

no parameter-map type {**connection** | **generic** | **http** | **optimization http** | **rtsp** | **sip** | **skinny** | **ssl**} *name*

Syntax Description

connection	Specifies a connection-type parameter map. After you create the connection-type parameter map, you configure TCP, IP, and other settings for the map in the parameter map connection configuration mode. For information about the commands in parameter map connection configuration mode, see the "Parameter Map Connection Configuration Mode Commands" section.
dns	Specifies a DNS parameter map. After you create a DNS parameter map, you configure settings for the map in the parameter map DNS configuration mode. For information about the commands in parameter map DNS configuration mode, see the "Parameter Map DNS Configuration Mode Commands" section.
generic	Specifies a generic Layer 7 parameter map. After you create the generic Layer 7 parameter map, you configure settings for the map in the parameter map generic configuration mode. For information about the commands in parameter map generic configuration mode, see the "Parameter Map HTTP Configuration Mode Commands" section.
http	Specifies an HTTP-type parameter map. After you create the HTTP-type parameter map, you configure HTTP settings for the map in the parameter map HTTP configuration mode. For information about the commands in parameter map HTTP configuration mode, see the "Parameter Map HTTP Configuration Mode Commands" section.
optimization http	Specifies an optimization HTTP-type parameter map and define its application acceleration and optimization settings. After you create the optimization HTTP-type parameter map, you configure settings for the map in the parameter map optimization HTTP configuration mode. For information about the commands in parameter map HTTP connection configuration mode, see the "Parameter Map Optimization Configuration Mode Commands" section.
rtsp	Specifies an RTSP-type parameter map. After you create the RTSP-type parameter map, you configure RTSP settings for the map in the parameter map RTSP configuration mode. For information about the commands in parameter map RTSP configuration mode, see the "Parameter Map RTSP Configuration Mode Commands" section.
sip	Specifies a SIP-type parameter map. After you create the SIP-type parameter map, you configure SIP settings for the map in the parameter map SIP configuration mode. For information about the commands in parameter map SIP configuration mode, see the "Parameter Map SIP Configuration Mode Commands" section.
skinny	Specifies a Skinny Client Control Protocol (SCCP) type parameter map. After you create the SCCP-type parameter map, you configure SCCP settings for the map in the parameter map SCCP configuration mode. For information about the commands in parameter map SCCP configuration mode, see the "Parameter Map SCCP Configuration Mode Commands" section.

ssl	Specifies an SSL-type parameter map. After you create the SSL-type parameter map, you configure SSL settings for the map in the parameter map SSL configuration mode. For information about the commands in parameter map SSL connection configuration mode, see the "Parameter Map SSL Configuration Mode Commands" section.
name	Name assigned to the parameter map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised.

Usage Guidelines

The **connection** and **http** commands requires the connection feature in your user role. The **optimization http** commands in this mode require the loadbalance feature in your user role. The **ssl** commands in this mode require the connection or SSL feature. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The **parameter-map type** command allows you to configure a series of Layer 3 and Layer 4 statements that instruct the ACE how to handle TCP termination, normalization and reuse, SSL termination, and advanced HTTP behavior for server load-balancing connections. After you enter this command, the system enters the corresponding parameter map configuration mode.

To access one of the parameter-map configuration modes, enter the appropriate **parameter-map type** command. For example, enter **parameter-map type connection**, **parameter-map type http**, or **parameter-map type ssl**. The CLI prompt changes to the corresponding mode, for example, (config-parammap-conn), (config-parammap-http), or (config-parammap-ssl).

After you configure the parameter map, you associate it with a specific action statement in a policy map.

Examples

To create a connection-type parameter map called TCP_MAP, enter:

```
host1/Admin(config)# parameter-map type connection TCP_MAP
host1/Admin(config-parammap-conn)#
```

To create an HTTP-type parameter map called HTTP_MAP, enter:

```
host1/Admin(config)# parameter-map type http HTTP_MAP
host1/Admin(config-parammap-http)#
```

To create an optimization HTTP parameter map called OPTIMIZE_MAP, enter:

```
host1/Admin(config)# parameter-map type optimization http OPTIMIZE_MAP
host1/Admin(config-parammap-optmz)#
```

To create an SSL-type parameter map called SSL_MAP, enter:

```
host1/Admin(config)# parameter-map type ssl SSL_MAP
host1/Admin(config-parammap-ssl)#
```

Related Commands

show running-config
(config) policy-map

(config) peer hostname

To specify a hostname for the peer ACE in a redundant configuration, use the **peer hostname** command. The hostname is used for the command line prompts and default configuration filenames. If you establish sessions to multiple devices, the hostname helps you track where you enter commands. Use the **no** form of this command to reset the hostname of the peer to the default of switch.

peer hostname *name*

no peer hostname *name*

Syntax Description

name	New hostname for the peer ACE. Enter a case-sensitive text string that contains from 1 to 32 alphanumeric characters.

Command Modes

Configuration mode

Admin context only

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

By default, the hostname for the ACE is switch.

Examples To change the hostname of the peer ACE from switch to ACE_1, enter:

```
switch/Admin(config)# peer hostname ACE_1
ACE_1/Admin(config)#
```

Related Commands **(config) hostname**

(config) peer shared-vlan-hostid

To configure a specific bank of MAC addresses for a peer ACE in a redundant configuration, use the **peer shared-vlan-hostid** command. Use the **no** form of this command to remove the configured bank of MAC addresses.

peer shared-vlan-hostid *number*

no peer shared-vlan-hostid

Syntax Description

number	Bank of MAC addresses that the ACE uses. Enter a number from 1 to 16. Be sure to configure different bank numbers for multiple ACEs.

Command Modes Configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines This command requires the interface feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples To configure bank 3 for a peer ACE, enter:

```
host1/Admin(config)# peer shared-vlan-hostid 3
```

To remove the configured bank of MAC addresses, enter:

```
host1/Admin(config)# no peer shared-vlan-hostid
```

Related Commands **(config) arp**

(config) shared-vlan-hostid

(config) policy-map

Use the **policy-map** command to create a Layer 3 and Layer 4 or Layer 7 policy map. To access one of the policy map configuration modes, use the **policy-map** command. Use the **no** form of this command to remove a policy map from the ACE.

policy-map multi-match *map_name*

policy-map type inspect {**ftp first-match** | **http all-match** | **sip all-match** | **skinny**} *map_name*

policy-map type loadbalance {**first-match** | **generic first-match** | **http first-match** | **radius first-match** | **rdp first-match** | **rtsp first-match** | **sip first-match**} *map_name*

policy-map type management first-match *map_name*

policy-map type optimization http first-match *map_name*

no policy-map multi-match *map_name*

no policy-map type inspect {**ftp first-match** | **http all-match** | **sip all-match** | **skinny**} *map_name*

no policy-map type loadbalance {**first-match** | **generic first-match** | **http first-match** | **radius first-match** | **rdp first-match** | **rtsp first-match** | **sip first-match**} *map_name*

no policy-map type management first-match *map_name*

Syntax Description

multi-match	Configures a Layer 3 and Layer 4 policy map that defines the different actions applied to traffic passing through the ACE. The ACE attempts to match multiple classes within the Layer 3 and Layer 4 policy map to allow a multifeature Layer 3 and Layer 4 policy map. The ACE executes the action for only one matching class within each of the class sets. The definition of which classes are in the same class set depends on the actions applied to the classes; the ACE associates each policy map action with a specific set of classes. For information about the commands in policy map configuration mode, see the "Policy Map Configuration Mode Commands" section.
map_name	Name assigned to the policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
type	Specifies the type of policy map to be defined. When you specify a policy map type, you enter its corresponding policy map configuration mode (for example, RADIUS load balancing).
inspect ftp first-match	Specifies a Layer 7 policy map that defines the inspection of File Transfer Protocol (FTP) commands by the ACE. The ACE executes the action for the first matching classification. For a list of classes in a policy map, the actions associated with the first class that matches the packet are the actions that the ACE executes on the packet. For information about the commands in policy map FTP inspection configuration mode, see the "Policy Map FTP Inspection Configuration Mode Commands" section.

inspect http all-match	Specifies a Layer 7 policy map that defines the deep packet inspection of the HTTP protocol by the ACE. The ACE attempts to match all specified conditions against the matching classification and executes the actions of all matching classes until it encounters a deny for a match request. For information about the commands in policy map inspection HTTP configuration mode, see the "Policy Map Inspection HTTP Configuration Mode Commands" section.
inspect sip all-match	Specifies a Layer 7 policy map that defines the inspection of SIP protocol packets by the ACE. The ACE attempts to match all specified conditions against the matching classification and executes the actions of all matching classes until it encounters a deny for a match request. For information about the commands in policy map inspection SIP configuration mode, see the "Policy Map Inspection SIP Configuration Mode Commands" section.
inspect skinny	Specifies a Layer 7 policy map that defines the inspection of SCCP or skinny protocol packets by the ACE. The ACE uses the SCCP inspection policy to filter traffic based on message ID and to perform user-configurable actions on that traffic. For information about the commands in policy map inspection SIP configuration mode, see the "Policy Map Inspection Skinny Configuration Mode Commands" section.
loadbalance first-match	Specifies a Layer 7 policy map that defines Layer 7 HTTP server load-balancing decisions. The ACE executes the action for the first matching classification. For a list of classes in a policy-map, the actions associated with the first class that matches the packet are the actions that the ACE executes on the packet. For information about the commands in policy map load balance configuration mode, see the "Policy Map Load Balancing HTTP Configuration Mode Commands" section.
loadbalance generic first-match	Specifies a Layer 7 policy map that defines Layer 7 HTTP server load-balancing decisions. The ACE executes the action for the first matching classification. For a list of classes in a policy-map, the actions associated with the first class that matches the packet are the actions that the ACE executes on the packet. For information about the commands in policy map load balance configuration mode, see the "Policy Map Load Balancing Generic Configuration Mode Commands" section.
loadbalance http first-match	Specifies a Layer 7 policy map that defines Layer 7 HTTP server load-balancing decisions. The ACE executes the action for the first matching classification. For a list of classes in a policy-map, the actions associated with the first class that matches the packet are the actions that the ACE executes on the packet. For information about the commands in policy map load balance configuration mode, see the "Policy Map Load Balancing HTTP Configuration Mode Commands" section.

loadbalance radius first-match	Specifies a Layer 7 policy map that defines Layer 7 HTTP server load-balancing decisions. The ACE executes the action for the first matching classification. For a list of classes in a policy-map, the actions associated with the first class that matches the packet are the actions that the ACE executes on the packet. For information about the commands in policy map load balance configuration mode, see the "Policy Map Load Balancing RADIUS Configuration Mode Commands" section.
loadbalance rdp first-match	Specifies a Layer 7 policy map that defines Layer 7 HTTP server load-balancing decisions. The ACE executes the action for the first matching classification. For a list of classes in a policy-map, the actions associated with the first class that matches the packet are the actions that the ACE executes on the packet. For information about the commands in policy map load balance configuration mode, see the "Policy Map Load Balancing RDP Configuration Mode Commands" section.
loadbalance rtsp first-match	Specifies a Layer 7 policy map that defines Layer 7 HTTP server load-balancing decisions. The ACE executes the action for the first matching classification. For a list of classes in a policy-map, the actions associated with the first class that matches the packet are the actions that the ACE executes on the packet. For information about the commands in policy map load balance configuration mode, see the "Policy Map Load Balancing RDP Configuration Mode Commands" section.
loadbalance sip first-match	Specifies a Layer 7 policy map that defines Layer 7 HTTP server load-balancing decisions. The ACE executes the action for the first matching classification. For a list of classes in a policy-map, the actions associated with the first class that matches the packet are the actions that the ACE executes on the packet. For information about the commands in policy map load balance configuration mode, see the "Policy Map Load Balancing SIP Configuration Mode Commands" section.
management first-match	Specifies a Layer 3 and Layer 4 policy map that defines the IP management protocols that can be received by the ACE. The ACE executes the specified action only for traffic that meets the first matching classification with a policy map. For information about the commands in policy map management configuration mode, see the "Policy Map Management Configuration Mode Commands" section.
optimization http first-match	Specifies a Layer 7 policy map that defines Layer 7 HTTP optimization operations. The Layer 7 optimization HTTP policy map associates an HTTP optimization action list and parameter map to configure the specified optimization actions. The ACE executes the action for the first matching classification. For a list of classes in a policy-map, the actions associated with the first class that matches the packet are the actions that the ACE executes on the packet. For information about the commands in policy map optimization configuration mode, see the "Policy Map Optimization Configuration Mode Commands" section.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised.

Usage Guidelines

This command requires the inspect, loadbalance, NAT, connection, or SSL feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Use the **policy map** configuration mode commands to configure a series of Layer 3 and Layer 4 or Layer 7 policies. Each policy map defines a series of actions (functions) that you apply to a set of classified inbound traffic. The CLI prompt changes correspondingly to the selected policy map configuration mode: config-pmap, config-pmap-c, config-pmap-insp-http, config-pmap-insp-http-c, config-pmap-insp-http-m, config-pmap-lb, config-pmap-lb-c, config-pmap-lb-m, config-pmap-mgmt, config-pmap-mgmt-c, config-pmap-optmz, and config-pmap-optmz-c.

For a Layer 3 and Layer 4 traffic classification, you create Layer 3 and Layer 4 policy maps with actions that configure the following:

- Network management traffic received by the ACE (HTTP, HTTPS, ICMP, SNMP, SSH, or Telnet)
- Server load balancing based on Layer 3 and Layer 4 connection information (virtual IP address)
- Secure Sockets Layer (SSL) security services between a web browser (the client) and the HTTP connection (the server)
- Static or dynamic Network Address Translation (NAT)
- Application protocol inspection (also known as protocol fixup)
- TCP termination, normalization, and reuse
- IP normalization and fragment reassembly

For a Layer 7 traffic classification, you create policy maps with actions that configure the following:

- Server load balancing based on the Layer 7 HTTP-related information (such as HTTP headers, cookies, and URLs), or the client IP address
- Application acceleration and optimization functions
- Deep packet inspection of the HTTP protocol
- FTP command inspection

The ACE supports a system-wide maximum of 4096 policy maps.

For details about creating a policy map, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To create a Layer 3 and Layer 4 server load-balancing policy map named L4_SLB_POLICY, enter:

```
host1/Admin(config)# policy-map multi-match L4_SLB_POLICY
host1/Admin(config-pmap)#
```

To create a Layer 3 and Layer 4 management protocol policy map named L4_MGMT-ACCESS_POLICY, enter:

```
host1/Admin(config)# policy-map type management match-any L4_MGMT-ACCESS_CLASS
```

```
host1/Admin(config-pmap-mgmt)#
```

To create a Layer 7 optimization HTTP policy map named L7OPTIMIZATION_POLICY, enter:

```
host/Admin(config)# policy-map type optimization http first-match L7OPTIMIZATION_POLICY
host/Admin(config-pmap-optmz)#
```

To create a Layer 7 HTTP server load-balancing policy map named L7_SLB_POLICY, enter:

```
host1/Admin(config)# policy-map type loadbalance first-match L7_SLB_POLICY
host1/Admin(config-pmap-lb)#
```

To create a Layer 7 HTTP deep packet inspection policy map named L7_HTTP_INSPECT_POLICY, enter:

```
host/Admin(config) # policy-map type inspect http all-match HTTP_INSPECT_L7POLICY
host/Admin(config-pmap-ins-http)#
```

To create a Layer 7 FTP command inspection policy map named L7_FTP_INSPECT_POLICY, enter:

```
host1/Admin(config)# class-map type ftp inspect match-any L7_FTP_INSPECT_POLICY
host1/Admin(config-pmap-ftp-ins)#
```

Related Commands

show startup-config
(config) class-map
(config) parameter-map type
(config) service-policy

(config) probe

To define a probe and access its configuration mode, use the **probe** command. The CLI prompt changes to (config-*probe_type*). Use the **no** form of this command to delete the probe.

probe *probe_type probe_name*

no probe *probe_type probe_name*

Syntax Description

probe_type	Probe types. The probe type determines what the probe sends to the real server. Enter one of the following keywords: • **dns**—Sends a request to a DNS server giving it a configured domain. To determine if the server is up, the ACE must receive the configured IP address for that domain. • **echo** {**tcp** | **udp**}—Sends a string to the server and compares the response to the original string. If the response string matches the original string, the server is marked as passed. Otherwise, the ACE retries a configured number of times and time interval before the server is marked as failed. • **finger**—Sends a Finger probe to a server to verify a defined username is a username on the server. Use the Finger protocol to configure the username string.

- **ftp**—Initiates an FTP session. By default, this probe is for an anonymous login with the option of configuring a user ID and password. The ACE performs an FTP GET or LS to determine the outcome of the probe. This probe supports only active connections.
- **http**—Sets up a TCP connection and issues an HTTP request. The default request is an HTTP 1.1 GET request with the URL /. Any valid HTTP response causes the probe to mark the real server as passed. You can also configure an HTTP response value.
- **https**—Similar to the HTTP probe, but this probe uses SSL to generate encrypted data.
- **icmp**—Sends an ICMP request and listens for a response. If the server returns a response, the ACE marks the real server as passed. If there is no response and the time times out, or an ICMP standard error such as DESTINATION_UNREACHABLE occurs, the ACE marks the real server as failed.
- **imap**—Identical to POP/POP3 probe, but uses IMAP.
- **pop**—Initiates a POP session, using a configured user ID and password. Then, the probe attempts to retrieve e-mail from the server and validates the result of the probe based on the return codes received from the server.
- **radius**—Connects to a RADIUS server and logs into it to determine whether the server is up.
- **rtsp**—Establishes a TCP connection and sends a request packet to the RTSP server to determine whether the server is up.
- **scripted**—Executes probes from a configured script to perform health probing. You can author specific scripts with features not present in standard health probes.
- **sip** {**tcp** | **udp**}— Establishes a TCP or UDP connection and sends an OPTIONS request packet to the user agent on the SIP server to determine whether the server is up.
- **smtp**—Initiates an SMTP session by logging into the server.
- **snmp**—Establishes a UDP connection and sends a maximum of eight SMNP OID queries to probe the server.
- **tcp**—Initiates a TCP handshake and expects a response. By default, a successful response causes the probe to mark the server as passed, and then the probe sends a FIN to end the session. If the response is not valid or if there is no response, the probe marks the real server as failed.
- **telnet**—Establishes a connection to the real server and verifies that a greeting from the application was received.
- **udp**—Sends a UDP packet to a real server. The probe marks the server as failed only if an ICMP Port Unreachable message is returned. Optionally, you can configure this probe to send specific data and expect a specific response to mark the real server as passed.

probe_name	Identifier for the probe. The probe name associates the probe to the real server. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised.

Usage Guidelines

This command requires the probe feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about commands in probe configuration mode, see the "Probe Configuration Mode Commands" section.

Examples

To define a TCP probe named PROBE1 and access its mode, enter:

```
host1/Admin(config)# probe tcp PROBE1
host1/Admin(config-probe-tcp)#
```

To delete a TCP probe named PROBE1, enter:

```
host1/Admin(config)# no probe tcp PROBE1
```

Related Commands

clear probe
show probe

(config) radius-server attribute nas-ipaddr

To specify a RADIUS NAS-IP-Address attribute, use the **radius-server attribute nas-ipaddr** command. Use the **no** form of this command to delete the RADIUS NAS-IP-Address and return to the default configuration.

radius-server attribute nas-ipaddr *nas_ip_address*

no radius-server attribute nas-ipaddr *nas_ip_address*

Syntax Description

nas_ip_address	IP address that is used as the RADIUS NAS-IP-Address, attribute 4. Enter the address in dotted-decimal IP notation (for example, 192.168.11.1).

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

By default, the NAS-IP-Address is not configured. The ACE performs a route lookup on the Remote Authentication Dial-In User Service (RADIUS) server IP address and uses the result.

The RADIUS NAS-IP-Address attribute allows you to configure an arbitrary IP address to be used as RADIUS attribute 4, NAS-IP-Address for each context.

The **radius-server attribute nas-ipaddr** command allows the ACE to behave as a single RADIUS client from the perspective of the RADIUS server. The configured NAS-IP-Address will be encapsulated in all outgoing RADIUS authentication request and accounting packets.

Examples

To specify a RADIUS NAS-IP-Address, enter:

```
host1/Admin(config)# radius-server attribute nas-ipaddr 192.168.1.1
```

To delete the RADIUS NAS-IP-Address and return to the default configuration, enter:

```
host1/Admin(config)# no radius-server attribute nas-ipaddr 192.168.1.1
```

Related Commands

show aaa
(config) aaa group server
(config) radius-server host

(config) radius-server deadtime

To globally set the time interval in which the ACE verifies whether a nonresponsive server is operational, use the **radius-server deadtime** command. Use the **no** form of this command to reset the Remote Authentication Dial-In User Service (RADIUS) server dead-time request to the default of 0.

radius-server deadtime *minutes*

no radius-server deadtime *minutes*

Syntax Description

minutes	Length of time that the ACE skips a nonresponsive RADIUS server for transaction requests. Enter an integer from 0 to 1440 (24 hours). The default is 0.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Use of this command causes the ACE to mark as "dead" any RADIUS servers that fail to respond to authentication requests. This action avoids the wait for the request to time out before trying the next configured server. The ACE skips a RADIUS server that is marked as dead by sending additional requests for the duration of minutes.

The dead-time interval starts when the server does not respond to the number of authentication request transmissions configured through the **radius-server retransmit** command. When the server responds to a probe access-request packet, the ACE transmits the authentication request to the server.

Examples

To globally configure a 15-minute dead-time for RADIUS servers that fail to respond to authentication requests, enter:

```
host1/Admin(config)# radius-server deadtime 15
```

To set the RADIUS server dead-time request to 0, enter:

```
host1/Admin(config)# no radius-server deadtime 15
```

Related Commands

show aaa
(config) aaa group server
(config) radius-server host

(config) radius-server host

To designate and configure a host for RADIUS server functions, use the **radius-server host** command. You can define multiple **radius-server host** commands to configure multiple Remote Authentication Dial-In User Service (RADIUS) servers. Use the **no** form of this command to remove the RADIUS server from the configuration.

radius-server host *ip_address* [**key** *shared_secret* [**0** *shared_secret* | **7** *shared_secret*]] [**auth-port** *port_number*] [**acct-port** *port_number*] [**authentication**] [**accounting**] [**timeout** *seconds*] [**retransmit** *count*]

no radius-server host *ip_address* [**key** *shared_secret* [**0** *shared_secret* | **7** *shared_secret*]] [**auth-port** *port_number*] [**acct-port** *port_number*] [**authentication**] [**accounting**] [**timeout** *seconds*] [**retransmit** *count*]

Syntax Description

ip_address	IP address for the RADIUS server. Enter the address in dotted-decimal IP notation (for example, 192.168.11.1).
key	(Optional) Enables an authentication key for communication between the ACE and the RADIUS daemon running on the RADIUS server. The key is a text string that must match the encryption key used on the RADIUS server.
shared_secret	Key that is used to authenticate communication between the RADIUS client and server. The shared secret must match the one configured on the RADIUS server. Enter the shared secret as a case-sensitive string with no spaces with a maximum of 63 alphanumeric characters.
0	(Optional) Configures a key specified in clear text (indicated by 0) to authenticate communication between the RADIUS client and server.
7	(Optional) Configures a key specified in encrypted text (indicated by 7) to authenticate communication between the RADIUS client and server.
auth-port *port_number*	(Optional) Specifies the UDP destination port for communicating authentication requests to the RADIUS server. By default, the RADIUS authentication port is 1812 (as defined in RFC 2138 and RFC 2139). The *port_number* argument specifies the RADIUS port number. Valid values are from 1 to 65535.
acct-port *port_number*	(Optional) Specifies the UDP destination port for communicating accounting requests to the RADIUS server. By default, the RADIUS accounting port is 1813 (as defined in RFC 2138 and RFC 2139). The *port_number* argument specifies the RADIUS port number. Valid values are from 1 to 65535.
authentication	(Optional) Specifies that the RADIUS server is used only for authentication purposes. If neither the authentication nor the accounting options are specified, the RADIUS server is used for both accounting and authentication purposes.
accounting	(Optional) Specifies that the RADIUS server is used only for accounting purposes. If neither the authentication nor the accounting options are specified, the RADIUS server is used for both accounting and authentication purposes.
timeout *seconds*	(Optional) Specifies the time interval that the ACE waits for the RADIUS server to reply to an authentication request before retransmitting a request. Valid entries are from 1 to 60 seconds. The default is 1 second.
retransmit *count*	(Optional) Specifies the number of times that the ACE retransmits an authentication request to a timed-out RADIUS server before declaring the server to be unresponsive and contacting the next server in the group. Valid entries are from 1 to 5 attempts. The default is one attempt.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The **key** option overrides the global setting of the **radius-server key** command. If you do not specify a key, the global value is used. RADIUS keys are always stored in encrypted form in persistent storage. The running configuration also displays keys in encrypted form.

If neither the **authentication** nor the **accounting** options are specified, the RADIUS server is used for both accounting and authentication.

If your RADIUS server uses a port other than 1813, use the **acct-port** keyword to configure the ACE for the appropriate port before starting the RADIUS service.

If your RADIUS server uses a port other than 1812, use the **auth-port** keyword to configure the ACE for the appropriate port before starting the RADIUS service.

The **retransmit** and **timeout** options override the global settings assigned for the specified server when you enter the **radius-server retransmit** and **radius-server timeout** commands.

Examples

To configure RADIUS server authentication parameters, enter:

```
host1/Admin(config)# radius-server host 192.168.2.3 key HostKey
host1/Admin(config)# radius-server host 192.168.2.3 key 7 secret_1256
host1/Admin(config)# radius-server host 192.168.2.3 auth-port 1645
host1/Admin(config)# radius-server host 192.168.2.3 acct-port 1646
host1/Admin(config)# radius-server host 192.168.2.3 authentication
host1/Admin(config)# radius-server host 192.168.2.3 accounting
host1/Admin(config)# radius-server host 192.168.2.3 timeout 25
host1/Admin(config)# radius-server host 192.168.2.3 retransmit 3
```

To revert to a default RADIUS server authentication setting, enter:

```
host1/Admin(config)# no radius-server host 192.168.2.3 acct-port 1646
```

Related Commands

show aaa
(config) aaa group server
(config) radius-server attribute nas-ipaddr

(config) radius-server key

To globally configure an authentication key for communication between the ACE and the Remote Authentication Dial-In User Service (RADIUS) daemon running on each RADIUS server, use the **radius-server key** command. Use the **no** form of this command to remove the global RADIUS server key setting from the configuration.

radius-server key {*shared_secret* | **0** *shared_secret* | **7** *shared_secret*}

no radius-server key {*shared_secret* | **0** *shared_secret* | **7** *shared_secret*}

Syntax Description

shared_secret	Key used to authenticate communication between the RADIUS client and the server. The shared secret must match the one configured on the RADIUS server. Enter the shared secret as a case-sensitive string with no spaces and a maximum of 63 alphanumeric characters.
0	Configures a key specified in clear text (indicated by 0) to authenticate communication between the RADIUS client and server.
7	Configures a key specified in encrypted text (indicated by 7) to authenticate communication between the RADIUS client and server.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The key is a text string that must match the encryption key used on the RADIUS server. RADIUS keys are always stored in encrypted form in persistent storage on the ACE. This global key will be applied to those RADIUS servers in a named server group for which a shared secret is not individually configured by the **(config) radius-server host** command.

Examples

To globally configure an authentication key to be sent in encrypted text (indicated by 7) to the RADIUS server, enter:

```
host1/Admin(config)# radius-server key 7 abe4DFeeweo00o
```

To delete the key, enter:

```
host1/Admin(config)# no radius-server key 7 abe4DFeeweo00o
```

Related Commands

show aaa
(config) aaa group server
(config) radius-server host

(config) radius-server retransmit

To globally change the number of times that the ACE sends an authentication request to a Remote Authentication Dial-In User Service (RADIUS) server, use the **radius-server retransmit** command. Use the **no** form of this command to revert to the default of one transmission attempt.

radius-server retransmit *count*

no radius-server retransmit *count*

Syntax Description

count	Number of times that the ACE attempts to connect to a RADIUS server(s) before trying to contact the next available server. Enter an integer from 1 to 5. The default is 1.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The ACE applies this global retransmission value to those RADIUS servers for which a value is not individually configured by the **(config) radius-server host** command.

If all servers in the group are unavailable for authentication and accounting, the ACE tries the local database if you configure a local fallback method by entering the **aaa authentication login** or the **aaa accounting default** commands. If you do not have a fallback method, the ACE continues to contact one of the AAA servers listed in the server group.

Examples

To globally configure the number of retransmissions to 3, enter:

```
host1/Admin(config)# radius-server retransmit 3
```

To revert to the default of one transmission attempt, enter:

```
host1/Admin(config)# no radius-server retransmit 3
```

Related Commands

show aaa
(config) aaa group server
(config) radius-server host

(config) radius-server timeout

To globally change the time interval that the ACE waits for the Remote Authentication Dial-In User Service (RADIUS) server to reply before retransmitting an authentication request to the RADIUS server, use the **radius-server timeout** command. Use the **no** form of this command to revert to the default of one second between transmission attempts.

radius-server timeout *seconds*

no radius-server timeout *seconds*

Syntax Description

seconds	Time in seconds between retransmissions to the RADIUS server. Enter an integer from 1 to 60 seconds. The default is 1 second.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The ACE applies this global timeout value to those RADIUS servers for which a timeout value is not individually configured by the **(config) radius-server host** command.

Examples

To globally configure the timeout value to 30 seconds, enter:

```
host1/Admin(config)# radius-server timeout 30
```

To revert to the default of one second between transmission attempts, enter:

```
host1/Admin(config)# no radius-server timeout 30
```

Related Commands

show aaa
(config) aaa group server
(config) radius-server host

(config) resource-class

To create a resource class and enter resource configuration mode, use the **resource-class** command. The CLI prompt changes to (config-resource). Configure a resource class to limit the use of system resources by one or more contexts. Use the **no** form of this command to remove the resource-class setting.

resource-class *name*

no resource-class *name*

Syntax Description

name	Name assigned to the resource class. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. You can also use the resource class called **default**.

Command Modes

Configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Use a resource class to allocate and limit system resources among contexts in your ACE. The default resource class allocates 100 percent of all configurable system resources to each context. By creating a resource class, you can prevent oversubscription by limiting the percentage of resources available to each context. After you create and configure a resource class, use the **(config-context) member** command in context configuration mode to assign a context to the class.

To use the stickiness feature, you must allocate a minimum percentage of resources to the feature. Otherwise, stickiness will not work. For more details, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the commands in the resource configuration mode, see the "Resource Configuration Mode Commands" section.

Examples

To create a resource class called RC1, enter:

```
host1/C1(config)# resource-class RC1
host1/C1(config-resource)
```

To remove the resource class from the configuration, enter:

```
host1/C1(config)# no resource-class RC1
```

Related Commands

show resource allocation
show resource usage
show user-account
show users
(config-context) member

(config) role

To assign a user role to a user and enter role configuration mode, use the **role** command. The CLI prompt changes to (config-role). User roles determine the privileges that a user has, the commands that a user can enter, and the actions that a user can perform in a particular context. You can apply the roles that you create only in the context in which you create them. See the "Role Configuration Mode Commands" section for details. Use the **no** form of this command to remove the user role assignment.

role *name*

no role *name*

Syntax Description

name	Identifier associated with a user role. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

If you do not assign a user role to a new user, the default user role is Network-Monitor. For users that you create in the Admin context, the default scope of access is the entire device. For users that you create in other contexts, the default scope of access is the entire context. If you need to restrict a user's access, you must assign a role-domain pair using the **(config) username** command.

For information about the commands in the role configuration mode, see the "Role Configuration Mode Commands" section.

For information about configuring roles and assigning them to users, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*

Examples

To assign a role, enter:

```
host1/C1(config)# role TECHNICIAN
host1/C1(config-role)#
```

To remove the role from the configuration, enter:

```
host1/C1(config)# no role TECHNICIAN
```

Related Commands

show role
show user-account
show users
(config) username

(config) rserver

To create a real server for server load balancing (SLB) and enter real server configuration mode, use the **rserver** command. The CLI prompt changes to (config-host-rserver) or (config-redirect-rserver), depending on the type of real server that you create. You can create a maximum of 16,384 real servers. Use the **no** form of this command to remove the real server from the configuration.

rserver [**host** | **redirect**] *name*

no rserver [**host** | **redirect**] *name*

Syntax Description

host	(Optional) Specifies a typical real server that provides content and services to clients. This is the default setting. For details on the commands in real server host configuration mode, see the "Real Server Host Configuration Mode Commands" section.
redirect	(Optional) Specifies a real server used to redirect traffic to a new location as specified in the *relocn-string* argument of the **webhost-redirection** command. For details on the commands in real server redirect configuration mode, see the "Real Server Redirect Configuration Mode Commands" section.
name	Identifier for the real server. Enter an unquoted text string with no spaces and maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the rserver feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

All servers in a server farm must be of the same type: **host** or **redirect**. You can create a maximum of 4096 real servers in each ACE.

Examples

To create a real server of type host, enter:

```
host1/Admin(config)# rserver server1
```

To remove the real server of type host from the configuration, enter:

```
host1/Admin(config)# no rserver server1
```

Related Commands

(config-rserver-redir) webhost-redirection
clear rserver
show rserver

(config) script file name

To load a script into memory on the ACE and enable it for use, use the **script file name** command. Use the **no** form of this command to remove a script from memory and the running configuration.

script file name*script_name*

no script file name *script_name*

Syntax Description

script_name	Name of the script on the disk0: filesystem. The script name must be unique across the context. You will use the filename when you configure the probe.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the probe feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To run a script or create a health probe using a script, you must see the script name, not the script file from which the script was loaded.

Examples

To load a script into memory, enter:

```
host1/Admin(config)# script file name ftp1.tcl
```

To remove the script, enter:

```
host1/Admin(config)# no script file name  ftp1.tcl
```

Related Commands show script

(config) serverfarm

To create a new server farm or modify an existing server farm and enter the serverfarm configuration mode, use the **serverfarm** command. You can configure a maximum of 4096 server farms on each ACE. Use the **no** form of this command to remove the server farm from the configuration.

serverfarm [**host** | **redirect**] *name*

no serverfarm [**host** | **redirect**] *name*

Syntax Description

host	(Optional) Specifies a typical server farm that consists of real servers that provide content and services to clients. This is the default. For details on the commands in the serverfarm host configuration mode, see the "Server Farm Host Configuration Mode Commands" section.
redirect	(Optional) Specifies that the server farm consist only of real servers that redirect client requests to alternate locations specified by the relocation string or port number in the real server configuration. For details on the commands in the serverfarm redirect host configuration mode, see the "Server Farm Redirect Configuration Mode Commands" section.
name	Unique identifier of the server farm. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the server-farm feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

After you create a server farm, you configure the other server farm attributes and add real servers to the farm. You can configure a maximum of 4096 server farms in each ACE.

Examples

To create a server farm of type **host** called SFARM1, enter:

```
host1/Admin(config)# serverfarm SFARM1
host1/Admin(config-sfarm-host)#
```

To remove a server farm called SFARM1, enter:

```
host1/Admin(config)# no serverfarm SFARM1
host1/Admin(config-sfarm-host)#
```

Related Commands

(config-rserver-redir) webhost-redirection
clear serverfarm
show serverfarm

(config) service-policy

To apply a previously created policy map and attach the traffic policy to a specific VLAN interface or globally to all VLAN interfaces in the same context, use the **service-policy** command. Use the **no** form of this command to remove a service policy.

service-policy input *policy_name*

no service-policy input *policy_name*

Syntax Description

input	Specifies that the traffic policy is to be attached to the input direction of an interface. The traffic policy evaluates all traffic received by that interface.
policy_name	Name of a previously defined policy map, configured with a previously created **policy-map** command. The name can be a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the interface feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Note the following when creating a service policy:

- Policy maps, applied globally in a context, are internally applied on all interfaces existing in the context.
- You can apply the policy in an input direction only.
- A policy activated on an interface overwrites any specified global policies for overlapping classification and actions.
- The ACE allows only one policy of a specific feature type to be activated on a given interface.

Examples

To specify an interface VLAN and apply the Layer 3 and Layer 4 SLB policy map to the VLAN, enter:

```
host1/C1(config)# interface vlan50
host1/C1(config-if)# mtu 1500
host1/C1(config-if)# ip address 172.20.1.100 255.255.0.0
host1/C1(config-if)# service-policy input L4SLBPOLICY
```

To globally apply the Layer 3 and Layer 4 SLB policy map to the entire context:

```
host1/C1(config)# service-policy input L4SLBPOLICY
```

To globally detach a traffic policy from a context, enter:

```
host1/C1(config)# no service-policy input L4SLBPOLICY
```

Related Commands

clear service-policy
show service-policy
(config-if) service-policy input

(config) shared-vlan-hostid

To configure a specific bank of MAC addresses for an ACE, use the **shared-vlan-hostid** command. Use the **no** form of this command to remove a configured bank of MAC addresses.

shared-vlan-hostid *number*

no shared-vlan-hostid

Syntax Description

number	Bank of MAC addresses that the ACE uses. Enter a number from 1 to 16. Be sure to configure different bank numbers for multiple ACEs.

Command Modes

Configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the interface feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

When contexts share a VLAN, the ACE assigns a different MAC address to the VLAN on each context. The MAC addresses reserved for shared VLANs are 0x001243dc6b00 to 0x001243dcaaff, inclusive. All ACE appliances derive these addresses from a global pool of 16k MAC addresses. This pool is divided into 16 banks, each containing 1,024 addresses. An ACE supports only 1,024 shared VLANs, and would use only one bank of MAC addresses out of the pool.

By default, the bank of MAC addresses that the ACE uses is randomly selected at boot time. However, if you configure two ACE appliances in the same Layer 2 network and they are using shared VLANs, the ACEs may select the same address bank and use the same MAC addresses. To avoid this conflict, you need to configure the bank that the ACEs will use.

Examples

To configure bank 2 of MAC addresses, enter:

```
host1/Admin(config)# shared-vlan-hostid 2
```

To remove the configured bank of MAC addresses, enter:

```
host1/Admin(config)# no shared-vlan-hostid
```

Related Commands

(config) arp

(config) peer shared-vlan-hostid

(config) snmp-server community

To create or modify Simple Network Management Protocol (SNMP) community names and access privileges, use the **snmp-server community** command. Each SNMP device or member is part of a community. An SNMP community determines the access rights for each SNMP device. SNMP uses communities to establish trust between managers and agents. Use the **no** form of this command to remove an SNMP community.

snmp-server community *community_name* [**group** *group_name* | **ro**]

no snmp-server community *community_name* [**group** *group_name* | **ro**]

Syntax Description

community_name	SNMP community name for this system. Enter an unquoted text string with no space and a maximum of 32 alphanumeric characters.

group *group_name*	(Optional) Identifies the role group to which the user belongs. Enter an unquoted text string with no space and a maximum of 32 alphanumeric characters. **Note** Only network monitoring operations are supported through the ACE implementation of SNMP. In this case, all SNMP users are automatically assigned the system-defined default group of Network-Monitor. For details on creating users, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.
ro	(Optional) Allows read-only access for this community.

Command Modes

Configuration mode

Admin and user contexts

Caution If you change the SNMP engine ID for an Admin or user context, all configured SNMP users become invalid. You must recreate all SNMP users by using the **snmp-server community** command in configuration mode.

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

After you create or modify a community, all SNMP devices assigned to that community as members have the same access rights (as described in RFC 2576). The ACE supports read-only access to the MIB tree for devices included in this community. The read-only community string allows a user to read data values but prevents that user from modifying the data.

SNMP communities are applicable only for SNMPv1 and SNMPv2c. SNMPv3 requires user configuration information such as specifying the role group that the user belongs to, authentication parameters for the user, authentication password, and message encryption parameters.

Examples

To specify an SNMP community called SNMP_Community1, which is a member of the user group, with read-only access privileges for the community, enter:

```
host1/Admin(config)# snmp-server community SNMP_Community1 group Network-Monitor
```

To remove an SNMP community, enter:

```
host1/Admin(config)# no snmp-server community SNMP_Community1 group Network-Monitor
```

Related Commands

(config) snmp-server host

(config) snmp-server contact

To specify the contact information for the Simple Network Management Protocol (SNMP) system, use the **snmp-server contact** command. You can specify information for only one contact name. Use the **no** form of this command to remove an SNMP contact.

snmp-server contact *contact_information*

no snmp-server contact

Syntax Description

contact_information	SNMP contact information for this system. Enter a text string with a maximum of 240 alphanumeric characters, including spaces. If the string contains more than one word, enclose the string in quotation marks (“ ”). You can include information on how to contact the person; for example, you can include a phone number or an e-mail address.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can specify only one contact name per SNMP system.

Examples

To specify SNMP system contact information, enter:

```
host1/Admin(config)# snmp-server contact “User1 user1@cisco.com”
```

To remove the specified SNMP contact information, enter:

```
host1/Admin(config)# no snmp-server contact
```

Related Commands

(config) snmp-server host

(config) snmp-server enable traps

To enable the ACE to send Simple Network Management Protocol (SNMP) traps and informs to the network management system (NMS), use the **snmp-server enable traps** command. This command enables both traps and inform requests for the specified notification types. Use the **no** form of this command to disable the sending of SNMP traps and inform requests.

snmp-server enable traps [*notification_type*] [*notification_option*]

no snmp-server enable traps [*notification_type*] [*notification_option*]

Syntax Description

notification_type	(Optional) Type of notification to enable. If no type is specified, the ACE sends all notifications. Specify one of the following keywords: • **license**—Sends SNMP license manager notifications. This keyword appears only in the Admin context. • **serverfarm** —Sends a trap when all servers are down in the server farm or the server farm has changed state. • **slb**—Sends server load-balancing notifications. When you specify the **slb** keyword, you can specify a *notification_option* value. • **snmp**—Sends SNMP notifications. When you specify the **snmp** keyword, you can specify a *notification_option* value. • **syslog**—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the **logging history** command. • **virtual-context**—Sends virtual context change notifications. This keyword appears only in the Admin context.
notification_option	(Optional) One of the following SNMP notifications to enable: • When you specify the **snmp** keyword, specify the **authentication**, **coldstart**, **linkdown**, or **linkup** keyword to enable SNMP notifications. This selection generates a notification if the community string provided in SNMP request is incorrect, or when a VLAN interface is either up or down. The **coldstart** keyword appears only in the Admin context. • When you specify the **slb** keyword, specify the **real** or **vserver** keyword to enable server load-balancing notifications. This selection generates a notification if one of the following occurs: – The real server changes state (up or down) due to such occurrences as user intervention, ARP failures, and probe failures. – The virtual server changes state (up or down). The virtual server represents the servers behind the content switch in the ACE to the outside world and consists of the following attributes: destination address (can be a range of IP addresses), protocol, destination port, incoming VLAN.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(2.4)	The **serverfarm** option was added to this command.

Usage Guidelines

This command has no user role restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The notification types used in the **snmp-server enable traps** command all have an associated MIB object that globally enables or disables them. However, not all of the notification types available in the **snmp-server host** command have notificationEnable MIB objects, so some of the notification types cannot be controlled using the **snmp-server enable traps** command.

The supported SNMP notifications (traps) in the CISCO-ENHANCED-SLB-MIB for the **serverfarm** option are as follows:

- esRealServerStateUpRev1 State of a real server configured in a server farm is up due to user intervention.The notification is sent with the following varbinds:
  - cesRealServerName
  - cesServerFarmRserverBackupPort
  - cesServerFarmName
  - cesServerFarmRserverAdminStatus
  - cesServerFarmRserverOperStatus
  - cesRserverIpAddressType
  - cesRserverIpAddress
  - cesServerFarmRserverDescr
- cesRealServerStateDownRev1 State of a real server configured in a server farm is down due to user intervention. The notification is sent with the following varbinds:
  - cesRealServerName
  - cesServerFarmRserverBackupPort
  - cesServerFarmName
  - cesServerFarmRserverAdminStatus
  - cesServerFarmRserverOperStatus
  - cesServerFarmRserverStateDescr
  - cesRserverIpAddressType
  - cesRserverIpAddress
  - cesServerFarmRserverDescr
- cesRealServerStateChangeRev1 State of a real server configured in a server farm changed to a new state as a result of something other than a user intervention. This notification is sent for situations such as ARP failures, probe failures, and so on. The notification is sent with the following varbinds:

- cesRealServerName
- cesServerFarmRserverBackupPort
- cesServerFarmName
- cesServerFarmRserverAdminStatus
- cesServerFarmRserverOperStatus
- cesServerFarmRserverStateDescr
- cesRserverIpAddressType
- cesRserverIpAddress
- cesProbeName
- cesServerFarmRserverDescr

To configure the ACE to send the SNMP notifications, specify at least one **snmp-server enable traps** command. To enable multiple types of notifications, you must enter a separate **snmp-server enable traps** command for each notification type and notification option. If you enter the command without any keywords, the ACE enables all notification types and traps.

The **snmp-server enable traps** command is used with the **snmp-server host** command. The **snmp-server host** command specifies which host receives the SNMP notifications. To send notifications, you must configure at least one SNMP server host.

Examples

To enable the ACE to send server load-balancing traps to the host myhost.cisco.com using the community string public, enter:

```
host1/Admin(config)# snmp-server host myhost.cisco.com
host1/Admin(config)# snmp-server community SNMP_Community1 group Network-Monitor
host1/Admin(config)# snmp-server enable traps slb real
```

To disable SNMP server notifications, enter:

```
host1/Admin(config)# no snmp-server enable traps slb real
```

Related Commands

(config) snmp-server host

(config) snmp-server engineid

To configure the SNMP engine ID for an ACE context, use the **snmp-server engineid** command. Use the **no** form of this command to reset the default engine ID for the context.

snmp-server engineid *number*

no snmp-server engineid *number*

Syntax Description

contact_information	SNMPv3 engine ID that you want to configure. Enter a range of 10 to 64 hexadecimal digits.

Command Modes

Configuration mode

Admin and user contexts

Caution If you change the SNMP engine ID for an Admin or user context, all configured SNMP users become invalid and all SNMP communities are deleted. You must recreate all SNMP users by using the **snmp-server user** command in configuration mode. You must recreate all SNMP communities by using the **snmp-server community** command in configuration mode.

Command History

Release	Modification
A3(2.3)	This command was introduced.

Usage Guidelines

The ACE allows you to configure an SNMP engine ID for the Admin or user context. By default, the ACE automatically creates an SNMP engine ID for the Admin context and each user context. The SNMP engine represents a logically separate SNMP agent. The IP address for an ACE context provides access to only one SNMP engine ID.

For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To configure an engine ID 884395734985738888439573498573888 for the Admin context, enter:

```
host1/Admin(config)# snmp-server engineID 884395734985738888439573498573888
```

To reset the default engine ID for the Admin context, enter:

```
host1/Admin(config)# no snmp-server engineID
```

To display the engine ID for a context, use the **show snmp engineID** command in Exec mode for the context. For example, to display the engine ID for the Admin context, enter:

```
host1/Admin# show snmp engineID
```

Related Commands

(config) snmp-server host
(config) snmp-server community
(config) snmp-server user

(config) snmp-server host

To specify which host receives Simple Network Management Protocol (SNMP) notifications, use the **snmp-server host** command. To send notifications, you must configure at least one SNMP host using the **snmp-server host** command. Use the **no** form of this command to remove the specified host.

snmp-server host *host_address* {*community-string_username* | **informs** | **traps** | **version** {**1** {**udp-port**} | **2c** {**udp-port**} | **3** [**auth** | **noauth** | **priv**]}}

no snmp-server host *host_address* {*community-string_username* | **informs** | **traps** | **version** {**1** {**udp-port**} | **2c** {**udp-port**} | **3** [**auth** | **noauth** | **priv**]}}

Syntax Description

host_address	IP address of the host (the targeted recipient). Enter the address in dotted-decimal IP notation (for example, 192.168.11.1).
community-string_username	SNMP community string or username with the notification operation to send. Enter an unquoted text string with no space and a maximum of 32 alphanumeric characters.
informs	Sends SNMP inform requests to the identified host, which allows for manager-to-manager communication. Inform requests can be useful when you need more than one NMS in the network.
traps	Sends SNMP traps to the identified host. An agent uses a trap to tell the NMS that a problem has occurred. The trap originates from the agent and is sent to the trap destination, as configured within the agent itself. The trap destination is typically the IP address of the NMS.
version	Specifies the version of SNMP used to send the traps. SNMPv3 is the most secure model because it allows packet encryption with the **priv** keyword.
1	Specifies SNMPv1. This option is not available for use with SNMP inform requests. SNMPv1 has one optional keyword (**udp-port**) that specifies the port UDP port of the host to use. The default is 162.
2c	Specifies SNMPv2C. SNMPv2C has one optional keyword (**udp-port**) that specifies the port UDP port of the host to use. The default is 162.
3	Specifies SNMPv3. SNMPv3 has three optional keywords (**auth**, **no auth**, or **priv**).
auth	(Optional) Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication.
noauth	(Optional) Specifies the noAuthNoPriv security level.
priv	Enables Data Encryption Standard (DES) packet encryption (privacy).

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The ACE supports a maximum of 10 SNMP hosts per context.

Examples

To specify the recipient of an SNMP notification, enter:

```
host1/Admin(config)# snmp-server host 192.168.1.1 traps version 2c abcddsfsf udp-port 500
```

To remove the specified host, enter:

```
host1/Admin(config)# no snmp-server host 192.168.1.1 traps version 2c abcddsfsf udp-port
500
```

Related Commands

(config) snmp-server enable traps

(config) snmp-server location

To specify the Simple Network Management Protocol (SNMP) system location, use the **snmp-server location** command. You can specify only one location. Use the **no** form of this command to remove the SNMP system location.

snmp-server location *location*

no snmp-server location

Syntax Description

location	Physical location of the system. Enter a text string with a maximum of 240 alphanumeric characters, including spaces. If the string contains more than one word, enclose the string in quotation marks (“ ”).

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can specify only one location per SNMP system.

Examples

To specify SNMP system location information, enter:

```
host1/Admin(config)# snmp-server location "Boxborough MA"
```

To remove the specified SNMP system location information, enter:

```
host1/Admin(config)# no snmp-server location
```

Related Commands

(config) snmp-server community

(config) snmp-server trap link ietf

To instruct the ACE to send the linkUp and linkDown traps with the IETF standard IF-MIB (RFC 2863) variable bindings that consist of ifIndex, ifAdminStatus, and ifOperStatus, use the **snmp-server trap link ietf** command. Use the **no** form of this command to revert to the Cisco implementation of linkUp and linkDown traps.

snmp-server trap link ietf

no snmp-server trap link ietf

Syntax Description

This command has no keywords or arguments.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

By default, the ACE sends the Cisco implementation of linkUp and linkDown traps to the NMS. The ACE sends the Cisco Systems IF-MIB variable bindings that consist of ifIndex, ifAdminStatus, ifOperStatus, ifName, ifType, clogOriginID, and clogOriginIDType. You can configure the ACE to send the IETF standards-based implementation for linkUp and linkDown traps (as outlined in RFC 2863).

The Cisco var-binds are sent by default. To receive RFC 2863-compliant traps, you must specify the **snmp-server trap link ietf** command.

Examples To configure the linkUp and linkDown traps to be compliant with RFC 2863, enter:

```
host1/Admin(config)# snmp-server trap link ietf
```

To revert to the Cisco implementation of linkUp and linkDown traps, enter:

```
host1/Admin(config)# no snmp-server trap link ietf
```

Related Commands **(config) snmp-server enable traps**

(config) snmp-server trap-source vlan

To specify the use of the IP address configured on a VLAN as the trap-source address in the SNMPv1 trap PDU, use the **snmp-server trap-source vlan** command. If the VLAN interface does not contain a valid IP address, the sending of notifications fails for SNMPv1 traps. Use the **no** form of this command to remove the specified VLAN as the source address in the SNMPv1 trap PDU and reset the default behavior.

snmp-server trap-source vlan *number*

no snmp-server trap-source vlan *number*

Syntax Description

number	VLAN number of the configured interface. Enter a value from 2 to 4094 for an existing VLAN.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(2.1)	You can no longer select the VLAN number of the FT VLAN interface that has been specified between redundant ACE appliances as the trap source address contained in the SNMP v1 trap PDU.

Usage Guidelines

By default, the ACE uses the trap source IP address from the internal routing table, depending on the destination host address, where the ACE will send the notification.

The ACE restricts you from selecting the VLAN number of the FT VLAN interface that has been specified between redundant ACE appliances as the trap source address contained in the SNMP v1 trap PDU.

For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples To specify VLAN 50 in the VLAN interface as the source address in the SNMPv1 trap PDUs, enter:

```
host1/Admin(config)# snmp-server trap-source vlan 50
```

To remove the specified VLAN as the source address in the SNMPv1 trap PDU and reset the default behavior, enter:

```
host1/Admin(config)# no snmp-server trap-source
```

Related Commands (config) snmp-server enable traps

(config) snmp-server unmask-community

To unmask the snmpCommunityName and snmpCommunitySecurityName OIDs of the SNMP-COMMUNITY-MIB, use the **snmp-server unmask-community** command. By default, these OIDs are masked. Use the **no** form of this command to mask these OIDs.

snmp-server unmask-community

no snmp-server unmask-community

Syntax Description This command has no keywords or arguments.

Command Modes Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(2.3)	This command was introduced.

Usage Guidelines This command has no user role restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To assign multiple roles to a user, enter multiple **snmp-server user** commands.

You can create a maximum of 28 SNMP users for each context.

User configuration through the **snmp-server user** command is applicable only for SNMPv3; SNMPv1 and SNMPv2c use a community string match for user authentication.

The ACE synchronizes the interactions between a user created with the **username** command and the same user specified using the **snmp-server user** command; updates made to a user configuration in the ACE CLI are automatically reflected in the SNMP server. For example, when you delete a user, the user is automatically deleted from both the SNMP server and the CLI. In addition, user-role mapping changes are synchronized in SNMP and CLI.

Only network monitoring operations are supported through the ACE implementation of SNMP where all SNMP users are automatically assigned to the system-defined default group of Network-Monitor.

Examples

To set the user information, enter:

```
host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
host1/Admin(config)# snmp-server user joe Network-Monitor auth sha abcd1234
host1/Admin(config)# snmp-server user sam Network-Monitor auth md5 abcdefgh
host1/Admin(config)# snmp-server user Bill Network-Monitor auth sha abcd1234 priv abcdefgh
```

To disable the SNMP user configuration or to remove an SNMP user, enter:

```
host1/Admin(config)# no snmp-server user Bill Network-Monitor auth sha abcd1234 priv
abcdefgh
```

Related Commands

This command has no related commands.

(config) snmp-server user

To configure Simple Network Management Protocol (SNMP) user information, use the **snmp-server user** command. Use the **no** form of this command to disable the SNMP user configuration or to remove an SNMP user.

snmp-server user *user_name* [*group_name*] [**auth** {**md5** | **sha**} *password1* [**localizedkey** | **priv** {*password2* | **aes-128** *password2*}]]

no snmp-server user *user_name* [*group_name*] [**auth** {**md5** | **sha**} *password1* [**localizedkey** | **priv** {*password2* | **aes-128** *password2*}]]

Syntax Description

user_name	Username. Enter an unquoted text string with no spaces and a maximum of 24 alphanumeric characters.
group_name	(Optional) User role group to which the user belongs. Enter an unquoted text string with no space sand a maximum of 32 characters. SNMP access rights are organized by groups. Each group in SNMP is similar to a role through the CLI. The *group_name* is defined by the **role** configuration mode command.
auth	(Optional) Sets authentication parameters for the user. Authentication determines that the message is from a valid source.
md5	Specifies the HMAC Message Digest 5 (MD5) encryption algorithm for user authentication.
sha	Specifies the HMAC Secure Hash Algorithm (SHA) encryption algorithm for user authentication.
password1	User authentication password. Enter an unquoted text string with no space and a maximum of 130 alphanumeric characters. The ACE automatically synchronizes the SNMP authentication password as the password for the CLI user. The ACE supports the following special characters in a password: , . / = + - ^ @ ! % ~ # $ * ( ) Note that the ACE encrypts clear text passwords in the running-config.

localizedkey	(Optional) Specifies that the password is in a localized key format for security encryption.
priv	(Optional) Specifies encryption parameters for the user. The **priv** option and the **aes-128** option indicate that this privacy password is for generating a 128-bit AES key.
aes-128	(Optional) Specifies the 128-byte Advanced Encryption Standard (AES) algorithm for privacy. AES is a symmetric cipher algorithm and is one of the privacy protocols for SNMP message encryption. It conforms with RFC 3826.
password2	Encryption password for the user. The AES priv password can have a minimum of eight alphanumeric characters. If the passphrases are specified in clear text, you can specify a maximum of 64 alphanumeric characters. If you use the localized key, you can specify a maximum of 130 alphanumeric characters. Spaces are not allowed. The ACE supports the following special characters in a password: , . / = + - ^ @ ! % ~ # $ * ( ) Note that the ACE encrypts clear text passwords in the running-config.

Command Modes

Configuration mode

Admin and user contexts

Note If you change the SNMP engine ID for an Admin or user context, all configured SNMP users become invalid. You must recreate all SNMP users by using the **snmp-server user** command in configuration mode.

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To assign multiple roles to a user, enter multiple **snmp-server user** commands.

You can create a maximum of 28 SNMP users for each context.

User configuration through the **snmp-server user** command is applicable only for SNMPv3; SNMPv1 and SNMPv2c use a community string match for user authentication.

The ACE synchronizes the interactions between a user created with the **username** command and the same user specified using the **snmp-server user** command; updates made to a user configuration in the ACE CLI are automatically reflected in the SNMP server. For example, when you delete a user, the user is automatically deleted from both the SNMP server and the CLI. In addition, user-role mapping changes are synchronized in SNMP and CLI.

Only network monitoring operations are supported through the ACE implementation of SNMP where all SNMP users are automatically assigned to the system-defined default group of Network-Monitor.

Examples

To set the user information, enter:

```
host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
host1/Admin(config)# snmp-server user joe Network-Monitor auth sha abcd1234
host1/Admin(config)# snmp-server user sam Network-Monitor auth md5 abcdefgh
host1/Admin(config)# snmp-server user Bill Network-Monitor auth sha abcd1234 priv abcdefgh
```

To disable the SNMP user configuration or to remove an SNMP user, enter:

```
host1/Admin(config)# no snmp-server user Bill Network-Monitor auth sha abcd1234 priv
abcdefgh
```

Related Commands

(config) snmp-server community

(config) ssh key

To generate the Secure Shell (SSH) private key and the corresponding public key for use by the SSH server, use the **ssh key** command. Use the **no** form of this command to remove an SSH key pair.

ssh key {**dsa** | **rsa** | **rsa1**} [*bits* [**force**]]

no ssh key {**dsa** | **rsa** | **rsa1**}

Syntax Description

dsa	Generates the DSA key pair for the SSH version 2 protocol.
rsa	Generates the RSA key pair for the SSH version 2 protocol.
rsa1	Generates the RSA1 key pair for the SSH version 1 protocol.
bits	(Optional) Number of bits for the key pair. For DSA, enter an integer from 768 to 2048. For RSA and RSA1, enter an integer from 768 to 4096. The greater the number of bits that you specify, the longer it takes to generate the key. The default is 768.
force	(Optional) Forces the generation of a DSA or RSA key even when previous keys exist. If the SSH key pair option is already generated for the required version, use the **force** option to overwrite the previously generated key pair.

Command Modes

Configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Before you generate the key, set the hostname. This setting is used in the generation of the key.

The global administrator performs the key generation in the Admin context. All contexts associated with the ACE share the common key. There is only a single host-key pair.

If you are the administrator or another user authorized in the Admin context, use the **changeto** command in exec mode to move to the Admin context. An administrator can perform all allowable functions within the Admin context.

Ensure that you have an SSH host key pair with the appropriate version before you enable the SSH service. The SSH service accepts three types of key pairs for use by SSH versions 1 and 2. Generate the SSH host key pair according to the SSH client version used.

Examples

To generate an RSA1 key pair in the Admin context, enter:

```
host1/Admin(config)# ssh key rsa1 1024
generating rsa1 key
.....
generated rsa1 key
```

To remove the SSH host key pair, enter:

```
host1/Admin(config)# no ssh key rsa1
```

Related Commands

(config) ssh maxsessions
(config-cmap-mgmt) match protocol

(config) ssh maxsessions

To control the maximum number of Secure Shell (SSH) sessions allowed for each context, use the **ssh maxsessions** command. By default, the ACE supports four concurrent SSH management sessions for each user context and 16 concurrent SSH management sessions for the Admin context. Use the **no** form of this command to revert to the default number of SSH sessions.

ssh maxsessions *max_sessions*

no ssh maxsessions

Syntax Description

max_sessions	Maximum number of concurrent SSH sessions allowed for the associated context. The range is from 1 to 4 SSH sessions per user context and from 1 to 16 SSH sessions for the Admin context. The defaults are 4 (user context) and 16 (Admin context).

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The ACE supports a total maximum of 256 concurrent SSH sessions.

Examples

To set the maximum number of concurrent SSH sessions in the Admin context to 3, enter:

```
host1/Admin(config)# ssh maxsessions 3
```

To revert to the default of 16 SSH sessions for the Admin context, enter:

```
host1/Admin(config)# no ssh maxsessions
```

Related Commands

(config) ssh key
(config-cmap-mgmt) match protocol

(config) ssl-proxy service

To create a Secure Sockets Layer (SSL) proxy service, use the **ssl-proxy service** command. For SSL termination, you configure the ACE with an SSL proxy *server* service because the ACE acts as an SSL server. Once you create an SSL proxy service, the CLI enters into the ssl-proxy configuration mode, where you define each of the proxy service attributes that the ACE uses during the SSL handshake. Use the **no** form of this command to delete an existing SSL proxy service.

ssl-proxy service *pservice_name*

no ssl-proxy service *pservice_name*

Syntax Description

pservice_name	Name of the SSL proxy service. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the SSL feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

When you create a SSL proxy service, the CLI prompt changes to the ssl-proxy configuration mode, where you define the following SSL proxy service attributes:

- Authentication group
- Certificate
- Key pair
- Chain group
- Parameter map

For information about the commands in SSL proxy configuration mode, see the "SSL Proxy Configuration Mode Commands" section.

Examples

To create the SSL proxy service PSERVICE_SERVER, enter:

```
host1/Admin(config)# ssl-proxy service PSERVICE_SERVER
host1/Admin(config-ssl-proxy)#
```

To delete an existing SSL proxy service, enter:

```
host1/Admin(config)# no ssl-proxy PSERVICE_SERVER
```

Related Commands

(config-ssl-proxy) cert
(config-ssl-proxy) authgroup
(config-ssl-proxy) chaingroup
(config-ssl-proxy) key
(config-ssl-proxy) ssl advanced-options

(config) sticky http-content

To create a sticky group for HTTP content stickiness, use the **sticky http-content** command. The prompt changes to the sticky HTTP content configuration mode (config-sticky-content). Use the **no** form of this command to remove the sticky group from the configuration.

sticky http-content *name*

no sticky http-content *name*

Syntax Description

name	Unique identifier of the sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command requires the sticky feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To use the stickiness feature, you must allocate a minimum percentage of system resources to stickiness. Otherwise, the feature will not work. For more information about allocating resources, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the commands in sticky HTTP content configuration mode, see the "Sticky HTTP Content Configuration Mode Commands" section.

Examples

To create a sticky group for HTTP packet content stickiness, enter:

```
host1/Admin(config)# sticky http-content HTTP_CONTENT_GROUP
host1/Admin(config-sticky-content)#
```

To remove the sticky group from the configuration, enter:

```
host1/Admin(config)# no sticky http-content HTTP_CONTENT_GROUP
```

Related Commands

show running-config
show sticky database

(config) sticky http-cookie

To configure the ACE to use HTTP cookies for stickiness and enter sticky cookie configuration mode, use the **sticky http-cookie** command. The CLI prompt changes to (config-sticky-cookie). The ACE uses the learned cookie to provide stickiness between a client and a server for the duration of a transaction. Use the **no** form of this command to remove the sticky group from the configuration.

sticky http-cookie *name1 name2*

no sticky http-cookie *name1 name2*

Syntax Description

http-cookie *name1*	Specifies that the ACE learn the cookie value from the HTTP header of the client request or from the Set-Cookie message from the server. Enter a unique identifier for the cookie as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
name2	Unique identifier of the sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the sticky feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To use the stickiness feature, you must allocate a minimum percentage of system resources to stickiness. Otherwise, the feature will not work. For more information about allocating resources, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the commands in sticky cookie configuration mode, see the "Sticky HTTP Cookie Configuration Mode Commands" section.

Examples

To create a sticky group for cookie stickiness, enter:

```
host1/Admin(config)# sticky http-cookie cisco.com GROUP3
```

To remove the sticky group from the configuration, enter:

```
host1/Admin(config)# no sticky http-cookie cisco.com GROUP3
```

Related Commands

show running-config
show sticky database

(config) sticky http-header

To create an HTTP header sticky group to enable the ACE to stick client connections to the same real server based on HTTP headers, use the **sticky http-header** command. The prompt changes to the sticky-header configuration mode (config-sticky-header). Use the **no** form of this command to remove the sticky group from the configuration.

sticky http-header *name1 name2*

no sticky http-header *name1 name2*

Syntax Description

name1	HTTP header name. Enter the HTTP header name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. Alternatively, you can select one of the following standard headers: • **Accept** • **Accept-Charset** • **Accept-Encoding** • **Accept-Language** • **Authorization** • **Cache-Control** • **Connection** • **Content-MD5** • **Expect** • **From** • **Host** • **If-Match** • **Pragma** • **Referer** • **Transfer-Encoding** • **User-Agent** • **Via** See the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide* for a definition of each standard header.
name2	Unique identifier of the sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the sticky feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To use the stickiness feature, you must allocate a minimum percentage of system resources to stickiness. Otherwise, the feature will not work. For more information about allocating resources, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the commands in HTTP sticky header configuration mode, see the "Sticky HTTP Header Configuration Mode Commands" section.

Examples

To create a group for HTTP header stickiness, enter:

```
host1/Admin(config)# sticky http-header Host GROUP4
host1/Admin(config-sticky-header)#
```

To remove the sticky group from the configuration, enter:

```
host1/Admin(config)# no sticky http-header Host GROUP4
```

Related Commands

show running-config
show sticky database

(config) sticky ip-netmask

To create a sticky group for IP address stickiness, use the **sticky-ip netmask** command. The prompt changes to the sticky-IP configuration mode (config-sticky-ip). You can create a maximum of 4096 sticky groups on an ACE. Use the **no** form of this command to remove the sticky group from the configuration.

sticky ip-netmask *netmask* **address** {**both** | **destination** | **source**} *name*

no sticky ip-netmask *netmask* **address** {**both** | **destination** | **source**} *name*

Syntax Description

netmask	Network mask that the ACE applies to the IP address. Enter a network mask in dotted-decimal notation (for example, 255.255.255.0).
address {**both** | **destination** | **source**}	Specifies the IP address used for stickiness. Enter one of the following options after the address keyword: • **both**—Specifies that the ACE use both the source IP address and the destination IP address to stick the client to a server. • **destination**—Specifies that the ACE use the destination address specified in the client request to stick the client to a server. You typically use this keyword in caching environments. • **source**—Specifies that the ACE use the client source IP address to stick the client to a server. You typically use this keyword in web application environments.
name	Unique identifier of the sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the sticky feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To use the stickiness feature, you must allocate a minimum percentage of system resources to stickiness. Otherwise, the feature will not work. For more information about allocating resources, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the commands in sticky IP configuration mode, see the "Sticky IP Configuration Mode Commands" section.

Examples

To create a sticky group that uses IP address stickiness based on both the source IP address and the destination IP address, enter:

```
host1/Admin(config)# sticky ip-netmask 255.255.255.0 address both GROUP1
host1/Admin(config-sticky-ip)#
```

To remove the sticky group from the configuration, enter:

```
host1/Admin(config)# no sticky ip-netmask 255.255.255.0 address both GROUP1
```

Related Commands

show running-config
show sticky database

(config) sticky layer4-payload

To create a sticky group for Layer 4 payload stickiness, use the **sticky layer4-payload** command. The prompt changes to the sticky Layer 4 payload configuration mode (config-sticky-l4payloa). Use the **no** form of this command to remove the sticky group from the configuration.

sticky layer4-payload *name*

no sticky layer4-payload *name*

Syntax Description

name	Unique identifier of the sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command requires the sticky feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To use the stickiness feature, you must allocate a minimum percentage of system resources to stickiness. Otherwise, the feature will not work. You can create a maximum of 4096 sticky groups on an ACE.For more information about allocating resources, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the commands in sticky Layer 4 payload configuration mode, see the "Sticky Layer 4 Payload Configuration Mode Commands" section.

Examples

To create a sticky group that uses Layer 4 payload stickiness, enter:

```
host1/Admin(config)# sticky layer4-payload L4_PAYLOAD_GROUP
host1/Admin(config-sticky-l4payloa)#
```

To remove the sticky group from the configuration, enter:

```
host1/Admin(config)# no sticky layer4-payload L4_PAYLOAD_GROUP
```

Related Commands

show running-config
show sticky database

(config) sticky radius framed-ip

To create a sticky group for RADIUS attribute stickiness, use the **sticky radius framed-ip** command. The prompt changes to the sticky RADIUS configuration mode (config-sticky-radius). Use the **no** form of this command to remove the sticky group from the configuration.

sticky radius framed-ip [**calling-station-id** | **username**] *name*

no sticky radius framed-ip [**calling-station-id** | **username**] *name*

Syntax Description

calling-station-id	(Optional) Specifies stickiness based on the RADIUS framed IP attribute and the calling station ID attribute.
username	(Optional) Specifies stickiness based on the RADIUS framed IP attribute and the username attribute.
name	Unique identifier of the RADIUS sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command requires the sticky feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To use the stickiness feature, you must allocate a minimum percentage of system resources to stickiness. Otherwise, the feature will not work. For more information about allocating resources, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For information about the commands in sticky RADIUS configuration mode, see the "Sticky RADIUS Configuration Mode Commands" section.

Examples

To create a sticky group for RADIUS attribute stickiness, enter:

```
host1/Admin(config)# sticky radius framed-ip calling-station-id RADIUS_GROUP
host1/Admin(config-sticky-radius)#
```

To remove the sticky group from the configuration, enter:

```
host1/Admin(config)# no sticky radius framed-ip calling-station-id RADIUS_GROUP
```

Related Commands

show running-config
show sticky database

(config) sticky rtsp-header

To create an RTSP header sticky group to enable the ACE to stick client connections to the same real server based on the RTSP Session header field, use the **sticky rtsp-header** command. The prompt changes to the sticky header configuration mode prompt (config-sticky-header). Use the **no** form of this command to remove the sticky group from the configuration.

sticky rtsp-header *name1 name2*

no sticky rtsp-header *name1 name2*

Syntax Description

name1	RTSP header field. The ACE supports only the RTSP Session header field for stickiness. Enter **Session**.
name2	Unique identifier of the sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command requires the sticky feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To use the stickiness feature, you must allocate a minimum percentage of system resources to stickiness. Otherwise, the feature will not work. For more information about allocating resources, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The ACE supports only the RTSP Session header field for stickiness.

For information about the commands in RTSP sticky header configuration mode, see the "Sticky RTSP Header Configuration Mode Commands" section.

Examples

To create a group for RTSP header stickiness, enter:

```
host1/Admin(config)# sticky rtsp-header Session RTSP_GROUP
host1/Admin(config-sticky-header)#
```

To remove the sticky group from the configuration, enter:

```
host1/Admin(config)# no sticky rtsp-header Session RTSP_GROUP
```

Related Commands

show running-config
show sticky database

(config) sticky sip-header

To create a SIP header sticky group to enable the ACE to stick client connections to the same real server based on the SIP Call-ID header field, use the **sticky sip-header** command. The prompt changes to the sticky header configuration mode prompt (config-sticky-header). Use the **no** form of this command to remove the sticky group from the configuration.

sticky sip-header *name1 name2*

no sticky sip-header *name1 name2*

Syntax Description

name1	SIP header field. The ACE supports only the SIP Call-ID header field for stickiness. Enter **Call-ID**.
name2	Unique identifier of the sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command requires the sticky feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To use the stickiness feature, you must allocate a minimum percentage of system resources to stickiness. Otherwise, the feature will not work. For more information about allocating resources, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The ACE supports only the SIP Call-ID header field for stickiness.

For information about the commands in SIP sticky header configuration mode, see the "Sticky SIP Header Configuration Mode Commands" section.

Examples

To create a group for SIP header stickiness, enter:

```
host1/Admin(config)# sticky sip-header Call-ID SIP_GROUP
host1/Admin(config-sticky-header)#
```

To remove the sticky group from the configuration, enter:

```
host1/Admin(config)# no sticky sip-header Call-ID SIP_GROUP
```

Related Commands

show running-config
show sticky database

(config) tacacs-server deadtime

To globally set the time interval in which the ACE verifies whether a nonresponsive server is operational, use the **tacacs-server deadtime** command. Use the **no** form of this command to reset the Terminal Access Controller Access Control System Plus (TACACS+) server dead-time request to the default of 0.

tacacs-server deadtime *minutes*

no tacacs-server deadtime *minutes*

Syntax Description

minutes	Length of time in minutes that the ACE skips a nonresponsive TACACS+ server for transaction requests. Enter an integer from 0 to 1440 (24 hours). The default is 0.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The dead-time interval starts when the server does not respond to an authentication request transmission. When the server responds to a probe access-request packet, the ACE retransmits the authentication request to the server.

Using this command causes the ACE to mark as dead any TACACS+ servers that fail to respond to authentication requests. This action avoids the wait for the request to time out before trying the next configured server. The ACE skips a TACACS+ server that is marked as dead by additional requests for the duration of minutes.

Examples

To globally configure a 15-minute dead time for TACACS+ servers that fail to respond to authentication requests, enter:

```
host1/Admin(config)# tacacs-server deadtime 15
```

To set the TACACS+ server dead-time request to 0, enter:

```
host1/Admin(config)# no tacacs-server deadtime 15
```

Related Commands

show aaa
(config) aaa group server
(config) tacacs-server host

(config) tacacs-server host

To specify the Terminal Access Controller Access Control System Plus (TACACS+) server IP address, encrypted key, destination port, and other options, use the **tacacs-server host** command. You can enter multiple **tacacs-server host** commands to configure multiple TACACS+ servers. Use the **no** form of this command to revert to the default TACACS+ server authentication setting.

tacacs-server host *ip_address* [**key** *shared_secret* [**0** *shared_secret* | **7** *shared_secret*]] [**port** *port_number*] [**timeout** *seconds*]

no tacacs-server host *ip_address* [**key** *shared_secret* [**0** *shared_secret* | **7** *shared_secret*]] [**port** *port_number*] [**timeout** *seconds*]

Syntax Description

ip_address	IP address for the TACACS+ server. Enter the address in dotted-decimal IP notation (for example, 192.168.11.1).
key	(Optional) Enables an authentication key for communication between the ACE and the daemon running on the TACACS+ server.
shared_secret	Key used to authenticate communication between the TACACS+ client and server. The shared secret must match the one configured on the TACACS+ server. Enter the shared secret as a case-sensitive string with no spaces with a maximum of 63 alphanumeric characters.
0	(Optional) Configures a key specified in clear text (indicated by 0) to authenticate communication between the TACACS+ client and server.
7	(Optional) Configures a key specified in encrypted text (indicated by 7) to authenticate communication between the TACACS+ client and server.
port *port_number*	(Optional) Specifies the TCP destination port for communicating authentication requests to the TACACS+ server. By default, the TACACS+ authentication port is 1812 (as defined in RFC 2138 and RFC 2139). If your TACACS+ server uses a port other than 1812, use the **port** keyword to configure the ACE for the appropriate port before starting the TACACS+ service. The *port_number* argument specifies the TACACS+ port number. Enter an integer from 1 to 65535.
timeout *seconds*	(Optional) Specifies the time interval that the ACE waits for the TACACS+ server to reply to an authentication request. Enter an integer from 1 to 60. The default is 1 second.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The **key** *shared_secret* text string must match the encryption key used on the TACACS+ server. This key overrides the global setting of the **(config) tacacs-server key** command. If you do not specify a key, the global value is used. TACACS+ keys are always stored in encrypted form in persistent storage. The running configuration also displays keys in encrypted form.

For the specified server, the **timeout** keyword used with the **tacacs-server host** command overrides the global setting assigned using the **(config) tacacs-server timeout** command.

By default, the ACE waits 1 second for the TACACS+ server to reply to an authentication request before it declares a timeout and attempts to contact the next server in the group. If all servers in the group are unavailable for authentication and accounting, the ACE tries the local database if you configure the database as the local fallback method by entering the **(config) aaa authentication login** or the **(config) aaa accounting default** command.

Examples

To configure TACACS+ server authentication parameters, enter:

```
host1/Admin(config)# tacacs-server host 192.168.3.2 key HostKey
host1/Admin(config)# tacacs-server host 192.168.3.2 tacacs3 key 7 1234
host1/Admin(config)# tacacs-server host 192.168.3.2 port 1645
host1/Admin(config)# tacacs-server host 192.168.3.2 timeout 5
```

To revert to a default TACACS+ server authentication setting, enter:

```
host1/Admin(config)# no tacacs-server host 192.168.3.2 tacacs3 key 7 1234
```

Related Commands

show aaa
(config) aaa group server

(config) tacacs-server key

To globally configure an authentication key for communication between the ACE and the Terminal Access Controller Access Control System Plus (TACACS+) daemon running on each TACACS+ server, use the **tacacs-server key** command. Use the **no** form of this command to delete the key.

tacacs-server key [**0** | **7**] *shared_secret*

no tacacs-server key [**0** | **7**] *shared_secret*

Syntax Description

0	(Optional) Configures a key specified in clear text (indicated by 0) to authenticate communication between the TACACS+ client and server.
7	(Optional) Configures a key specified in encrypted text (indicated by 7) to authenticate communication between the TACACS+ client and server.
shared_secret	Key used to authenticate communication between the TACACS+ client and server. The shared secret must match the one configured on the TACACS+ server. Enter the shared secret as a case-sensitive string with no spaces with a maximum of 63 alphanumeric characters or you can include spaces if you enclose the entire key with quotation marks (for example, “my key”).

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The key is a text string that must match the encryption key used on the TACACS+ server. TACACS+ keys are always stored in encrypted form in persistent storage on the ACE. This global key will be applied to those TACACS+ servers in a named server group for which a shared secret is not individually configured using the **(config) tacacs-server host** command.

Examples

To globally configure an authentication key in encrypted text (indicated by 7) to authenticate communication between the TACACS+ client and server, enter:

```
host1/Admin(config)# tacacs-server key 7 abe4DFeeweo00o
```

To delete the key, enter:

```
host1/Admin(config)# no tacacs-server key 7 abe4DFeeweo00o
```

Related Commands

show aaa
(config) aaa group server
(config) tacacs-server host

(config) tacacs-server timeout

To globally change the time interval that the ACE waits for the Terminal Access Controller Access Control System Plus (TACACS+) server to reply before retransmitting an authentication request to the TACACS+ server, use the **tacacs-server timeout** command. The ACE applies the global timeout value to those TACACS+ servers for which a timeout value is not individually configured using the **(config) tacacs-server host** command. Use the **no** form of this command to revert to the default of 1 second between transmission attempts.

tacacs-server timeout *seconds*

no tacacs-server timeout *seconds*

Syntax Description

seconds	Timeout value in seconds. Valid entries are from 1 to 60 seconds. The default is 1 second.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To globally configure the timeout value to 30 seconds, enter:

```
host1/Admin(config)# tacacs-server timeout 30
```

To revert to the default of 1 second between transmission attempts, enter:

```
host1/Admin(config)# no tacacs-server timeout 30
```

Related Commands

show aaa
(config) aaa group server
(config) tacacs-server host

(config) telnet maxsessions

To control the maximum number of Telnet sessions allowed for each context, use the **telnet maxsessions** command. By default, the ACE supports 4 concurrent Telnet management sessions for each user context and 16 concurrent Telnet management sessions for the Admin context. Use the **no** form of this command to revert to the default number of Telnet sessions.

telnet maxsessions *sessions*

no telnet maxsessions

Syntax Description

sessions	Maximum number of concurrent Telnet sessions allowed for the associated context. The range is from 1 to 4 Telnet sessions per user context and from 1 to 16 Telnet sessions for the Admin context. The defaults are 4 (user context) and 16 (Admin context).

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The ACE supports a total maximum of 256 concurrent Telnet sessions.

Examples

To set the maximum number of concurrent Telnet sessions to 3 in the Admin context, enter:

```
host1/Admin(config)# telnet maxsessions 3
```

To revert to the default of 16 Telnet sessions for the Admin context, enter:

```
host1/Admin(config)# no telnet maxsessions
```

Related Commands

telnet
clear telnet
show telnet
(config-cmap-mgmt) match protocol

(config) timeout xlate

To configure an idle timeout for Network Address Translation (NAT), use the **timeout xlate** command. Use the **no** form of this command to reset the idle timeout to the default of 10800 seconds (3 hours).

timeout xlate *seconds*

no timeout xlate

Syntax Description

seconds	Time in seconds that the ACE waits to free the Xlate slot after it becomes idle. Enter an integer from 60 to 2147483. The default is 10800 seconds (3 hours).

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the NAT feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To specify an idle timeout of 120 seconds (2 minutes), enter:

```
host1/Admin(config)# timeout xlate 120
```

To reset the NAT idle timeout to the default value of 10800 seconds (3 hours), enter:

```
host1/Admin(config)# no timeout xlate
```

Related Commands

(config) policy-map
(config-pmap-c) nat dynamic
(config-pmap-c) nat static

(config) username

To change the default username and password, use the **username** command. Use the **no** form of this command to remove the username from the configuration.

username *name1* [**password** [**0** | **5**] {*password*}] [**expire** *date*] [**role** *name2* {**domain** *name3 name4 . . . namen*}]

no username *name1* [**password** [**0** | **5**] {*password*}] [**expire** *date*] [**role** *name2* {**domain** *name3 name4 . . . namen*}]

Syntax Description

name1	Identifier of the user that you are creating. Enter an unquoted text string with no spaces and a maximum of 24 alphanumeric characters.
password	(Optional) Indicates that a password follows.
0	(Optional) Specifies a clear text password.
5	(Optional) Specifies an MD5-hashed strong encryption password.
password	Password in clear text, encrypted text, or MD5 strong encryption, depending on the numbered option that you enter. If you do not enter a numbered option, the password is in clear text by default. If you enter the **password** keyword, you must enter a password. Enter a password as an unquoted text string with a maximum of 64 alphanumeric characters. The ACE supports the following special characters in a password: , . / = + - ^ @ ! % ~ # $ * ( ) Note that the ACE encrypts clear text passwords in the running-config.
expire *date*	(Optional) Specifies the expiration date of the user account. Enter the expiration date in the format *yyyy-mm-dd*.
role *name2*	(Optional) Specifies an existing role that you want to assign to the user.
domain *name3 name4 . . . namen*	Specifies the domains in which the user can operate. You can enter multiple domain names up to a maximum of 10, including **default-domain**.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the context Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

If you do not assign a role to a new user, the default role is Network-Monitor. For users that you create in the Admin context, the default scope of access is the entire device. For users that you create in other contexts, the default scope of access is the entire context. If you need to restrict a user's access, you must assign a role-domain pair. For more information about creating users, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To change the default username, enter:

```
host1/Admin(config)# username USER1 password MYSECRET expire 2005-12-31 role TECHNICIAN
domain D1 default-domain

host1/Admin(config)# username USER2 password HERSECRET expire 2005-12-31 role Admin
domain default-domain D2
```

To remove a username from the configuration, enter:

```
host1/Admin(config)# no username USER1
```

Related Commands

clear user
show role
show user-account
show users

Action List Modify Configuration Mode Commands

Action list modify configuration mode commands allow you to configure ACE action lists. An action list is a named group of actions that you associate with a Layer 7 HTTP class map in a Layer 7 HTTP policy map. You can create an action list to modify an HTTP header or to rewrite an HTTP redirect URL for Secure Sockets Layer (SSL).

To create an action list, use the **action-list type modify http** command. The CLI prompt changes to (config-actlist-modify). Use the **no** form of this command to remove the action list from the configuration.

action-list type modify http *name*

no action-list type modify http *name*

Syntax Description

name	Unique name for the action list. Enter an unquoted text string with a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To create an action list, enter:

```
host1/Admin(config)# action-list type modify http HTTP_MODIFY_ACTLIST
host1/Admin(config-actlist-modify)#
```

To remove the action list from the configuration, enter:

```
host1/Admin(config)# no action-list type modify http HTTP_MODIFY_ACTLIST
```

Related Commands

show running-config
show stats

(config-actlist-modify) description

To add a description about the action list, use the **description** command. Use the **no** form of this command to remove the description from the action list.

description *text_string*

no description

Syntax Description

text_string	Description for the action list. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Action list modify configuration mode

Admin and user contexts

Command History

Release	Modification
A3(2.3)	This command was introduced.

Usage Guidelines

After you create an action list and associate actions with it, you must associate the action list with a Layer 7 policy map. For details, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To add a description for the action list, enter:

```
host1/Admin(config)# action-list type modify http HTTP_MODIFY_ACTLIST
host1/Admin(config-actlist-modify)# description action - delete request
```

To remove the description from the action list, enter:

```
host1/Admin(config-actlist-modify)# no description
```

Related Commands

show action-list

(config-actlist-modify) header delete

To delete an HTTP header from a client request, a server response, or from both, use the **header delete** command in action list modify configuration mode. Use the **no** form of this command to remove the HTTP header delete action from the action list.

header delete {**request** | **response** | **both**} *header-name*

no header delete {**request** | **response** | **both**} *header-name*

Syntax Description

request	Specifies that the ACE delete the header from HTTP request packets from clients.
response	Specifies that the ACE delete the header from HTTP response packets from servers.
both	Specifies that the ACE delete the header from both HTTP request packets and response packets.
header-name	Identifier of the HTTP header that you want to delete. Enter an unquoted text string with a maximum of 255 alphanumeric characters.

Command Modes

Action list modify configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

After you create an action list and associate actions with it, you must associate the action list with a Layer 7 policy map. For details, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To delete the Host header from request packets only, enter:

```
host1/Admin(config)# action-list type modify http HTTP_MODIFY_ACTLIST
host1/Admin(config-actlist-modify)# header delete request Host
```

To remove the header delete action from the action list, enter:

```
host1/Admin(config-actlist-modify)# no header delete request Host
```

Related Commands

(config) action-list type modify http
(config-actlist-modify) header insert
(config-actlist-modify) header rewrite

(config-actlist-modify) header insert

When the ACE uses NAT to translate the source IP address of a client to a VIP address, servers need a way to identify that client for the TCP and IP return traffic. To identify a client whose source IP address has been translated using NAT, you can instruct the ACE to insert a generic header and string value in the client HTTP request.

To insert a header name and value in an HTTP request from a client, a response from a server, or both, use the **header insert** command in action list modify configuration mode. Use the **no** form of this command to remove the HTTP header insert action from the action list.

header insert {**request | response | both**} *header-name* **header-value** *expression*

no header insert {**request | response | both**} *header-name* **header-value** *expression*

Syntax Description

request	Specifies that the ACE insert an HTTP header in HTTP request packets from clients.
response	Specifies that the ACE insert an HTTP header in HTTP response packets from servers.
both	Specifies that the ACE insert an HTTP header in both HTTP request packets and response packets.
header-name	Identifier of an HTTP header. Enter an unquoted text string with a maximum of 255 alphanumeric characters.
header-value *expression*	Specifies the value of the HTTP header that you want to insert in request packets, response packets, or both. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters. You can also use the following dynamic replacement strings: • **%is**—Insert the source IP address in the HTTP header. • **%id**—Insert the destination IP address in the HTTP header. • **%ps**—Insert the source port in the HTTP header. • **%pd**—Insert the destination port in the HTTP header.

Command Modes

Action list modify configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

After you create an action list and associate actions with it, you must associate the action list with a Layer 7 policy map. For details, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

With either TCP server reuse or persistence rebalance enabled, the ACE inserts a header in every client request. For information about TCP server reuse, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To include a header insert action for both request and response packets in an action list, enter:

```
host1/Admin(config)# action-list type modify http HTTP_MODIFY_ACTLIST
host1/Admin(config-actlist-modify)# header insert both Host header-value www.cisco.com
```

To remove the insert action from the action list, enter:

```
host1/Admin(config-actlist-modify)# no header insert both Host header-value www.cisco.com
```

Related Commands

(config) action-list type modify http
(config-actlist-modify) header delete
(config-actlist-modify) header rewrite

(config-actlist-modify) header rewrite

To rewrite an HTTP header value in request packets from a client, response packets from a server, or both, use the **header rewrite** command in action list modify configuration mode. Use the **no** form of this command to remove the HTTP header rewrite action from the action list.

header rewrite {**request** | **response** | **both**} *header-name* **header-value** *expression* **replace** *pattern*

no header rewrite {**request** | **response** | **both**} *header-name* **header-value** *expression* **replace** *pattern*

Syntax Description

request	Specifies that the ACE rewrite an HTTP header string in HTTP request packets from clients.
response	Specifies that the ACE rewrite an HTTP header string in HTTP response packets from servers.
both	Specifies that the ACE rewrite an HTTP header string in both HTTP request packets and response packets.
header-name	Identifier of the HTTP header that you want to rewrite. Enter an unquoted text string with a maximum of 255 alphanumeric characters.
header-value *expression*	Specifies the value of the HTTP header that you want to replace in request packets, response packets, or both. Enter a text string from 1 to 255 alphanumeric characters. The ACE supports the use of regular expressions for matching data strings. Use parenthesized expressions for dynamic replacement using %1 and %2 in the replacement pattern. **Note** When matching data strings, the period (.) and question mark (?) characters do not have a literal meaning in regular expressions. Use brackets ([]) to match these symbols (for example, enter www[.]xyz[.]com instead of www.xyz.com). You can also use a backslash (\) to escape a dot (.) or a question mark (?).

replace *pattern*	Specifies the pattern string that you want to substitute for the header value regular expression. For dynamic replacement of the first and second parenthesized expressions from the header value, use %1 and %2, respectively.

Command Modes

Action list modify configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

After you create an action list and associate actions with it, you must associate the action list with a Layer 7 policy map. For details, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To include a header replace action for HTTP request packets in an action list, enter:

```
host1/Admin(config)# action-list type modify http HTTP_MODIFY_ACTLIST
host1/Admin(config-actlist-modify)# header rewrite request Host header-value www.cisco.com
replace ?
```

To remove the replace action from the action list, enter:

```
host1/Admin(config-actlist-modify)# no header rewrite request Host header-value
www.cisco.com replace ?
```

Related Commands

(config) action-list type modify http
(config-actlist-modify) header delete
(config-actlist-modify) header insert

(config-actlist-modify) ssl url rewrite location

To specify the SSL URL, SSL port, and clear port for rewrite, use the **ssl url rewrite location** command. SSL URL rewrite changes the redirect URL from http:// to https:// in the Location response header from the server before sending the response to the client. By doing so, it allows you to avoid nonsecure HTTP redirects because all client connections to the web server will be SSL, thus ensuring the secure delivery of HTTPS content back to the client. Use the **no** form of this command to remove the SSL rewrite specification from the configuration.

ssl url rewrite location *expression* [**clearport** *number*] [**sslport** *number*]

no ssl url rewrite location *expression* [**clearport** *number*] [**sslport** *number*]

Syntax Description

location *expression*	Specifies the rewriting of the URL in the Location response header based on a URL regular expression match. If the URL in the Location header matches the URL regular expression string that you specify, the ACE rewrites the URL from http:// to https:// and rewrites the port number. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters. You can enter a text string with spaces if you enclose the entire string in quotation marks (“). The ACE supports the use of regular expressions for matching data strings. **Note** When matching data strings, the period (.) and question mark (?) characters do not have a literal meaning in regular expressions. Use brackets ([]) to match these symbols (for example, enter www[.]xyz[.]com instead of www.xyz.com). You can also use a backslash (\) to escape a dot (.) or a question mark (?).
clearport *number1*	(Optional) Specifies the clear port number to which the ACE translates the SSL port number before sending a server redirect response to the client. Enter an integer from 1 to 65535. The default is 80.
sslport *number*	(Optional) Specifies the SSL port number from which the ACE translates a clear port number before sending the server redirect response to the client. Enter an integer from 1 to 65535. The default is 443.

Command Modes

Action list modify configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

After you create an action list and configure an HTTP redirect URL for SSL, you must associate the action list with a Layer 3 and Layer 4 policy map. For details, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To specify SSL URL rewrite using the default SSL port of 443 and clear port of 80, enter:

```
host1/Admin(config)# action-list type modify http HTTP_MODIFY_ACTLIST
host1/Admin(config-actlist-modify)# ssl url rewrite location www\.website\.com
```

In this case, the ACE rewrites all HTTP redirects to http://www.website.com/ as https://www.website.com/ and forwards them to the client.

Related Commands

(config) action-list type modify http

Action List Optimization Configuration Mode Commands

The action list optimization mode allows you to configure a series of application acceleration and optimization statements. An action list groups a series of individual application acceleration and optimization functions that apply to a specific type of operation. After you enter this command, the system enters the corresponding action list configuration mode.

To access the action list optimization mode, enter the **action-list type optimization http** command. The CLI prompt changes to (config-actlist-optm). To remove an action list optimization selection, use the **no** form of the command. For details about using the commands in the action list optimization mode, see the *Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide*.

action-list type optimization http *list_name*

no action-list type optimization http *list_name*

Syntax Description

list_name	Name assigned to the action list. Enter a unique name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The **action-list type** command allows you to configure a series of statements. An action list groups a series of individual functions that apply to a specific type of application acceleration and optimization operation. After you enter this command, the system enters the corresponding action list configuration mode.

After you configure the action list, you associate it with a specific statement in a Layer 7 HTTP optimization policy map. The Layer 7 optimization HTTP policy map activates an optimization HTTP action list that allows you to configure the specified optimization actions.

Examples

To create an optimization HTTP action list, enter:

```
host1/Admin(config)# action-list type optimization http ACT_LIST1
host1/Admin(config-actlist-optm)#
```

To remove the action list from the configuration, enter:

```
host1/Admin(config)# no action-list type optimization http ACT_LIST1
```

Related Commands

show action-list
show running-config
(config) parameter-map type
(config) policy-map

(config-actlist-optm) appscope

To enable AppScope performance monitoring by the optional Cisco AVS 3180A Management Station for use with the ACE, use the **appscope** command. Use the **no** form of this command to disable the AppScope function from the action list.

appscope

no appscope

Syntax Description

This command has no keywords or arguments.

Command Modes

Action list optimization mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The statistical log contains an entry for each ACE optimization request to the server and is used for statistical analysis by the optional Cisco AVS 3180A Management Station. The ACE collects statistical log and sends it to the Cisco AVS 3180A Management Station for loading into the database. For details about the use of the Cisco AVS 3180A Management Station for database, management, and reporting features for the ACE optimization functionality, including AppScope reporting, see the *Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide*.

To control the AppScope features that measure application acceleration and optimization performance, use the **appscope** commands in parameter map optimization configuration mode. See the "Parameter Map Optimization Configuration Mode Commands" section for details.

To specify the host (the syslog server on the Management Station) that receives the syslog messages sent by the ACE, use the **logging host** configuration command. See the **(config) logging host** command. This command allows you to identify the IP address of the Management Station that will be used as the syslog server. You can specify that the host uses either UDP or TCP to send messages to the syslog server.

Examples

For example, enter:

```
host1/Admin(config)# action-list type optimization http ACT_LIST1
host1/Admin(config-actlist-optm)# appscope
```

To disable the AppScope function from the action list, enter:

```
host1/Admin(config-actlist-optm)# no appscope
```

Related Commands

(config) logging host
(config-parammap-optmz) appscope optimize-rate-percent
(config-parammap-optmz) parameter-summary parameter-value-limit
(config-parammap-optmz) request-grouping-string

(config-actlist-optm) cache

To enable cache optimization for the corresponding URLs, use the **cache** command. Use the **no** form of this command to disable the cache function from the action list.

cache {**dynamic** | **forward** | **forward-with-wait**}

no cache {**dynamic** | **forward** | **forward-with-wait**}

Syntax Description

dynamic	Enables Adaptive Dynamic Caching for the corresponding URLs, even if the expiration settings in the response indicate that the content is dynamic. The expiration of cache objects is controlled by the cache expiration settings based on the time or server load (performance assurance).
forward	Enables the cache forward feature for the corresponding URLs. This keyword allows the ACE to serve the object from its cache (static or dynamic) even when the object has expired if the maximum cache TTL time period has not yet expired (set using the **cache ttl** command in parameter map optimization mode). At the same time, the ACE sends an asynchronous request to the origin server to refresh its cache of the object.
forward-with-wait	Enables the cache forward with wait feature for the corresponding URLs. If the object has expired but the maximum cache TTL time period has not expired (set using the **cache ttl** command in parameter map optimization mode), the ACE sends a request to the origin server for the object. The rest of the users requesting this page will still continue to receive the content from the cache during this time. When the fresh object is returned, it is sent to the requesting user and the cache is also updated. This keyword is similar to the **forward** keyword, except that a single user must wait for the object to be updated before the request is satisfied. This keyword is useful in situations where you are unable to specify the **forward** keyword because the application requires a context for processing and an asynchronous update process is not appropriate.

Command Modes

Action list optimization mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You define the ACE cache object key, cache freshness, and cache request/response policy settings by configuring the cache and cache-policy commands in parameter map optimization configuration mode. See "Parameter Map Optimization Configuration Mode Commands" section for details.

The ACE restricts you from enabling Adaptive Dynamic Caching if you have previously specified either the **delta** command (see "(config-actlist-optm) delta") or the **dynamic etag** command (see "(config-actlist-optm) dynamic etag").

Examples

For example, to enable the cache forward feature for the corresponding URLs, enter:

```
host1/Admin(config)# action-list type optimization http ACT_LIST1
host1/Admin(config-actlist-optm)# cache forward
```

To disable the cache function from the action list, enter:

```
host1/Admin(config-actlist-optm)# no cache forward
```

Related Commands

(config-parammap-optmz) cache key-modifier
(config-parammap-optmz) cache parameter
(config-parammap-optmz) cache ttl
(config-parammap-optmz) cache-policy request
(config-parammap-optmz) cache-policy response

(config-actlist-optm) delta

To enable delta optimization to condense corresponding URLs, use the **delta** command. Use the **no** form of this command to disable delta optimization from the action list.

delta

no delta

Syntax Description

This command has no keywords or arguments.

Command Modes

Action list optimization mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The ACE restricts you from enabling delta optimization if you have previously specified either the **cache dynamic** command (see "(config-actlist-optm) cache") or the **dynamic etag** command (see "(config-actlist-optm) dynamic etag").

Examples

For example, enter:

```
host1/Admin(config)# action-list type optimization http ACT_LIST1
host1/Admin(config-actlist-optm)# delta
```

To disable delta optimization from the action list, enter:

```
host1/Admin(config-actlist-optm)# no delta
```

Related Commands

(config-parammap-optmz) delta

(config-actlist-optm) description

To add a description about the action list, use the **description** command. Use the **no** form of this command to remove the description from the action list.

description *text_string*

no description

Syntax Description

text_string	Description for the action list. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Action list modify configuration mode

Admin and user contexts

Command History

Release	Modification
A3(2.3)	This command was introduced.

Usage Guidelines

After you create an action list and associate actions with it, you must associate the action list with a Layer 7 policy map. For details, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To add a description for the action list, enter:

```
host1/Admin(config)# action-list type optimization http ACT_LIST1
host1/Admin(config-actlist-optm)# description action - delta
```

To remove the description from the action list, enter:

```
host1/Admin(config-actlist-optm)# no description
```

Related Commands

show action-list

(config-actlist-optm) dynamic etag

To enable just-in-time object acceleration for the corresponding URLs, use the **dynamic etag** command. Use the **no** form of this command to disable just-in-time object acceleration from the action list.

dynamic etag

no dynamic etag

Syntax Description

This command has no keywords or arguments.

Command Modes

Action list optimization mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The ACE restricts you from enabling just-in-time object acceleration if you have previously specified either the **cache dynamic** command (see "(config-actlist-optm) cache") or the **delta** command (see "(config-actlist-optm) delta").

Examples

For example, enter:

```
host1/Admin(config)# action-list type optimization http ACT_LIST1
host1/Admin(config-actlist-optm)# dynamic etag
```

To disable just-in-time object acceleration from the action list, enter:

```
host1/Admin(config-actlist-optm)# no dynamic etag
```

Related Commands

This command has no related commands.

(config-actlist-optm) flashforward

To enable FlashForward for the corresponding URLs and to transform embedded objects, use the **flashforward** command. Use the **no** form of this command to disable FlashForward from the action list.

flashforward

no flashforward

Syntax Description

This command has no keywords or arguments.

Command Modes

Action list optimization mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The **flashforward** and **flashforward-object** commands cannot be configured in the same optimization action list; these two commands are mutually exclusive.

Examples

For example, enter:

```
host1/Admin(config)# action-list type optimization http ACT_LIST1
host1/Admin(config-actlist-optm)# flashforward
```

To disable FlashForward from the action list, enter:

```
host1/Admin(config-actlist-optm)# no flashforward
```

Related Commands

(config-actlist-optm) flashforward-object
(config-parammap-optmz) flashforward refresh-policy
(config-parammap-optmz) rebase

(config-actlist-optm) flashforward-object

To enable FlashForward static caching for the corresponding URLs, use the **flashforward-object** command. Use the **no** form of this command to disable FlashForward static caching from the action list.

flashforward-object

no flashforward-object

Syntax Description

This command has no keywords or arguments.

Command Modes

Action list optimization mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The **flashforward-object** and **flashforward** commands cannot be configured in the same optimization action list; these two commands are mutually exclusive.

Examples

For example, enter:

```
host1/Admin(config)# action-list type optimization http ACT_LIST1
host1/Admin(config-actlist-optm)# flashforward-object
```

To disable FlashForward static caching from the action list, enter:

```
host1/Admin(config-actlist-optm)# no flashforward-object
```

Related Commands

(config-actlist-optm) flashforward
(config-parammap-optmz) flashforward refresh-policy
(config-parammap-optmz) rebase

Authentication Group Configuration Mode Commands

Authentication group configuration mode commands allow you to configure client authentication on a Secure Sockets Layer (SSL)-proxy service by assigning the authentication group to the service.

To create an authentication group and access authgroup configuration mode, use the **crypto authgroup** command. The CLI prompt changes to (config-authgroup). Use the **no** form of this command to delete an existing authentication group.

crypto authgroup *group_name*

no crypto authgroup *group_name*

Syntax Description

group_name	Name that you assign to the certificate authentication group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command requires the SSL feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

During the flow of a normal SSL handshake, the server send its certificate to the client. The client verifies the identity of the server through the certificate. However, the client does not send any identification of its own to the server. When the client authentication feature is enabled on the ACE, it requires that the client send a certificate to the server.

On the ACE, you can implement a group of certificates that are trusted as certificate signers by creating an authentication group.

Examples

To create the authentication group AUTH-CERT1, enter:

```
host1/Admin(config)# crypto authgroup AUTH-CERT1
```

Related Commands

(config) ssl-proxy service

(config-authgroup) cert

To add certificate files to the authentication group, use the **cert** command. You can configure an authentication group with up to four certificates. Use the **no** form of this command to remove a certificate file from the authentication group.

cert *cert_filename*

no cert *cert_filename*

Syntax Description

cert_filename	Name of an existing certificate file stored on the ACE. Enter an unquoted text string with no spaces and a maximum of 40 alphanumeric characters. To display a list of available certificate files, use the **do show crypto files** command.

Command Modes

Chaingroup configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

It is not necessary to add the certificates in any type of hierarchical order because the device that verifies the certificates determines the correct order.

Examples

To add the certificate files MYCERTS.PEM and MYCERTS_2.PEM to the authentication group, enter:

```
host1/Admin(config-authgroup)# cert MYCERTS.PEM
host1/Admin(config-authgroup)# cert MYCERTS_2.PEM
```

To remove the certificate file MYCERTS_2.PEM from the authentication group, enter:

```
host1/Admin(config-authgroup)# no cert MYCERTS_2.PEM
```

Related Commands

(config) crypto authgroup

Chaingroup Configuration Mode Commands

Chaingroup configuration mode commands allow you to add Secure Sockets Layer (SSL) certificate files to a chain group.

To create a new chain group (or modify an existing chain group) and access chaingroup configuration mode, use the **crypto chaingroup** command. The CLI prompt changes to (config-chaingroup). Use the **no** form of the command to delete an existing chain group.

crypto chaingroup *group_name*

no crypto chaingroup *group_name*

Syntax Description

group_name	Name that you assign to the chain group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the SSL feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

A chain group specifies the certificate chains that the ACE sends to its peer during the handshake process. A certificate chain is a hierarchical list of certificates that includes the subject's certificate, the root CA certificate, and any intermediate CA certificates. You include a chain group in the handshake process by configuring the SSL proxy-service with the chain group (see the **(config) ssl-proxy service** command).

The ACE supports the following certificate chain group capabilities:

- A chain group can contain up to eight certificate chains.
- Each context on the ACE can contain up to eight chain groups.
- The maximum size of a chain group is 16 KB.

Examples

To create the chain group MYCHAINGROUP, enter:

```
host1/Admin(config)# crypto chaingroup MYCHAINGROUP
```

Related Commands

(config) ssl-proxy service

(config-chaingroup) cert

To add certificate files to a chain group, use the **cert** command. Use the **no** form of the command to remove a certificate file from a chain group.

cert *cert_filename*

no cert *cert_filename*

Syntax Description

cert_filename	Name of an existing certificate file stored on the ACE. Enter an unquoted text string with no spaces and a maximum of 40 alphanumeric characters. To display a list of available certificate files, use the **do show crypto files** command.

Command Modes

Chaingroup configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

It is not necessary to add the certificates in any type of hierarchical order because the device verifying the certificates determines the correct order.

The ACE supports the following certificate chain group capabilities:

- A chain group can contain up to eight certificate chains.
- Each context on the ACE can contain up to eight chain groups.
- The maximum size of a chain group is 16 KB.

Examples

To add the certificate files MYCERTS.PEM, MYCERTS_2.PEM, and MYCERTS_3.PEM to the chain group, enter:

```
host1/Admin(config-chaingroup)# cert MYCERTS.PEM
host1/Admin(config-chaingroup)# cert MYCERTS_2.PEM
host1/Admin(config-chaingroup)# cert MYCERTS_3.PEM
```

To remove the certificate file MYCERTS_2.PEM from the chain group, enter:

```
host1/Admin(config-chaingroup)# no cert MYCERTS_2.PEM
```

Related Commands

(config) crypto chaingroup

Class Map Configuration Mode Commands

Class-map configuration mode commands allow you to create and configure a Layer 3 and Layer 4 class map to classify network traffic that passes through the ACE. To create a Layer 3 and Layer 4 class map and access class map configuration mode, use the **class-map** command. The prompt changes to (config-cmap). Use the **no** form of this command to remove a Layer 3 and Layer 4 class map from the ACE.

class-map [**match-all** | **match-any**] *map_name*

no class-map [**match-all** | **match-any**] *map_name*

Syntax Description

match-all | **match-any**	(Optional) Determines how the ACE evaluates Layer 3 and Layer 4 network traffic when multiple match criteria exist in a class map. The class map is considered a match if the **match** commands meet one of the following conditions: • **match-all**—(Default) All of the match criteria listed in the class map are satisfied to match the network traffic class in the class map, typically, **match** commands of different types. • **match-any**—Only one of the match criteria listed in the class map is satisfied to match the network traffic class in the class map, typically, **match** commands of the same type.
map_name	Name assigned to the Layer 3 and Layer 4 class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The features required in your user role to execute a specific class map configuration command is described in the "Usage Guidelines" section of the command. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The ACE supports a system-wide maximum of 8192 class maps.

Examples

To create a Layer 3 and Layer 4 class map named L4VIP_CLASS to identify the network traffic that can pass through the ACE for server load balancing, enter:

```
host1/Admin(config)# class-map match-all L4VIP_CLASS
host1/Admin(config-cmap)#
```

Related Commands (config) policy-map

(config-cmap) description

To provide a brief summary about a Layer 3 and Layer 4 class map, use the **description** command. Use the **no** form of this command to remove the Layer 3 and Layer 4 class map description from the class map.

description *text*

no description

Syntax Description

text	Description about a Layer 3 and Layer 4 class map. Enter a description as an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Class map configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To add a description that the class map is to filter network traffic based on the source IP address, enter:

```
host1/Admin(config)# class-map L4_SOURCE_IP_CLASS
host1/Admin(config-cmap)# description match on source IP address of incoming traffic
```

Related Commands

This command has no related commands.

(config-cmap) match access-list

To configure the Layer 3 and Layer 4 class map to filter network traffic using a predefined access control list, use the **match access-list** command. When a packet matches an entry in an access list, and if it is a **permit** entry, the ACE allows the matching result. If it is a **deny** entry, the ACE blocks the matching result. Use the **no** form of this command to clear the access control list match criteria from the class map.

[*line_number*] **match access-list** *name*

no [*line_number*] **match access-list** *name*

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 255 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
name	Previously created access list identifier. Enter an unquoted text string with a maximum of 64 alphanumeric characters.

Command Modes

Class map configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

A single class map can have multiple **match access-list** commands. You can combine multiple **match access-list**, **match source-address**, **match destination-address**, and **match port** commands in a class map.

See the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide* for details about the creating access control lists in the ACE.

Examples

To specify that the class map is to match on the access control list INBOUND, enter:

```
host1/Admin(config)# class-map match-any L4_FILTERTRAFFIC_CLASS
host1/Admin(config-cmap)# match access-list INBOUND
```

Related Commands

(config-cmap) description

(config-cmap) match any

To instruct the ACE to perform a match on any network traffic that passes through the device, use the **match any** command. Use the **no** form of this command to remove the match any criteria from the class map.

[*line_number*] **match any**

no [*line_number*] **match any**

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 255 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.

Command Modes

Class map configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can include only one **match any** command within a class map, and you cannot combine the **match any** command with other types of **match** commands in a class map because the match criteria will be ignored.

Examples

To specify that the class map is to match on any network traffic, enter:

```
host1/Admin(config)# class-map match-any L4_MATCHANYTRAFFIC_CLASS
host1/Admin(config-cmap)# match any
```

Related Commands

(config-cmap) description

(config-cmap) match destination-address

To specify the destination IP address and subnet mask as the network traffic matching criteria, use the **match destination-address** command. Use the **no** form of this command to clear the destination IP address and subnet mask match criteria from the class map.

[*line_number*] **match destination-address** *ip_address* [*mask*]

no [*line_number*] **match destination-address** *ip_address* [*mask*]

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 255 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
ip_address	Destination IP address. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
mask	(Optional) Subnet mask entry in dotted-decimal notation (for example, 255.255.255.0).

Command Modes

Class map configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

A single class map can have multiple **match destination-address** commands. You can combine multiple **match destination-address**, **match access-list**, **match source-address**, and **match port** commands in a class map.

An entry of 0.0.0.0 0.0.0.0 indicates a wildcard match for any destination IP address and subnet mask.

Examples

To specify that the class map is to match on the destination IP address 172.16.20.1 255.255.0.0, enter:

```
host1/Admin(config)# class-map L4_DEST_IP_CLASS
host1/Admin(config-cmap)# match destination-address 172.16.20.1 255.255.0.0
```

Related Commands

(config-cmap) description

(config-cmap) match port

To specify a TCP or UDP port number or port range as the network traffic matching criteria, use the **match port** command. Use the **no** form of this command to clear the TCP or UDP port number match criteria from the class map.

[*line_number*] **match port** {**tcp** | **udp**} {**any** | **eq** {*port_number*} | **range** *port1 port2*}

no [*line_number*] **match port** {**tcp** | **udp**} {**any** | **eq** {*port_number*} | **range** *port1 port2*}

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 255 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
tcp | **udp**	Specifies the protocol: TCP or UDP.
any	Specifies that any TCP or UDP port number can match the specified value.

eq *port_number*	Specifies that the TCP or UDP port number must match the specified value. Enter an integer from 0 to 65535. A value of 0 instructs the ACE to include all ports. Alternatively, you can enter the name of a well-known TCP or UDP port as follows: • TCP port—Specify one of the following names or well-known port numbers: – **domain**—Specifies the Domain Name Service (53) – **ftp**—Specifies the File Transfer Protocol (21) – **ftp-data**—Specifies the File Transfer Protocol Data (20) – **http**—Specifies the Hypertext Transfer Protocol (80) – **https**—Specifies the HTTP over SSL protocol (443) – **irc**—Specifies the Internet Relay Chat protocol (194) – **matip-a**—Specifies the Matip Type A protocol (350) – **nntp**—Specifies the Network News Transport Protocol (119) – **pop2**—Specifies the Post Office Protocol v2 (109) – **pop3**—Specifies the Post Office Protocol v3 (110) – **rtsp**—Specifies the Real Time Streaming Protocol (554) – **sip**—Specifies the Session Initiation Protocol (5060) – **skinny**—Specifies the Cisco Skinny Client Protocol (2000) – **smtp**—Specifies the Simple Mail Transfer Protocol (25) – **sunrpc**—Specifies the Sun Remote Procedure Call (111) – **telnet**—Specifies the Telnet protocol (23) – **www**—Specifies the World Wide Web (80) – **xot**—Specifies X25 over TCP (1998) • UDP port—Specify one of the following protocols: – **domain**—Specifies the Domain Name Service (53) – **sip**—Specifies the Session Initiation Protocol (5060) – **wsp**—Specifies the Connectionless Wireless Session Protocol (9200) – **wsp-wtls**—Specifies the Secure Connectionless WSP (9202) – **wsp-wtp**—Specifies the Connection-based WSP (9201) – **wsp-wtp-wtls**—Specifies the Secure Connection-based WSP (9203)
range *port1 port2*	Specifies a port range to use for the TCP or UDP port. Valid port ranges are from 0 to 65535. A value of 0 (for *port1*and *port2*) instructs the ACE to match all ports.

Command Modes

Class map configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

A single class map can have multiple **match port** commands. You can combine multiple **match port**, **match access-list**, **match source-address**, and **match destination-address** commands in a class map.

Examples

To specify that the class map is to match on TCP port number 23 (Telnet client), enter:

```
host1/Admin(config)# class-map L4_TCPPORT_CLASS
host1/Admin(config-cmap)# match port tcp eq 23
```

Related Commands

(config-cmap) description

(config-cmap) match source-address

To specify a client source host IP address and subnet mask from which the ACE accepts traffic as the network traffic matching criteria, use the **match source-address** command. You configure the associated policy map to permit or restrict management traffic to the ACE from the specified source network or host. Use the **no** form of this command to clear the source IP address and subnet mask match criteria from the class map.

[*line_number*] **match source-address** *ip_address mask*

no [*line_number*] **match source-address** *ip_address mask*

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 255 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
ip_address	Source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
mask	Subnet mask of the client entry in dotted-decimal notation (for example, 255.255.255.0).

Command Modes

Class map configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

A single class map can have multiple **match source-address** commands. You can combine multiple **match source-address**, **match access-list**, **match destination-address**, and **match port** commands in a class map.

An entry of 0.0.0.0 0.0.0.0 indicates a wildcard match for any source IP address and subnet mask.

Examples

To specify that the class map match on the source IP address 192.168.11.2 255.255.255.0, enter:

```
host1/Admin(config)# class-map type http loadbalance match-any L7SLBCLASS
host1/Admin(config-cmap-http-lb)# match source-address 192.168.11.2 255.255.255.0
```

Related Commands

(config-cmap) description

(config-cmap) match virtual-address

To define a 3-tuple flow of the virtual IP (VIP) address, protocol, and port as matching criteria for server load balancing, use the **match virtual-address** command. You can configure multiple match criteria statements to define the VIPs for server load balancing. Use the **no** form of this command to remove the VIP match statement from the class map.

[*line_number*] **match virtual-address** *vip_address* {[*netmask*] *protocol_number* | **any** | {**tcp** | **udp** {**any** | **eq** *port_number* | **range** *port1 port2*}}}

no [*line_number*] **match virtual-address** *vip_address* {[*netmask*] *protocol_number* | **any** | {**tcp** | **udp** {**any** | **eq** *port_number* | **range** *port1 port2*}}}

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 255 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
vip_address	VIP server IP address of the ACE, specified in dotted-decimal format (for example, 192.168.1.2).
netmask	(Optional) Subnet mask for the VIP address, specified in dotted-decimal format (for example, 255.255.255.0).
protocol_number	(Optional) Number of an IP protocol. Enter an integer from 1 to 255 that represents the IP protocol number.
any	Specifies the wildcard value that allows connections from any IP protocol.
tcp | **udp**	Specifies the protocol: TCP or UDP.
any	Specifies the wildcard value for the TCP or UDP port number. With **any** used in place of either the **eq** or **range** values, packets from any incoming port match.

eq *port_number*	Specifies that the TCP or UDP port number must match the specified value. Enter an integer from 0 to 65535. A value of 0 instructs the ACE to include all ports. Alternatively, you can enter the name of a well-known TCP port or a well-known UDP port as follows: • TCP port—Specify one of the following names or well-known port numbers: – **domain**—Specifies the Domain Name Service (53) – **ftp**—Specifies the File Transfer Protocol (21) – **ftp-data**—Specifies the File Transfer Protocol Data (20) – **http**—Specifies the Hypertext Transfer Protocol (80) – **https**—Specifies the HTTP over SSL protocol (443) – **irc**—Specifies the Internet Relay Chat protocol (194) – **matip-a**—Specifies the Matip Type A protocol (350) – **nntp**—Specifies the Network News Transport Protocol (119) – **pop2**—Specifies the Post Office Protocol v2 (109) – **pop3**—Specifies the Post Office Protocol v3 (110) – **rdp**—Specifies the Remote Desktop Protocol (3389) – **rtsp**—Specifies the Real-Time Streaming Protocol (554) – **sip**—Specifies the Session Initiation Protocol (5060) – **skinny**—Specifies the Skinny Client Control protocol (2000) – **smtp**—Specifies the Simple Mail Transfer Protocol (25) – **telnet**—Specifies the Telnet protocol (23) – **www**—Specifies the World Wide Web (80) – **xot**—Specifies X25 over TCP (1998) • UDP port—Specify one of the following protocols: – **domain**—Specifies the Domain Name Service (53) – **radius-acct**—Specifies the Remote Authentication Dial-In User Service (accounting) (1813) – **radius-auth**—Specifies the Remote Authentication Dial--In User Service (server) (1812) – **sip**—Specifies the Session Initiation Protocol (5060) – **wsp**—Specifies the Connectionless Wireless Session Protocol (9200) – **wsp-wtls**—Specifies the Secure Connectionless WSP (9202) – **wsp-wtp**—Specifies the Connection-based WSP (9201) – **wsp-wtp-wtls**—Specifies the Secure Connection-based WSP (9203)

range *port1 port2*	Specifies a port range to use for the TCP or UDP port. Valid port ranges are from 0 to 65535. A value of 0 (for *port1* and *port2*) instructs the ACE to match all ports.

Command Modes

Class map configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised.
A3(2.2)	The ACE no longer allows the configuration of a class-map VIP address that overlaps with an ACE interface IP address.

Usage Guidelines

This command requires the VIP feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can specify multiple **match virtual-address** commands within a class map.

The **match virtual-address** command cannot be combined with other types of **match** commands.

For KAL-AP, the ACE verifies whether the VIP addresses are active in all Layer 3 class maps that are configured with the addresses. It ignores all other protocol-specific information for the VIP addresses.

See the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide* for details about configuring the ACE to perform server load balancing.

Examples

To specify that the class map L4VIPCLASS matches traffic destined to VIP address 192.168.1.10 and TCP port number 80, enter:

```
host1/Admin(config)# class-map L4VIPCLASS
host1/Admin(config-cmap)# match virtual-address 192.168.1.10 tcp port eq 80
```

Related Commands

(config-cmap) description

Class Map FTP Inspection Configuration Mode Commands

Class map File Transfer Protocol (FTP) inspection configuration mode commands allow you to create and configure a Layer 7 class map to be used for the inspection of FTP request commands. To create this class map and access class map FTP inspection configuration mode, use the **class-map type ftp inspect** command. The prompt changes to (config-cmap-ftp-insp). Use the **no** form of this command to remove the class map from the ACE.

class-map type ftp inspect match-any *map_name*

no class-map type ftp inspect match-any *map_name*

Syntax Description

match-any	Determines how the ACE inspects FTP request commands when multiple match criteria exist in a class map. The FTP request commands being inspected must match only one of the match criteria listed in the class map.
map_name	Name assigned to the Layer 7 FTP command request class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the inspect feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To create a Layer 7 class map named FTP_INSPECT_L7CLASS that performs FTP command inspection, enter:

```
host1/Admin(config)# class-map type ftp inspect match-any FTP_INSPECT_L7CLASS
host1/Admin(config-cmap-ftp-insp)#
```

Related Commands

(config) policy-map

(config-cmap-ftp-insp) description

To provide a brief summary about the Layer 7 File Transfer Protocol (FTP) command inspection class map, use the **description** command. Use the **no** form of this command to remove the description from the class map.

description *text*

no description *text*

Syntax Description

text	Description about the class map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Class map FTP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description that the class map is to perform FTP command inspection, enter:

```
host1/Admin(config-cmap-ftp-insp)# description FTP command inspection of incoming traffic
```

To remove a description from the FTP class map, enter:

```
host1/Admin(config-cmap-ftp-insp)# no description FTP command inspection of incoming
traffic
```

Related Commands

This command has no related commands.

(config-cmap-ftp-insp) match request-method

To define File Transfer Protocol (FTP) command inspection decisions by the ACE, use the **match request-method** command. The **match** command identifies the FTP commands that you want filtered by the ACE. Use the **no** form of this command to clear the FTP inspection request method from the class map.

[*line_number*] **match request-method** *ftp_command*

no [*line_number*] **match request-method** *ftp_command*

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
ftp_command	FTP command in the class map to be subjected to FTP inspection by the ACE. The possible FTP commands are as follows: • **appe**—Append to a file. • **cd**—Change to the specified directory. • **cdup**—Change to the parent of the current directory. • **dele**—Delete a file at the server side. • **get**—Retrieve a file. • **help**—Help information from the server. • **mkd**—Create a directory. • **put**—Store a file. • **rmd**—Remove a directory. • **rnfr**—Rename from. • **rnto**—Rename to. • **site**—Specify the server-specific command. • **stou**—Store a file with a unique name. • **syst**—Get system information.

Command Modes

Class map FTP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You can specify multiple **match request-method** commands within a class map.

Examples

To specify FTP_INSPECT_L7CLASS as the name of a class map and identify that at least one FTP inspection command in the class map must be satisfied for the ACE to indicate a match, enter:

```
(config)# class-map type ftp inspect match-any FTP_INSPECT_L7CLASS
host1/Admin(config-cmap-ftp-insp)# match request-method cdup
host1/Admin(config-cmap-ftp-insp)# match request-method get
host1/Admin(config-cmap-ftp-insp)# match request-method stou
host1/Admin(config-cmap-ftp-insp)# match request-method put
```

Related Commands

(config-cmap-ftp-insp) description

Class Map Generic Configuration Mode Commands

Generic TCP and UDP data parsing allows you to perform regular expression (regex) matches on packets from protocols that the ACE does not explicitly support. Such regex matches can be based on a custom protocol configuration. To accomplish this task, you create a Layer 7 class map for generic TCP or UDP data parsing and then instruct the ACE to perform a policy-map action based on the payload of a TCP stream or UDP packet.

To create a class map for generic TCP or UDP data parsing and access class map generic configuration mode, use the **class-map type generic** command in configuration mode. Use the **no** form of this command to remove a generic class map from the ACE.

class-map type generic {**match-all** | **match-any**} *map_name*

no class-map type generic {**match-all** | **match-any**} *map_name*

Syntax Description

match-all | **match-any**	Determines how the ACE evaluates Layer 3 and Layer 4 network traffic when multiple match criteria exist in a class map. • **match-all**—Network traffic needs to satisfy all of the match criteria (implicit AND) to match the class map. • **match-any**—Network traffic needs to satisfy only one of the match criteria (implicit OR) to match the class map.
map_name	Name assigned to the Layer 7 class map for generic TCP and UDP data parsing. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To create a class map named GENERIC_L7_CLASS, enter:

```
host1/Admin(config)# class-map type generic match-any GENERIC_L7_CLASS
host1/Admin(config-cmap-generic)#
```

To remove the class map from the configuration, enter:

```
host1/Admin(config)# no class-map type generic match-any GENERIC_L7_CLASS
```

Related Commands

(config) class-map

(config-cmap-generic) description

To provide a brief description of the Layer 7 class map for generic TCP and UDP data parsing, use the **description** command. Use the **no** form of this command to remove the description from the class map.

description *text*

no description

Syntax Description

text	Description of the class map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Class map generic configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description for the generic class map, enter:

```
host1/Admin(config-cmap-generic)# description GENERIC TCP UDP CLASS MAP
```

To remove a description from a generic class map, enter:

```
host1/Admin(config-cmap-generic)# no description
```

Related Commands

This command has no related commands.

(config-cmap-generic) match class-map

To identify one Layer 7 generic class map as a matching criterion for another Layer 7 generic class map, use the **match class-map** command. Use the **no** form of this command to remove the nested class map from the generic class map.

[*line_number*] **match class-map** *name*

no [*line_number*] **match class-map** *name*

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. For example, you can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate any priority for the match statements. Enter a unique integer from 2 to 1024.
name	Name of an existing Layer 7 generic class map.

Command Modes

Class map generic configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The **match class-map** command allows you to combine the use of the **match-any** and **match-all** keywords in the same class map. To combine **match-all** and **match-any** characteristics in a class map, create a class map that uses one **match** command (either **match-any** or **match-all**) and then use this class map as a match statement in a second class map that uses a different match type.

The ACE restricts the nesting of class maps to two levels to prevent you from including a nested class map under another class map. The nesting of class maps allows you to achieve complex logical expressions for Layer 7 server load balancing.

Examples

To combine the characteristics of two class maps, one with **match-any** and one with **match-all** characteristics, into a single class map, enter:

```
(config)# class-map type generic match-all GENERIC_CLASS3
(config-cmap-generic)# 100 match layer4-payload offset 500 regex abc123.*
(config-cmap-generic)# exit

(config)# class-map type generic match-any GENERIC_CLASS4
(config-cmap-generic)# 10 match class-map GENERIC_CLASS3
(config-cmap-generic)# 20 match source-address 192.168.11.2
(config-cmap-generic)# 30 match source-address 192.168.11.3
(config-cmap-generic)# exit
```

Related Commands

(config-cmap-generic) description

(config-cmap-generic) match layer4-payload

To define match criteria for Layer 4 payloads, use the **match layer4-payload** command in class map generic configuration mode. Use the **no** form of this command to remove the Layer 4 payload match criteria from the class map.

[*line_number*] **match layer4-payload** [**offset** *number*] **regex** *expression*

no [*line_number*] **match layer4-payload** [**offset** *number*] **regex** *expression*

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. For example, you can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate any priority for the match statements. Enter a unique integer from 2 to 1024.
offset *number*	(Optional) Specifies an absolute offset in the data where the Layer 4 payload expression search string starts. The offset starts at the first byte of the TCP or UDP body. Enter an integer from 0 to 999. The default is 0.
regex *expression*	Specifies the Layer 4 payload expression that is contained within the TCP or UDP entity body. The range is from 1 to 255 alphanumeric characters. For a list of the supported characters that you can use in regular expression strings, see Table 2-5.

Command Modes

Class map generic configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

You cannot configure more than one **match layer4-payload** command in the same **match-all** class map.

Generic data parsing begins at Layer 4 with the TCP or UDP payload, which allows you the flexibility to match Layer 5 data (in the case of LDAP or DNS) or any Layer 7 header or payload (for example, HTTP).

Table 2-5 Characters Supported in Regular Expressions

Convention	Description
.*	Zero or more characters.
.	Exactly one character.
\ .	Escaped character.
\xhh	Any ASCII character as specified in two-digit hex notation.
()	Expression grouping.
Bracketed range [for example, 0-9]	Matches any single character from the range.
A leading ^ in a range [^charset]	Does not match any character in the range; all other characters represent themselves.
(expr1 | expr2)	OR of expressions.
(expr)*	0 or more of expressions.
(expr)+	1 or more of expressions.
(expr{m,n}	Matches the previous item between *m* and *n* times; valid entries are from 1 to 255.
(expr{m}	Matches the previous item exactly *m* times; valid entries are from 1 to 255.
(expr{m,}	Matches the previous item *m* or more times; valid entries are from 1 to 255.
\a	Alert (ASCII 7).
\b	Backspace (ASCII 8).
\f	Form-feed (ASCII 12).
\n	New line (ASCII 10).
\r	Carriage return (ASCII 13).
\t	Tab (ASCII 9).
\v	Vertical tab (ASCII 11).
\0	Null (ASCII 0).
.\\	Backslash.

Examples

To configure match criteria for generic Layer 4 data parsing, enter:

```
host1/Admin(config)# class-map type generic match-any GENERIC_L4_CLASS
host1/Admin(config-cmap-generic)# 10 match layer4-payload offset 500 regex abc123.*
```

To remove the match statement from the class map, enter:

```
host1/Admin(config-cmap-generic)# no 10
```

Related Commands

(config-cmap-generic) description

(config-cmap-generic) match source-address

To configure the generic class map to filter traffic based on a client source IP address, use the **match source-address** command. Use the **no** form of this command to remove the source IP address match statement from the class map.

[*line_number*] **match source-address** *ip_address* [*netmask*]

no [*line_number*] **match source-address** *ip_address* [*netmask*]

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. For example, you can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate any priority for the match statements. Enter a unique integer from 2 to 1024.
ip_address	Source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.2).
netmask	(Optional) Subnet mask of the IP address. Enter the netmask in dotted-decimal notation (for example, 255.255.255.0). The default is 255.255.255.255.

Command Modes

Class map generic configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

You cannot configure more than one **match source-address** command in the same **match-all** class map.

Examples

To specify that the class map match on source IP address 192.168.11.2 255.255.255.0, enter:

```
host1/Admin(config)#  class-map type generic match-any GENERIC_L7_CLASS
host1/Admin(config-cmap-generic)# 50 match source-address 192.168.11.2 255.255.255.0
```

To remove the source IP address match statement from the class map, enter:

```
host1/Admin(config-cmap-generic)# no 50
```

Related Commands

(config-cmap-generic) description

Class Map HTTP Inspection Configuration Mode Commands

Class map HTTP inspection configuration mode commands allow you to create a Layer 7 HTTP deep packet inspection class map. To create this class map and access class map HTTP inspection configuration mode, use the **class-map type http inspect** command. The prompt changes to (config-cmap-http-insp). Use the **no** form of this command to remove an HTTP deep packet inspection class map from the ACE.

class-map type http inspect [**match-all | match-any**] *map_name*

no class-map type http inspect [**match-all | match-any**] *map_name*

Syntax Description

match-all | match-any	(Optional) Determines how the ACE performs the deep packet inspection of HTTP traffic when multiple match criteria exist in a class map. The class map is considered a match if the match commands meet one of the following conditions: • **match-all** —(Default) Specifies that network traffic needs to satisfy all of the match criteria (implicit AND) to match the Layer 7 HTTP deep packet inspection class map. The **match-all** keyword is applicable only for match statements of different HTTP deep packet inspection types. For example, specifying a **match-all** condition for URL, HTTP header, and URL content statements in the same class map is valid. However, specifying a **match-all** condition for multiple HTTP headers with the same names or multiple URLs in the same class map is invalid. • **match-any**—Network traffic needs to satisfy only one of the match criteria (implicit OR) to match the Layer 7 HTTP deep packet inspection class map. The **match-any** keyword is applicable for match statements of different Layer 7 HTTP deep packet inspection type or multiple instances of the same type with different names. For example, the ACE allows you to specify a **match-any** condition for cookie, HTTP header, and URL content statements in the same class map, but it does not allow you to specify a **match-any** condition for URL length, HTTP header length, and content length statements in the same class map.
map_name	Name assigned to the Layer 7 HTTP deep packet inspection class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines The commands in this mode require the inspect feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples To create a Layer 7 class map named HTTP_INSPECT_L7CLASS that performs HTTP deep packet inspection, enter:

```
(config)# class-map type http inspect match-any HTTP_INSPECT_L7CLASS
host1/Admin(config-cmap-http-insp)#
```

Related Commands **(config) policy-map**

(config-cmap-http-insp) description

To provide a brief summary about the Layer 7 HTTP inspection class map, use the **description** command. Use the **no** form of this command to remove the description from the class map.

description *text*

no description

Syntax Description

text	Description about the class map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes Class map HTTP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines This command has no usage guidelines.

Examples To add a description that the class map is to perform HTTP deep packet inspection, enter:

```
host1/Admin(config-cmap-http-insp)# description HTTP protocol deep inspection of incoming
traffic
```

Related Commands This command has no related commands.

(config-cmap-http-insp) match content

To define HTTP application inspection decisions based on content expressions contained within the HTTP entity body, use the **match content** command. Use the **no** form of this command to clear content expression checking match criteria from the class map.

[*line_number*] **match content** *expression* [**offset** *number*]

no [*line_number*] **match content** *expression* [**offset** *number*]

Syntax Description

[*line_number*]	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
expression	Content expression contained within the HTTP entity body. The range is from 2 to 1024 alphanumeric characters. For a list of the supported characters that you can use in regular expressions, see Table 2-5.
offset *number*	(Optional) Provides an absolute offset where the content expression search string starts. The offset starts at the first byte of the message body, after the empty line (CR, LF, CR, LF) between the headers and the body of the message. The offset value is from 1 to 4000 bytes.

Command Modes

Class map HTTP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To specify a content expression contained within the entity body sent with an HTTP request, enter:

```
(config)# class-map type http inspect match-any HTTP_INSPECT_L7CLASS
host1/Admin(config-cmap-http-insp)# match content .*newp2psig
```

Related Commands

(config-cmap-http-insp) description

(config-cmap-http-insp) match content length

To configure the class map to define application inspection decisions on HTTP traffic up to the configured maximum content parse length, use the **match content length** command. Messages that meet the specified criteria will be either allowed or denied based on the Layer 7 HTTP deep packet inspection policy map action. Use the **no** form of this command to clear the HTTP content length match criteria from the class map.

[*line_number*] **match content length** {**eq** *bytes* | **gt** *bytes* | **lt** *bytes* | **range** *bytes1 bytes 2*}

no [*line_number*] **match content length** {**eq** *bytes* | **gt** *bytes* | **lt** *bytes* | **range** *bytes1 bytes 2*}

Syntax Description

[*line_number*]	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
eq *bytes*	Specifies a value for the content parse length in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with a content length size equal to the specified value. Valid entries are from 1 to 65535 bytes.
gt *bytes*	Specifies a minimum value for the content parse length in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with a content length size greater than the specified value. Valid entries are from 1 to 65535 bytes.
lt *bytes*	Specifies a maximum value for the content parse length in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with a content length size less than the specified value. Valid entries are from 1 to 65535 bytes.
range *bytes1 bytes*	Specifies a size range for the content parse length in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with a content length size within this range. The range is from 1 to 65535 bytes.

Command Modes

Class map HTTP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To identify content parse length in an HTTP message that can be received by the ACE, enter:

```
(config)# class-map type http inspect match-any HTTP_INSPECT_L7CLASS
host1/Admin(config-cmap-http-insp)# match content length eq 3495
```

Related Commands

(config-cmap-http-insp) description

(config-cmap-http-insp) match cookie secondary

To configure a class map to define HTTP inspection decisions based on the name or prefix and value of a secondary cookie (URL query string), use the **match cookie secondary** command. Use the **no** form of this command to clear secondary cookie match criteria from the class map.

[*line_number*] **match cookie secondary** [**name** *cookie_name* | **prefix** *prefix_name*] **value** *expression*

no [*line_number*] **match cookie secondary** [**name** *cookie_name* | **prefix** *prefix_name*] **value** *expression*

Syntax Description

[*line_number*]	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
name *cookie_name*	Identifier of the secondary cookie to match. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
prefix *prefix_name*	Prefix of the secondary cookie to match. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
value *expression*	Regular expression of the secondary cookie to match. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters.

Command Modes

Class map HTTP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The following configuration guidelines apply when you configure a secondary cookie match statement for HTTP inspection:

- Ensure that secondary cookie names do not overlap with other secondary cookie names in the same match-all class map. For example, the following configuration is not allowed because the two match statements have overlapping cookie names:

```
(config)#  class-map type http inspect match-any HTTP_INSPECT_L7CLASS
host1/Admin(config-cmap-http-insp)# match cookie secondary prefix id value .*
host1/Admin(config-cmap-http-insp)# match cookie secondary name identity value bob
```

- When you configure a secondary cookie value match across all secondary cookie names in a match-all class map, you cannot configure any other secondary cookie match in the same class map. That is because a secondary cookie match on value alone is equivalent to a wildcard match on name. In the following example, the second match statement is not allowed:

```
(config)#  class-map type http inspect match-any HTTP_INSPECT_L7CLASS
host1/Admin(config-cmap-http-insp)# match cookie secondary value bob
host1/Admin(config-cmap-http-insp)# match cookie secondary name identity value jane
```

Examples

To match a secondary cookie called “matchme” with a regular expression value of .*abc123, enter the following commands:

```
(config)#  class-map type http inspect match-any HTTP_INSPECT_L7CLASS
host1/Admin(config-cmap-http-insp)# match cookie secondary name matchme value .*abc123
```

Related Commands

(config-pmap-ins-http) match cookie secondary

(config-cmap-http-insp) match header

To configure the class map to define application inspection decisions based on the name and value in an HTTP header, use the **match header** command. The ACE performs regular expression matching against the received packet data from a particular connection based on the HTTP header expression. Use the **no** form of this command to clear an HTTP header match criteria from the class map.

[*line_number*] **match header** {*header_name* | *header_field*} **header-value** *expression*

no [*line_number*] **match header** {*header_name* | *header_field*} **header-value** *expression*

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
header_name	Name of the HTTP header to match (for example, www.example1.com.) The range is from 1 to 64 alphanumeric characters. **Note** The *header_name* argument cannot include the colon in the name of the HTTP header; the ACE rejects the colon as an invalid token.

header_field	Standard HTTP/1.1 header field. Valid selections include request-header fields, general-header fields, and entity-header fields. Selections also include two lower-level header-matching commands: "length" and "mime-type." The supported selections are as follows: • **Accept**—Semicolon-separated list of representation schemes (content type metainformation values) that will be accepted in the response to the request. • **Accept-Charset**—Character sets that are acceptable for the response. This field allows clients capable of understanding more comprehensive or special-purpose character sets to signal that capability to a server that can represent documents in those character sets. • **Accept-Encoding**—Restricts the content encoding that a user will accept from the server. • **Accept-Language**—ISO code for the language in which the document is written. The language code is an ISO 3316 language code with an optional ISO639 country code to specify a national variant. • **Authorization**—Specifies that the user agent wants to authenticate itself with a server, usually after receiving a 401 response. • **Cache-Control**—Directives that must be obeyed by all caching mechanisms along the request/response chain. The directives specify behavior intended to prevent caches from adversely interfering with the request or response. • **Connection**—Allows the sender to specify connection options. • **Content-MD5**—MD5 digest of the entity body that provides an end-to-end integrity check. Only a client or an origin server can generate this header field. • **Expect**—Used by a client to inform the server about the behaviors that the client requires. • **From**—Contains the e-mail address of the person that controls the requesting user agent. • **Host**—Internet host and port number of the resource being requested, as obtained from the original URL given by the user or referring resource. The Host field value must represent the naming authority of the origin server or gateway given by the original URL.

	• **If-Match**—Used with a method to make it conditional. A client that has one or more entities previously obtained from the resource can verify that one of those entities is current by including a list of their associated entity tags in the If-Match header field. This feature allows efficient updates of cached information with a minimum amount of transaction overhead. It is also used on updating requests to prevent inadvertent modification of the wrong version of a resource. As a special case, the value "*" matches any current entity of the resource. • **length**—See the **(config-cmap-http-insp) match header length** command. • **mime-type**—See the **(config-cmap-http-insp) match header mime-type** command. • **Pragma**—Pragma directives that are understood by servers to whom the directives are relevant. The syntax is the same as for other multiple-value fields in HTTP. For example, the accept field is a comma-separated list of entries for which the optional parameters are separated by semicolons. • **Referer**—Address (URI) of the resource from which the URI in the request was obtained. • **Transfer-Encoding**—Indicates what (if any) type of transformation has been applied to the message body in order to safely transfer it between the sender and the recipient. • **User-Agent**—Information about the user agent (for example, a software program that originates the request). This information is for statistical purposes, the tracing of protocol violations, and automated recognition of user agents. • **Via**—Used by gateways and proxies to indicate the intermediate protocols and recipients between the user agent and the server on requests and between the origin server and the client on responses.
header-value *expression*	Specifies the header value expression string to compare against the value in the specified field in the HTTP header. The range is from 1 to 255 alphanumeric characters. Table 2-5 lists the supported characters that you can use in regular expressions.

Command Modes

Class map HTTP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The ACE supports the use of regular expressions for matching. Expressions are stored in a header map in the form *header-name: expression*. Header expressions allow spaces, provided that the spaces are escaped or quoted. Table 2-5 lists the supported characters that you can use in regular expressions.

Examples

To filter on content and allow HTTP headers that contain the expression *html*, enter:

```
host1/Admin(config)# class-map type http inspect match-all L7_CLASSFLTRHTML1
host1/Admin(config-cmap-http-insp)# match header accept header-value html
```

Related Commands

(config-cmap-http-insp) description

(config-cmap-http-insp) match header length

To limit the HTTP traffic allowed through the ACE based on the length of the entity body in the HTTP message, use the **match header length** command. Messages will be either allowed or denied based on the Layer 7 HTTP deep packet inspection policy map action. Use the **no** form of this command to clear an HTTP header length match criteria from the class map.

[*line_number*] **match header length** {**request** | **response**} {**eq** *bytes* | **gt** *bytes* | **lt** *bytes* | **range** *bytes1 bytes 2*}

no [*line_number*] **match header length** {**request** | **response**} {**eq** *bytes* | **gt** *bytes* | **lt** *bytes* | **range** *bytes1 bytes 2*}

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
request	Specifies the size of the HTTP header request message that can be received by the ACE.
response	Specifies the size of the HTTP header response message sent by the ACE.
eq *bytes*	Specifies a value for the entity body in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with an entity body size equal to the specified value. Valid entries are from 1 to 65535 bytes.
gt *bytes*	Specifies a minimum value for the entity body in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with an entity body size greater than the specified value. Valid entries are from 1 to 65535 bytes.

lt *bytes*	Specifies a maximum value for the entity body in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with an entity body size less than the specified value. Valid entries are from 1 to 65535 bytes.
range *bytes1 bytes 2*	Specifies a size range for the entity body in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with a entity body size within this range. The range is from 1 to 65535 bytes.

Command Modes

Class map HTTP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

By default, the maximum header length for HTTP deep packet inspection is 2048 bytes.

Examples

To specify that the class map match on HTTP traffic received with a length less than or equal to 3600 bytes in the entity body of the HTTP message, enter:

```
(config)# class-map type http inspect HTTP_INSPECT_L7CLASS
host1/Admin(config-cmap-http-insp)# match header length request eq 3600
```

Related Commands

This command has no related commands.

(config-cmap-http-insp) match header mime-type

To specify a subset of the Multipurpose Internet Mail Extension (MIME)-type messages that the ACE permits or denies based on the actions in the policy map, use the **match header mime-type** command. MIME-type validation extends the format of Internet mail to allow non-US-ASCII textual messages, non-textual messages, multipart message bodies, and non-US-ASCII information in message headers. Use the **no** form of this command to deselect the specified MIME message match criteria from the class map.

[*line_number*] **match header mime-type** *mime_type*

no [*line_number*] **match header mime-type** *mime_type*

Syntax Description

[*line_number*]	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
mime_type	MIME-type message. The ACE includes a predefined list of mime-types, such as image\Jpeg, text\html, application\msword, audio\mpeg. Choose whether only the mime-types included in this list are permitted through the ACE firewall or whether all mime-types are acceptable. The default behavior is to allow all mime-types. The following lists the supported mime-types: • **application\msexcel** • **application\mspowerpoint** • **application\msword** • **application\octet-stream**

- **application\pdf**
- **application\postscript**
- **application\x-gzip**
- **application\x-java-archive**
- **application\x-java-vm**
- **application\x-messenger**
- **application\zip**
- **audio***
- **audio\basic**
- **audio\midi**
- **audio\mpeg**
- **audio\x-adpcm**
- **audio\x-aiff**
- **audio\x-ogg**
- **audio\x-wav**
- **image ***
- **image\gif**
- **image\jpeg**
- **image\png**
- **image\tiff**
- **image\x-3ds**
- **image\x-bitmap**
- **image\x-niff**
- **image\x-portable-bitmap**
- **image\x-portable-greymap**
- **image\x-xpm**
- **text***
- **text\css**
- **text\html**
- **text\plain**
- **text\richtext**
- **text\sgml**
- **text\xmcd**
- **text\xml**

- **video***
- **video\flc**
- **video\mpeg**
- **video\quicktime**
- **video\sgi**
- **video\x-fli**

Command Modes

Class map HTTP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

To define MIME type messages in addition to what is supported under the **match header mime-type** command, use the **match header** command. For example, to define a match for a new MIME-type audio\myaudio, you could enter the following match statement: `match header Content-type header-value audio\myaudio`.

Examples

To specify the MIME-type audio\midi and audio\mpeg messages permitted through the ACE, enter:

```
(config)# class-map type http inspect match-any HTTP_INSPECT_L7CLASS
host1/Admin(config-cmap-http-insp)# match header mime-type audio\midi
host1/Admin(config-cmap-http-insp)# match header mime-type audio\mpeg
```

Related Commands

This command has no related commands.

(config-cmap-http-insp) match port-misuse

To configure the class map to define application inspection compliance decisions that restrict certain HTTP traffic from passing through the ACE, use the **match port-misuse** command. This class map detects the misuse of port 80 (or any other port running HTTP) for tunneling protocols such as peer-to-peer (p2p) applications, tunneling applications, and instant messaging. Use the **no** form of this command to clear the HTTP restricted application category match criteria from the class map.

[*line_number*] **match port-misuse** {**im** | **p2p** | **tunneling**}

no [*line_number*] **match port-misuse** {**im** | **p2p** | **tunneling**}

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
im	Defines the instant messaging application category. The ACE checks for the Yahoo Messenger instant messaging application.
p2p	Defines the peer-to-peer application category. The applications checked include Kazaa, GoToMyPC, and Gnutella.
tunneling	Defines the tunneling application category. The applications checked include: HTTPort/HTTHost, GNU Httptunnel, GotoMyPC, Firethru, and Http-tunnel.com Client.

Command Modes

Class map HTTP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You can specify multiple **match port-misuse** commands within a class map. Each **match port-misuse** command configures a single application type.

The port misuse application inspection process requires a search of the entity body of the HTTP message, which may degrade performance of the ACE.

The ACE disables the **match port-misuse** command by default. If you do not configure a restricted HTTP application category, the default action by the ACE is to allow the applications without generating a log.

Examples

To identify that peer-to-peer applications are restricted HTTP traffic, enter:

```
(config)# class-map type http inspect HTTP_INSPECT_L7CLASS
host1/Admin(config-cmap-http-insp)# match port-misuse p2p
```

Related Commands (config-cmap-http-insp) description

(config-cmap-http-insp) match request-method

To configure the class map to define application inspection compliance decisions based on the request methods defined in RFC 2616 and by HTTP extension methods, use the **match request-method** command. If the HTTP request method or extension method compliance checks fails, the ACE denies or resets the specified HTTP traffic based on the policy map action. Use the **no** form of this command to clear the HTTP request method match criteria from the class map.

[*line_number*] **match request-method** {**ext** *method* | **rfc** *method*}

no [*line_number*] **match request-method** {**ext** *method* | **rfc** *method*}

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
ext *method*	Specifies an HTTP extension method. If the RFC request messages does not contain one of the RFC 2616 HTTP request methods, the ACE verifies if it is an extension method. The ACE supports the inspection of the following HTTP request extension methods: **bcopy**, **bdelete**, **bmove**, **bpropfind**, **bproppatch**, **copy**, **edit**, **getattr**, **getattrname**, **getprops**, **index**, **lock**, **mkdir**, **mkcol**, **move**, **propfind**, **proppatch**, **revadd**, **revlabel**, **revlog**, **revnum**, **save**, **search**, **setattr**, **startrev**, **stoprev**, **unedit**, and **unlock**.
rfc *method*	Specifies a RFC 2616 HTTP request method that you want to perform an RFC compliance check on. The ACE supports the inspection of the following RFC 2616 HTTP request methods: **connect**, **delete**, **get**, **head**, **options**, **post**, **put**, and **trace**.

Command Modes

Class map HTTP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You can specify multiple **match request-method** commands within a class map.Each **match request-method** command configures a single request method.

For unsupported HTTP request methods, include the **inspect http strict** command as an action in the Layer 3 and Layer 4 policy map.

The ACE disables the **match request-method** command by default. If you do not configure a request method, the default action by the ACE is to allow the RFC 2616 HTTP request method without generating a log. By default, the ACE allows all request and extension methods.

Examples

To identify that the **connect**, **get**, **head**, and **index** HTTP RFC 2616 protocols are to be used for application inspection, enter:

```
(config)# class-map type http inspect match-any HTTP_INSPECT_L7CLASS
host1/Admin(config-cmap-http-insp)# match request-method rfc connect
host1/Admin(config-cmap-http-insp)# match request-method rfc get
host1/Admin(config-cmap-http-insp)# match request-method rfc head
host1/Admin(config-cmap-http-insp)# match request-method ext index
```

Related Commands

(config-cmap-http-insp) description

(config-cmap-http-insp) match transfer-encoding

To configure the class map to define application inspection decisions that limit the HTTP transfer-encoding types that can pass through the ACE, use the **match transfer-encoding** command. The transfer-encoding general-header field indicates the type of transformation, if any, that has been applied to the HTTP message body to safely transfer it between the sender and the recipient. When an HTTP request message contains the configured transfer-encoding type, the ACE performs the configured action in the policy map. Use the **no** form of this command to clear the HTTP transfer-encoding match criteria from the class map.

[*line_number*] **match transfer-encoding** {**chunked** | **compressed** | **deflate** | **gzip** | **identity**}

no [*line_number*] **match transfer-encoding** {**chunked** | **compressed** | **deflate** | **gzip** | **identity**}

Syntax Description

line_number	(Optional) Line number to assist you in editing or deleting individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
chunked	Transfers the message body as a series of chunks.
compressed	Defines the encoding format produced by the common UNIX file compression program “compress”. This format is an adaptive Lempel-Ziv-Welch coding (LZW).
deflate	Defines the .zlib format defined in RFC 1950 in combination with the deflate compression mechanism described in RFC 1951.
gzip	Defines the encoding format produced by the file compression program gzip (GNU zip) as described in RFC 1952. This format is a Lempel-Ziv coding (LZ77) with a 32 bit CRC.
identity	Defines the default (identity) encoding, which does not require the use of transformation.

Command Modes

Class map HTTP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You can specify multiple **match transfer-encoding** commands within a class map. Each **match transfer-encoding** command configures a single application type.

The ACE disables the **match transfer-encoding** command by default. If you do not configure a transfer-encoding type, the default action by the ACE is to allow the HTTP transfer-encoding types without generating a log.

Examples

To specify a chunked HTTP transfer encoding type to limit the HTTP traffic that flows through the ACE, enter:

```
(config)# class-map type http inspect HTTP_INSPECT_L7CLASS
host1/Admin(config-cmap-http-insp)# match transfer-encoding chunked
```

Related Commands

(config-cmap-http-insp) description

(config-cmap-http-insp) match url

To configure the class map to define application inspection decisions based on URL name and, optionally, HTTP method, use the **match url** command. HTTP performs regular expression matching against the received packet data from a particular connection based on the URL expression. Use the **no** form of this command to clear a URL match criteria from the class map.

[*line_number*] **match url** *expression*

no [*line_number*] **match url** *expression*

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
expression	URL or portion of a URL to match. The URL string range is from 1 to 255 characters. Include only the portion of the URL following www.hostname.domain in the match statement. For a list of the supported characters that you can use in regular expressions, see Table 2-5.

Command Modes

Class map HTTP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Include only the portion of the URL following www.hostname.domain in the match statement. For example, in the URL www.anydomain.com/latest/whatsnew.html, include only /latest/whatsnew.html. To match the www.anydomain.com portion, the URL string can take the form of a URL regular expressions. The ACE supports the use of regular expressions for matching.

When matching URLs, the period (.) character does not have a literal meaning in regular expressions. Use either the brackets ([ ]) or the slash (/) character classes to match this symbol, for example, specify www[.]xyz[.]com instead of www.xyz.com.

Examples

To specify that the Layer 7 class map is to match and perform application inspection on a specific URL, enter:

```
(config)# class-map type http inspect HTTP_INSPECT_L7CLASS
host1/Admin(config-cmap-http-insp)# match url whatsnew/latest.*
```

To use regular expressions to emulate a wildcard search to match on any .gif or .html file, enter:

```
(config)# class-map type http inspect match-any HTTP_INSPECT_L7CLASS
host1/Admin(config-cmap-http-insp)# match url .*.gif
host1/Admin(config-cmap-http-insp)# match url .*.html
```

Related Commands

(config-cmap-http-insp) description

(config-cmap-http-insp) match url length

To limit the HTTP traffic allowed through the ACE by specifying the maximum length of a URL in a request message that can be received by the ACE, use the **match url length** command. Messages will be either allowed or denied based on the Layer 7 HTTP deep packet inspection policy map action. Use the **no** form of this command to clear a URL length match criteria from the class map.

[*line_number*] **match url length** {**eq** *bytes* | **gt** *bytes* | **lt** *bytes* | **range** *bytes1 bytes 2*}

no [*line_number*] **match url length** {**eq** *bytes* | **gt** *bytes* | **lt** *bytes* | **range** *bytes1 bytes 2*}

Syntax Description

line_number	(Optional) Line number to assist you in editing or deleting individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
eq *bytes*	Specifies a value for the HTTP URL length received by the ACE. Based on the policy map action, the ACE allows or denies messages with an HTTP URL length equal to the specified value. Valid entries are from 1 to 65535 bytes.
gt *bytes*	Specifies a minimum value value for the HTTP URL length received by the ACE. Based on the policy map action, the ACE allows or denies messages with an HTTP URL length greater than the specified value. Valid entries are from 1 to 65535 bytes.
lt *bytes*	Specifies a maximum value for the HTTP URL length received by the ACE. Based on the policy map action, the ACE allows or denies messages with an HTTP URL length less than the specified value. Valid entries are from 1 to 65535 bytes.
range *bytes1 bytes*	Specifies a size range for the HTTP URL length received by the ACE. Based on the policy map action, the ACE allows or denies messages with an HTTP URL length within this range. The range is from 1 to 65535 bytes.

Command Modes

Class map HTTP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To specify that the class map is to match on a URL with a length equal to 10000 bytes in the request message, enter:

```
(config)# class-map type http inspect HTTP_INSPECT_L7CLASS
host1/Admin(config-cmap-http-insp)# match url length eq 10000
```

Related Commands

(config-cmap-http-insp) description

Class Map HTTP Load Balancing Configuration Mode Commands

Class map HTTP load balancing configuration mode commands allow you to create a Layer 7 HTTP server load balancing (SLB) class map. To create this class map and access class map HTTP load balancing configuration mode, use the **class-map type http loadbalance** command. The prompt changes to (config-cmap-http-lb). Use the **no** form of this command to remove an HTTP SLB class map from the ACE.

class-map type http loadbalance [**match-all** | **match-any**] *map_name*

no class-map type http loadbalance [**match-all** | **match-any**] *map_name*

Syntax Description

match-all | **match-any**	(Optional) Determines how the ACE evaluates Layer 7 HTTP SLB operations when multiple match criteria exist in a class map. The class map is considered a match if the **match** commands meet one of the following conditions: • **match-all** —(Default) Specifies that network traffic needs to satisfy all of the match criteria (implicit AND) to match the Layer 7 load-balancing class map. The **match-all** keyword is applicable only for match statements of different Layer 7 load-balancing types. For example, specifying a **match-all** condition for URL, HTTP header, and URL cookie statements in the same class map is valid. However, specifying a **match-all** condition for multiple HTTP headers or multiple cookies with the same names or multiple URLs in the same class map is invalid. • **match-any**—Specifies that network traffic needs to satisfy only one of the match criteria (implicit OR) to match the HTTP load-balancing class map. The **match-any** keyword is applicable only for match statements of the same Layer 7 load-balancing type. For example, the ACE does not allow you to specify a **match-any** condition for URL, HTTP header, and URL cookie statements in the same class map but does allow you to specify a **match-any** condition for multiple URLs, or multiple HTTP headers or multiple cookies with different names in the same class map.
map_name	Name assigned to the Layer 7 HTTP SLB class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To create a Layer 7 class map named L7SLB_CLASS that performs server load balancing, enter:

```
host1/Admin(config)# class-map type http loadbalance match-any L7SLB_CLASS
host1/Admin(config-cmap-http-lb)#
```

Related Commands

(config) policy-map

(config-cmap-http-lb) description

To provide a brief summary about the Layer 7 HTTP SLB class map, use the **description** command. Use the **no** form of this command to remove the description from the class map.

description *text*

no description

Syntax Description

text	Description about the class map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Class map HTTP load balancing configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description that the class map is to perform server load balancing, enter:

```
host1/Admin(config-cmap-http-lb)# description HTTP LOAD BALANCE PROTOCOL 1
```

Related Commands

This command has no related commands.

(config-cmap-http-lb) match class-map

To identify one Layer 7 HTTP SLB class map as a matching criterion for another Layer 7 HTTP SLB class map, use the **match class-map** command. Use the **no** form of this command to remove the nested class map from the HTTP SLB class map.

[*line_number*] **match class-map** *name*

no [*line_number*] **match class-map** *name*

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
name	Name of an existing Layer 7 load-balancing class map.

Command Modes

Class map HTTP load balancing configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The **match class map** command allows you to combine the use of the **match-any** and **match-all** keywords in the same class map. To combine **match-all** and **match-any** characteristics in a class map, create a class map that uses one **match** command (either **match-any** or **match-all**) and then use this class map as a match statement in a second class map that uses a different match type.

The nesting of class maps allows you to achieve complex logical expressions for Layer 7 HTTP-based server load balancing. The ACE restricts the nesting of class maps to two levels to prevent you from including a nested class map under another class map.

See the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide* for details about configuring the ACE to perform server load balancing.

Examples

To combine the characteristics of two class maps, one with **match-any** and one with **match-all** characteristics, into a single class map, enter:

```
(config)# class-map type http loadbalance match-all class3
(config-cmap-http-lb)# 100 match http cookie testcookie1 cookie-value 123456
(config-cmap-http-lb)# 200 match http header Host header-value XYZ
(config-cmap-http-lb)# exit

(config)# class-map type http loadbalance match-any class4
(config-cmap-http-lb)# 10 match class-map class3
(config-cmap-http-lb)# 20 match source-address 192.168.11.2
(config-cmap-http-lb)# 30 match source-address 192.168.11.3
(config-cmap-http-lb)# exit
```

Related Commands

(config-cmap-http-lb) description

(config-cmap-http-lb) match cipher

To make server load-balancing (SLB) decisions based on a specific SSL cipher or cipher strength used to initiate a connection, use the **match cipher** command. Use the **no** form of this command to remove an SSL cipher content match statement from the class map.

match cipher {**equal-to** *cipher* | **less-than** *cipher_strength*}

no match cipher {**equal-to** *cipher* | **less-than** *cipher_strength*}

Syntax Description

equal-to *cipher*	Specifies the SSL cipher. The possible values for *cipher* are as follows: • RSA_EXPORT1024_WITH_DES_CBC_SHA • RSA_EXPORT1024_WITH_RC4_56_MD5 • RSA_EXPORT1024_WITH_RC4_56_SHA • RSA_EXPORT_WITH_DES40_CBC_SHA • RSA_EXPORT_WITH_RC4_40_MD5 • RSA_WITH_3DES_EDE_CBC_SHA • RSA_WITH_AES_128_CBC_SHA • RSA_WITH_AES_256_CBC_SHA • RSA_WITH_DES_CBC_SHA • RSA_WITH_RC4_128_MD5 • RSA_WITH_RC4_128_SHA
less-than *cipher_strength*	Specifies a noninclusive minimum SSL cipher bit strength. For example, if you specify a cipher strength value of 128, any SSL cipher that was no greater than 128 would hit the traffic polkcy. If the SSL cipher was 128-bit or greater, the connection would miss the policy. The possible values for *cipher_strength* are as follows: • 128 • 168 • 256 • 56

Command Modes

Class map HTTP load balancing configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines This command has no usage guidelines.

Examples To specify that the Layer 7 SLB class map load balances on a specific SSL cipher, enter:

```
host1/Admin(config)# class-map type http loadbalance http match-all L7SLBCLASS
host1/Admin(config-cmap-http-lb)# 10 match cipher equal-to RSA_WITH_RC4_128_CBC_SHA
```

To specify that the Layer 7 SLB class map load balances on a specific minimum SSL cipher bit strength, enter:

```
host1/Admin(config)# class-map type http loadbalance http match-all L7SLBCLASS
host1/Admin(config-cmap-http-lb)# 100 match cipher less-than 128
```

Related Commands This command has no related commands.

(config-cmap-http-lb) match http content

To configure a class map to make Layer 7 SLB decisions based on the HTTP packet content, use the **match http content** command. Use the **no** form of this command to remove an HTTP content match statement from the class map.

[*line_number*] **match http content** *expression* [**offset** *number*]

no [*line_number*] **match http content** *expression* [**offset** *number*]

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements. Enter an integer from 2 to 1024 as the line number.
expression	Regular expression content to match. Enter a string from 1 to 255 alphanumeric characters. The ACE supports the use of regular expressions for matching data strings. For a list of the supported characters that you can use in regular expressions, see Table 2-5.
offset *number*	(Optional) Specifies the byte at which the ACE begins parsing the packet data. Enter an integer from 0 to 999. The default is 0.

Command Modes Class map HTTP load balancing configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The ACE can perform regular expression matching against the received packet data from a particular connection based on a regular expression string in HTTP packet data (not the header).

When matching data strings, the period (.) and question mark (?) characters do not have a literal meaning in regular expressions. Use brackets ([]) to match these symbols (for example, enter www[.]xyz[.]com instead of www.xyz.com). You can also use a backslash (\) to escape a dot (.) or a question mark (?).

Examples

To specify that the Layer 7 class map performs SLB based on a specific HTTP header string, enter:

```
host1/Admin(config)# class-map type http loadbalance match-any L7_HTTP_CLASS
host1/Admin(config-cmap-http-lb)# 10 match http content abc*123 offset 50
```

Related Commands

(config-cmap-http-lb) description

(config-cmap-http-lb) match http cookie

To configure the class map to make Layer 7 server load-balancing (SLB) decisions based on the name and string of a cookie, use the **match http cookie** command. The ACE performs regular expression matching against the received packet data from a particular connection based on the cookie expression. You can configure a maximum of five cookie names per VIP. Use the **no** form of this command to remove an HTTP cookie match statement from the class map.

[*line_number*] **match http cookie** {*name* | **secondary** *name*} **cookie-value** *expression*

no [*line_number*] **match http cookie** {*name* | **secondary** *name*} **cookie-value** *expression*

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
name	Unique cookie name. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
secondary *name*	Specifies a cookie in a URL string. You can specify the delimiters for cookies in a URL string using a command in an HTTP parameter map. For more information, see the "Parameter Map HTTP Configuration Mode Commands" section.
cookie-value *expression*	Specifies a unique cookie value expression. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters. The ACE supports the use of regular expressions for matching string expressions. For a list of the supported characters that you can use for matching string expressions, see Table 2-5.

Command Modes

Class map HTTP load balancing configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To specify that the Layer 7 class map load balances on a cookie with the name of testcookie1 or testcookie2, enter:

```
(config)# class-map type http loadbalance match-any L7SLBCLASS
(config-cmap-http-lb)# 100 match http cookie testcookie1 cookie-value 123456
(config-cmap-http-lb)# 200 match http cookie testcookie2 cookie-value 789987
```

Related Commands

(config-cmap-http-lb) description

(config-cmap-http-lb) match http header

To configure a class map to make Layer 7 SLB decisions based on the name and value of an HTTP header, use the **match http header** command. The ACE performs regular expression matching against the received packet data from a particular connection based on the HTTP header expression. You can configure a maximum of 10 HTTP header names and cookie names per class. Use the **no** form of this command to remove all HTTP header match criteria from the class map.

[*line_number*] **match http header** *header_name* **header-value** *expression*

no [*line_number*] **match http header** *header_name* **header-value** *expression*

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.

header_name	Name of the field in the HTTP header. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. You can enter a text string with spaces if you enclose the entire string in quotation marks (“). You can enter any header field name, including a standard HTTP header field name or any user-defined header field name. Valid selections include request-header fields, general-header fields, and entity-header fields. **Note** The *header_name* argument cannot include the colon in the name of the HTTP header; the ACE rejects the colon as an invalid token. For a list of the standard HTTP/1.1 header field names, see Table 2-6.
header-value *expression*	Specifies the header value expression string to compare against the value in the specified field in the HTTP header. Enter a text string from 1 to 255 alphanumeric characters. For a list of the supported characters that you can use for regular expressions, see Table 2-5.

Command Modes

Class map HTTP load balancing configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The ACE supports the use of regular expressions for matching. Expressions are stored in a header map in the form *header-name: expression*. Header expressions allow spaces if the spaces are escaped or quoted. For a list of the supported characters that you can use for regular expressions, see Table 2-5.

Table 2-6 lists the standard HTTP header fields that you can use in an HTTP load-balancing class map.

Table 2-6 Standard HTTP Header Fields

Field Name	Description
Accept	Semicolon-separated list of representation schemes (content type metainformation values) that will be accepted in the response to the request.
Accept-Charset	Character sets that are acceptable for the response. This field allows clients capable of understanding more comprehensive or special-purpose character sets to signal that capability to a server that can represent documents in those character sets.
Accept-Encoding	Restricts the content encoding that a user will accept from the server.
Accept-Language	ISO code for the language in which the document is written. The language code is an ISO 3316 language code with an optional ISO 639 country code to specify a national variant.
Authorization	Specifies that the user agent wants to authenticate itself with a server, usually after receiving a 401 response.

Table 2-6 Standard HTTP Header Fields (continued)

Field Name	Description
Cache-Control	Directives that must be obeyed by all caching mechanisms along the request/response chain. The directives specify behavior intended to prevent caches from adversely interfering with the request or response.
Connection	Allows the sender to specify connection options.
Content-MD5	MD5 digest of the entity-body that provides an end-to-end integrity check. Only a client or an origin server can generate this header field.
Expect	Used by a client to inform the server about what behaviors the client requires.
From	E-mail address of the person that controls the requesting user agent.
Host	Internet host and port number of the resource being requested, as obtained from the original URI given by the user or referring resource. The Host field value must represent the naming authority of the origin server or gateway given by the original URL.
If-Match	Used with a method to make it conditional. A client that has one or more entities previously obtained from the resource can verify that one of those entities is current by including a list of their associated entity tags in the If-Match header field. This feature allows efficient updates of cached information with a minimum amount of transaction overhead. It is also used on updating requests to prevent inadvertent modification of the wrong version of a resource. As a special case, the asterisk (*) value matches any current entity of the resource.
Pragma	Pragma directives understood by servers to whom the directives are relevant. The syntax is the same as for other multiple-value fields in HTTP, for example, the **accept** field, a comma-separated list of entries, for which the optional parameters are separated by semicolons.
Referer	Address (URI) of the resource from which the URI in the request was obtained.
Transfer-Encoding	What (if any) type of transformation has been applied to the message body in order to safely transfer it between the sender and the recipient.
User-Agent	Information about the user agent, for example, a software program originating the request. This information is for statistical purposes, the tracing of protocol violations, and automated recognition of user agents to customize responses to avoid particular user agent limitations.
Via	Used by gateways and proxies to indicate the intermediate protocols and recipients between the user agent and the server on requests and between the origin server and the client on responses.

Examples

To specify that the Layer 7 class map performs SLB on an HTTP header named Host, enter:

```
(config)# class-map type http loadbalance match-any L7SLBCLASS
(config-cmap-http-lb)# 100 match http header Host header-value .*cisco.com
```

To use regular expressions in a class map to emulate a wildcard search to match the header value expression string, enter:

```
host1/Admin(config)# class-map type http loadbalance match-any L7SLBCLASS
host1/Admin(config-cmap-http-lb)# 10 match http header Host header-value .*cisco.com
host1/Admin(config-cmap-http-lb)# 20 match http header Host header-value .*yahoo.com
```

To specify that the Layer 7 class map performs SLB on an HTTP header named Via, enter:

```
host1/Admin(config)# class-map type http loadbalance match-all L7SLBCLASS
host1/Admin(config-cmap-http-lb)# 30 match http header Via header-value 192.*
```

Related Commands **(config-cmap-http-lb) description**

(config-cmap-http-lb) match http url

To configure a class map to make Layer 7 SLB decisions based on the URL name and, optionally, the HTTP method, use the **match http url** command. The ACE performs regular expression matching against the received packet data from a particular connection based on the HTTP URL string. Use the **no** form of this command to remove a URL match statement from the class map.

[*line_number*] **match http url** *expression* [**method** *name*]

no [*line_number*] **match http url** *expression* [**method** *name*]

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
expression	URL, or portion of a URL, to match. Enter a URL string from 1 to 255 alphanumeric characters. Include only the portion of the URL that follows www.*hostname*.*domain* in the match statement. For a list of the supported characters that you can use for regular expressions, see Table 2-5.
method *name*	(Optional) Specifies the HTTP method to match. Enter a method name as an unquoted text string with no spaces and a maximum of 15 alphanumeric characters. The method can either be one of the standard HTTP 1.1 method names (OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, or CONNECT) or a text string that must be matched exactly (for example, CORVETTE).

Command Modes

Class map HTTP load balancing configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Include only the portion of the URL that follows www.*hostname.domain* in the match statement. For example, in the URL www.anydomain.com/latest/whatsnew.html, include only /latest/whatsnew.html. To match the www.anydomain.com portion, the URL string can take the form of a URL regular expression. The ACE supports the use of regular expressions for matching URL strings. For a list of the supported characters that you can use for regular expressions, see Table 2-5.

When matching URLs, note that the period (.) and question mark (?) characters do not have a literal meaning in regular expressions. Use brackets ([]) to match these symbols (for example, enter www[.]xyz[.]com instead of www.xyz.com). You can also use a backslash (\) to escape a dot (.) or a question mark (?).

Examples

To specify that the Layer 7 class map performs SLB on a specific URL, enter:

```
host1/Admin(config)# class-map type http loadbalance L7SLBCLASS
host1/Admin(config-cmap-http-lb)# 10 match http url whatsnew/latest.*
```

To use regular expressions to emulate a wildcard search to match on any .gif or .html file, enter:

```
host1/Admin(config)# class-map type http loadbalance match-any L7SLBCLASS
host1/Admin(config-cmap-http-lb)# 100 match http url .*.gif
host1/Admin(config-cmap-http-lb)# 200 match http url .*.html
```

Related Commands

(config-cmap-http-lb) description

(config-cmap-http-lb) match source-address

To configure the class map to make Layer 7 SLB decisions based on a client source IP address, use the **match source-address** command. Use the **no** form of this command to remove the source IP address match statement from the class map.

[*line_number*] **match source-address** *ip_address* [*netmask*]

no [*line_number*] **match source-address** *ip_address* [*netmask*]

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
ip_address	Source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.2).
netmask	(Optional) Subnet mask of the IP address. Enter the netmask in dotted-decimal notation (for example, 255.255.255.0). The default is 255.255.255.255.

Command Modes

Class map HTTP load balancing configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To specify that the class map match on source IP address 192.168.11.2 255.255.255.0, enter:

```
host1/Admin(config)# class-map type http loadbalance match-any L7SLBCLASS
host1/Admin(config-cmap-http-lb)# 50 match source-address 192.168.11.2 255.255.255.0
```

Related Commands

(config-cmap-http-lb) description

Class Map Management Configuration Mode Commands

Class map management configuration mode allows you to create a Layer 3 and Layer 4 class map to classify the IP network management traffic received by the ACE. To create this class map and access class map management configuration mode, use the **class-map type management** configuration command. The prompt changes to (config-cmap-mgmt). This command permits network management traffic by identifying the incoming IP management protocols that the ACE can receive as well as the client source host IP address and subnet mask as the matching criteria. A class map of **type management** provides access for one or more of the following management protocols: HTTP, HTTPS, ICMP, SNMP, SSH, or Telnet.

Use the **no** form of this command to remove a network management class map.

class-map type management [**match-all** | **match-any**] *map_name*

no class-map type management [**match-all** | **match-any**] *map_name*

Syntax Description

match-all | **match-any**	(Optional) Determines how the ACE evaluates Layer 3 and Layer 4 network management traffic when multiple match criteria exist in a class map. The class map is considered a match if the **match** commands meet one of the following conditions. • **match-all**—(Default) Traffic being evaluated must match all of the match criteria listed in the class map (typically, **match** commands of different types). • **match-any**—Traffic being evaluated must match one of the match criteria listed in the class map (typically, **match** commands of the same type).
map_name	Name assigned to the Layer 3 and Layer 4 network management protocol class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the context Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples To create a Layer 3 and Layer 4 class map named MGMT-ACCESS_CLASS that classifies the network management protocols that can be received by the ACE, enter:

```
host1/Admin# class-map type management match-any MGMT-ACCESS_CLASS
host1/Admin(config-cmap-mgmt)#
```

Related Commands This command has no related commands.

(config-cmap-mgmt) description

To provide a brief summary about the Layer 3 and Layer 4 management class map, use the **description** command. Use the **no** form of this command to remove the description from the class map.

description *text*

no description

Syntax Description

text	Description about the class map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes Class map management configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines This command has no usage guidelines.

Examples To add a description that the class map is to allow remote Telnet access, enter:

```
host1/Admin# class-map type management TELNET-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# description Allow Telnet access to the ACE
```

Related Commands This command has no related commands.

(config-cmap-mgmt) match protocol

To configure the class map to identify the network management protocols that can be received by the ACE, use the **match protocol** command. You configure the associated policy map to permit access to the ACE for the specified management protocols. As part of the network management access traffic classification, you also specify either a client source host IP address and subnet mask as the matching criteria or instruct the ACE to allow any client source address for the management traffic classification. Use the **no** form of this command to deselect the specified network management protocol match criteria from the class map.

[*line_number*] **match protocol** {**http** | **https** | **icmp** | **kalap-udp** | **snmp** | **ssh** | **telnet** | **xml-https**} {**any** | **source-address** *ip_address mask*}

no [*line_number*] **match protocol** {**http** | **https** | **icmp** | **kalap-udp** | **snmp** | **ssh** | **telnet** | **xml-https**} {**any** | **source-address** *ip_address mask*}

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 255 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
http	Specifies the Hypertext Transfer Protocol (HTTP).
https	Specifies the secure (SSL) Hypertext Transfer Protocol (HTTP) for connectivity with the Device Manager GUI on the ACE using port 443.
icmp	Specifies the Internet Control Message Protocol (ping).
kalap-udp	Specifies the keepalive-appliance protocol (KAL-AP) over UDP.
snmp	Specifies the Simple Network Management Protocol (SNMP).
ssh	Specifies a Secure Shell (SSH) connection to the ACE.
telnet	Specifies a Telnet connection to the ACE.
xml-https	Specifies HTTPS as transfer protocol to send and receive XML documents between the ACE and a Network Management System (NMS). Communication is performed using port 10443.
any	Specifies any client source address for the management traffic classification.
source-address	Specifies a client source host IP address and subnet mask as the network traffic matching criteria. As part of the classification, the ACE implicitly obtains the destination IP address from the interface on which you apply the policy map.
ip_address	Source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
mask	Subnet mask of the client entry in dotted-decimal notation (for example, 255.255.255.0).

Command Modes

Class map management configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised.

Usage Guidelines

This command has no usage guidelines.

Examples

To specify that the class map allows SSH access to the ACE from the source IP address 192.168.10.1 255.255.255.0, enter:

```
host1/Admin# class-map type management SSH-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# match protocol ssh source-address 192.168.10.1
255.255.255.0
```

Related Commands

(config-cmap-mgmt) description

Class Map RADIUS Load Balancing Configuration Mode Commands

The ACE performs Layer 7 Remote Authentication Dial-In User Service (RADIUS) load balancing based on the calling-station-ID or the username RADIUS attribute. To create a RADIUS load-balancing class map and access class map RADIUS load balancing configuration mode, use the **class-map type radius loadbalance** command. The prompt changes to (config-cmap-radius-lb). Use the **no** form of this command to remove a RADIUS load-balancing class map from the configuration.

class-map type radius loadbalance [**match-all** | **match-any**] *map_name*

no class-map type radius loadbalance [**match-all** | **match-any**] *map_name*

Syntax Description

match-all | **match-any**	(Optional) Determines how the ACE evaluates RADIUS network traffic when multiple match criteria exist in a class map. • **match-all**—(Default) Network traffic needs to satisfy all of the match criteria (implicit AND) to match the RADIUS load-balancing class map. • **match-any**—Network traffic needs to satisfy only one of the match criteria (implicit OR) to match the RADIUS load-balancing class map.
map_name	Unique identifier assigned to the RADIUS load-balancing class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To create a class map named RADIUS_L7_CLASS, enter:

```
host1/Admin(config)# class-map type radius loadbalance match-any RADIUS_L7_CLASS
host1/Admin(config-cmap-radius-lb)#
```

To remove the RADIUS class map from the configuration, enter:

```
host1/Admin(config)# no class-map type radius loadbalance match-any RADIUS_L7_CLASS
```

Related Commands

(config) class-map
(config-cmap-radius-lb) description
(config-cmap-radius-lb) match radius attribute

(config-cmap-radius-lb) description

To provide a brief description of the RADIUS load-balancing class map, use the **description** command. Use the **no** form of this command to remove the description from the class map.

description *text*

no description

Syntax Description

text	Description of the class map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Class map RADIUS load balancing configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description for the RADIUS load-balancing class map, enter:

```
host1/Admin(config)# class-map type radius loadbalance match-any RADIUS_L7_CLASS
host1/Admin(config-cmap-radius-lb)# description RADIUS CLASS MAP
```

To remove a description from a RADIUS load-balancing class map, enter:

```
host1/Admin(config-cmap-radius-lb)# no description
```

Related Commands

(config-cmap-radius-lb) match radius attribute

(config-cmap-radius-lb) match radius attribute

To specify the RADIUS attribute match criteria for the class map, use the **match radius attribute** command. Use the **no** form of this command to remove the match statement from the RADIUS attribute class map.

[*line_number*] **match radius attribute** {**calling-station-id** | **username**} *expression*

no [*line_number*] **match radius attribute** {**calling-station-id** | **username**} *expression*

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. For example, you can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate any priority for the match statements. Enter a unique integer from 2 to 1024.
calling-station-id	Specifies the unique identifier of the calling station.
username	Specifies the name of the RADIUS user who initiated the connection.
expression	Calling station ID or username to match. Enter a string from 1 to 64 alphanumeric characters. The ACE supports the use of regular expressions for matching strings. For a list of the supported characters that you can use in regular expressions, see Table 2-5.

Command Modes

Class map RADIUS load balancing configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The ACE performs Layer 7 RADIUS load balancing based on the calling-station-ID or username RADIUS attribute.

Examples

To configure RADIUS match criteria based on the calling station ID attribute, enter:

```
host1/Admin(config)# class-map type radius loadbalance match-any RADIUS_L7_CLASS
host1/Admin(config-cmap-radius-lb)# 10 match radius attribute calling-station-id 122*
```

To remove the RADIUS attribute match statement from the RADIUS_L7_CLASS class map, enter:

```
host1/Admin(config-cmap-radius-lb)# no 10
```

Related Commands

(config-cmap-radius-lb) description

Class Map RTSP Load Balancing Configuration Mode Commands

Class map Real-Time Streaming Protocol (RTSP) load balancing configuration mode commands allow you to create a Layer 7 RTSP server load-balancing class map. To create an RTSP load-balancing class map and access class map RTSP load balancing configuration mode, use the **class-map type rtsp loadbalance** command. The prompt changes to (config-cmap-rtsp-lb). Use the **no** form of this command to remove an RTSP load-balancing class map from the configuration.

class-map type rtsp loadbalance [**match-all** | **match-any**] *map_name*

no class-map type rtsp loadbalance [**match-all** | **match-any**] *map_name*

Syntax Description

match-all | **match-any**	(Optional) Determines how the ACE evaluates RTSP network traffic when multiple match criteria exist in a class map. • **match-all**—(Default) Network traffic needs to satisfy all of the match criteria (implicit AND) to match the RTSP load-balancing class map. • **match-any**—Network traffic needs to satisfy only one of the match criteria (implicit OR) to match the RTSP load-balancing class map.
map_name	Unique identifier assigned to the RTSP load-balancing class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To create a class map named RTSP_L7_CLASS, enter:

```
host1/Admin(config)# class-map type rtsp loadbalance match-any RTSP_L7_CLASS
host1/Admin(config-cmap-rtsp-lb)#
```

To remove the RTSP class map from the configuration, enter:

```
host1/Admin(config)# no class-map type rtsp loadbalance match-any RTSP_L7_CLASS
```

Related Commands

(config) class-map
(config-cmap-sip-lb) description

(config-cmap-rtsp-lb) description

To provide a brief description of the RTSP load-balancing class map, use the **description** command. Use the **no** form of this command to remove the description from the class map.

description *text*

no description

Syntax Description

text	Description of the class map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Class map RTSP load balancing configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description for the RTSP load-balancing class map, enter:

```
host1/Admin(config)# class-map type rtsp loadbalance match-any RTSP_L7_CLASS
host1/Admin(config-cmap-rtsp-lb)# description RTSP CLASS MAP
```

To remove the description from an RTSP load-balancing class map, enter:

```
host1/Admin(config-cmap-rtsp-lb)# no description
```

Related Commands

This command has no related commands.

(config-cmap-rtsp-lb) match class-map

To identify one RTSP load-balancing class map as a matching criterion for another RTSP load-balancing class map, use the **match class-map** command. Use the **no** form of this command to remove the nested class map from an RTSP load-balancing class map.

[*line_number*] **match class-map** *name*

no [*line_number*] **match class-map** *name*

Syntax Description

line_number	(Optional) Line number that you can use to edit or delete individual **match** commands. For example, you can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate any priority for the match statements. Enter a unique integer from 2 to 1024.
name	Name of an existing RTSP load-balancing class map.

Command Modes

Class map RTSP load balancing configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The **match class-map** command allows you to combine the use of the **match-any** and **match-all** keywords in the same class map. To combine **match-all** and **match-any** characteristics in a class map, create a class map that uses one **match** command (either **match-any** or **match-all**) and then use this class map as a match statement in a second class map that uses the other match type.

The nesting of class maps allows you to achieve complex logical expressions for Layer 7 server load balancing. The ACE restricts the nesting of class maps to two levels to prevent you from including a nested class map under another class map.

Examples

To combine the characteristics of two class maps, one with **match-any** and one with **match-all** characteristics, into a single class map, enter:

```
host1/Admin(config)# class-map type rtsp loadbalance match-any CLASS3
host1/Admin(config-cmap-rtsp-lb)# 100 match rtsp url .*.gif
host1/Admin(config-cmap-rtsp-lb)# 200 match rtsp header Host header-value XYZ
host1/Admin(config-cmap-rtsp-lb)# exit

host1/Admin(config)# class-map type rtsp loadbalance match-all CLASS4
host1/Admin(config-cmap-rtsp-lb)# 10 match class-map CLASS3
host1/Admin(config-cmap-rtsp-lb)# 20 match source-address 192.168.11.2
host1/Admin(config-cmap-rtsp-lb)# exit
```

To remove the nested class map from the RTSP class map, enter:

```
host1/Admin(config-cmap-rtsp-lb)# no 10
```

Related Commands (config-cmap-sip-lb) description

(config-cmap-rtsp-lb) match rtsp header

To configure a class map to make RTSP SLB decisions based on the name and value of an RTSP header, use the **match rtsp header** command. Use the **no** form of this command to remove an RTSP header match statement from the RTSP load-balancing class map.

[*line_number*] **match rtsp header** *name* **header-value** *expression*

no [*line_number*] **match rtsp header** *name* **header-value** *expression*

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. For example, you can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate any priority for the match statements. Enter a unique integer from 2 to 1024.
name	Name of the field in the RTSP header. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. You can enter a text string with spaces if you enclose the entire string in quotation marks (“). You can enter any header field name, including a standard RTSP header field name or any user-defined header field name. Because RTSP is similar in syntax and operation to HTTP/1.1, you can use any HTTP header listed in Table 2-6 if the RTSP server supports it. For a complete list of RTSP headers, see RFC 2326.
expression	Header value expression string to compare against the value in the specified field in the RTSP header. Enter a text string with a maximum of 255 alphanumeric characters. The ACE supports the use of regular expressions for header matching. Expressions are stored in a header map in the form *header-name: expression*. Header expressions allow spaces if the entire string that contains spaces is quoted. If you use a **match-all** class map, all headers in the header map must be matched. For a list of the supported characters that you can use in regular expressions, see Table 2-5.

Command Modes

Class map RTSP load balancing configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

When the ACE receives an RTSP session request, the load-balancing decision is based on the first request message. All subsequent request and response message exchanges are forwarded to the same server. When you configure header match criteria, ensure that the header is included in the first request message by a media player.

The ACE can perform regular expression matching against the received packet data from a particular connection based on the RTSP header expression. You can configure a maximum of 10 RTSP header names per class map.

Examples

To configure an RTSP class map to load balance based on an RTSP header named Session, enter:

```
host1/Admin(config)# class-map type rtsp loadbalance match-any L7SLBCLASS
host1/Admin(config-cmap-rtsp-lb)# 10 match rtsp header Session header-value abc123
```

To configure an RTSP class map to load balance based on an RTSP header named Via, enter:

```
host1/Admin(config)# class-map type rtsp loadbalance match-any L7SLBCLASS
host1/Admin(config-cmap-rtsp-lb)# 20 match rtsp header Via header-value 192.*
```

To remove the RTSP header match criteria from the L7SLBCLASS class map, enter:

```
host1/Admin(config-cmap-rtsp-lb)# no 10
host1/Admin(config-cmap-rtsp-lb)# no 20
```

Related Commands

(config-cmap-sip-lb) description

(config-cmap-rtsp-lb) match rtsp url

To configure a class map to make RTSP SLB decisions based on the URL name and optionally, the RTSP method, use the **match rtsp url** command. Use the **no** form of this command to remove an RTSP URL match statement from the RTSP load-balancing class map.

[*line_number*] **match rtsp url** *expression* [**method** *name*]

no [*line_number*] **match rtsp url** *expression* [**method** *name*]

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. For example, you can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate any priority for the match statements. Enter a unique integer from 2 to 1024.

expression	URL, or portion of a URL, to match. The ACE performs matching on whatever URL string appears after the RTSP method, regardless of whether the URL includes the hostname. The ACE supports the use of regular expressions for matching URL strings. For a list of the supported characters that you can use for regular expressions, see Table 2-5.
method *name*	(Optional) Specifies the RTSP method to match. Enter a method name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. The method can either be one of the standard RTSP method names (DESCRIBE, ANNOUNCE, GET_PARAMETER, OPTIONS, PAUSE, PLAY, RECORD, REDIRECT, SETUP, SET_PARAMETER, TEARDOWN) or a text string that must be matched exactly (for example, STINGRAY).

Command Modes

Class map RTSP load balancing configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

When matching URLs, the period (.) and question mark (?) characters do not have a literal meaning in regular expressions. Use brackets ([]) to match these symbols (for example, enter www[.]xyz[.]com instead of www.xyz.com). You can also use a backslash (\) to escape a dot (.) or a question mark (?).

Examples

To configure an RTSP class map to load balance based on a specific URL, enter:

```
host1/Admin(config)# class-map type rtsp loadbalance L7SLBCLASS
host1/Admin(config-cmap-rtsp-lb)# 10 match rtsp url /whatsnew/latest.*
```

To configure a URL match criterion that emulates a wildcard search to match on any .wav or .mpg file, enter:

```
host1/Admin(config)# class-map type rtsp loadbalance match-any L7SLBCLASS
host1/Admin(config-cmap-rtsp-lb)# 100 match rtsp url .*.wmv
host1/Admin(config-cmap-rtsp-lb)# 200 match rtsp url .*.mpg
```

To remove a URL match statement from the L7SLBCLASS class map, enter:

```
host1/Admin(config-cmap-rtsp-lb)# no 100
```

Related Commands

(config-cmap-sip-lb) description

(config-cmap-rtsp-lb) match source-address

To configure the class map to make RTSP SLB decisions based on a client source IP address, use the **match source-address** command. Use the **no** form of this command to remove the source IP address match statement from the class map.

[*line_number*] **match source-address** *ip_address* [*netmask*]

no [*line_number*] **match source-address** *ip_address* [*netmask*]

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
ip_address	Source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.2).
netmask	(Optional) Subnet mask of the IP address. Enter the netmask in dotted-decimal notation (for example, 255.255.255.0). The default is 255.255.255.255.

Command Modes

Class map RTSP load balancing configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To specify that the class map match on source IP address 192.168.11.2 255.255.255.0, enter:

```
host1/Admin(config)# class-map type rtsp loadbalance match-any L7SLBCLASS
host1/Admin(config-cmap-rtsp-lb)# 50 match source-address 192.168.11.2 255.255.255.0
```

To remove the source IP address match statement from the class map, enter:

```
host1/Admin(config-cmap-rtsp-lb)# no 50
```

Related Commands

(config-cmap-sip-lb) description

Class Map SIP Inspection Configuration Mode Commands

SIP inspection configuration mode commands allow you to create a Layer 7 SIP inspection class map. The ACE uses class maps to filter SIP traffic based on a variety of parameters such as, called party, calling party, and media type. To create this class map and access class map SIP inspection configuration mode, use the **class-map type sip inspect** command. The prompt changes to (config-cmap-sip-insp). Use the **no** form of this command to remove the SIP inspection class map from the ACE.

class-map type sip inspect [**match-all | match-any**] *map_name*

no class-map type sip inspect [**match-all | match-any**] *map_name*

Syntax Description

match-all | match-any	(Optional) Determines how the ACE performs the inspection of SIP traffic when multiple match criteria exist in a class map. The class map is considered a match if the **match** commands meet one of the following conditions: • **match-all** —(Default) Network traffic needs to satisfy all of the match criteria (implicit AND) to match the Layer 7 SIP inspection class map. The **match-all** keyword is applicable only for match statements of different SIP inspection types. For example, specifying a **match-all** condition for SIP URI, SIP header, and SIP content statements in the same class map is valid. However, specifying a **match-all** condition for multiple SIP headers with the same names or multiple URLs in the same class map is invalid. • **match-any**—Network traffic needs to satisfy only one of the match criteria (implicit OR) to match the Layer 7 SIP inspection class map. The **match-any** keyword is applicable only for match statements of the same Layer 7 SIP inspection type. For example, the ACE allows you to specify a **match-any** condition for SIP URI, SIP header, and SIP content statements in the same class map and allows you to specify a **match-any** condition for multiple URLs, multiple SIP headers, or multiple SIP content statements in the same class map as long as the statements are logical. For example, you could not have two **match uri sip length** statements in the same class map, but you could have one **match uri sip length** and one **match uri tel length** statement in one class map.
map_name	Name assigned to the class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

To classify the SIP application inspection of traffic for evaluation by the ACE, include one or more of the following commands to configure the match criteria for the Layer 7 class map:

- **(config-cmap-sip-insp) match called-party**
- **(config-cmap-sip-insp) match calling-party**
- **(config-cmap-sip-insp) match content**
- **(config-cmap-sip-insp) match im-subscriber**
- **(config-cmap-sip-insp) match message-path**
- **(config-cmap-sip-insp) match request-method**
- **(config-cmap-sip-insp) match third-party registration**
- **(config-cmap-sip-insp) match uri**

You may include multiple **match** commands in the class map.

Examples

To specify SIP_INSPECT_L7CLASS as the name of a class map and identify that all commands in the Layer 7 SIP application inspection class map must be satisfied for the ACE to indicate a match, enter:

```
(config)# class-map type sip inspect match-all SIP_INSPECT_L7CLASS
host1/Admin(config-cmap-sip-insp)# match calling-id .*ABC123
host1/Admin(config-cmap-sip-insp)# match im-subscriber JOHN_Q_PUBLIC
host1/Admin(config-cmap-sip-insp)# match content type sdp
```

To remove the SIP inspection class map from the ACE, enter:

```
(config)# no class-map type sip inspect match-any SIP_INSPECT_L7CLASS
```

Related Commands

(config) policy-map
(config-cmap-sip-insp) description

(config-cmap-sip-insp) description

To provide a brief summary about the Layer 7 SIP inspection class map, use the **description** command. Use the **no** form of this command to remove the description from the class map.

description *text*

no description

Syntax Description

text	Description about the class map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Class map SIP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description to the SIP inspection class map, enter:

```
host1/Admin(config-cmap-sip-insp)# description SIP inspection class map
```

To remove the description from the class map, enter:

```
host1/Admin(config-cmap-sip-insp)# no description
```

Related Commands

This command has no related commands.

(config-cmap-sip-insp) match called-party

To filter SIP traffic based on the called party, use the **match called-party** command. Use the **no** form of this command to remove the **match** statement from the class map.

[*line_number*] **match called-party** *expression*

no [*line_number*] **match called-party** *expression*

Syntax Description

[*line_number*]	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
expression	Calling party in the URI of the To header. Enter a regular expression from 1 to 255 alphanumeric characters.

Command Modes

Class map SIP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

You can filter SIP traffic based on the called party (callee or destination) as specified in the URI of the SIP To header. The ACE does not include the display name or tag part of the field.

The ACE supports the use of regular expressions for matching. Expressions are stored in a header map in the form *header-name: expression*. Header expressions allow spaces if the spaces are escaped or quoted. Table 2-5 lists the supported characters that you can use in regular expressions.

Examples

To identify the called party in the SIP To header, enter:

```
host1/Admin(config-cmap-sip-insp)# match called-party sip:some-user@somenetwork.com
```

To remove the **match** statement from the class map, enter:

```
host1/Admin(config-cmap-sip-insp)# no match called-party sip:some-user@somenetwork.com
```

Related Commands

(config-cmap-sip-insp) match calling-party
(config-cmap-sip-insp) match content
(config-cmap-sip-insp) match im-subscriber
(config-cmap-sip-insp) match message-path
(config-cmap-sip-insp) match request-method
(config-cmap-sip-insp) match third-party registration
(config-cmap-sip-insp) match uri

(config-cmap-sip-insp) match calling-party

To filter SIP traffic based on the calling party, use the **match calling-party** command. Use the **no** form of this command to remove the description from the class map.

[*line_number*] **match calling-party** *expression*

no [*line_number*] **match calling-party** *expression*

Syntax Description

[*line_number*]	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
expression	Calling party in the URI of the SIP From header. Enter a regular expression from 1 to 255 alphanumeric characters. The ACE supports the use of regular expressions for matching.

Command Modes

Class map SIP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

You can filter SIP traffic based on the calling party (caller or source) as specified in the URI of the SIP From header. The ACE does not include the display name or tag part of the field.

The ACE supports the use of regular expressions for matching. Expressions are stored in a header map in the form *header-name: expression*. Header expressions allow spaces if the spaces are escaped or quoted. See Table 2-5 for a list of the supported characters that you can use in regular expressions.

Examples

To identify the calling party in the SIP From header, enter:

```
host1/Admin(config-cmap-sip-insp)# match calling-party
sip:this-user@thisnetwork.com;tag=745g8
```

To remove the match statement from the class map, enter:

```
host1/Admin(config-cmap-sip-insp)# no match calling-party
sip:this-user@thisnetwork.com;tag=745g8
```

Related Commands

(config-cmap-sip-insp) match called-party
(config-cmap-sip-insp) match content
(config-cmap-sip-insp) match im-subscriber
(config-cmap-sip-insp) match message-path
(config-cmap-sip-insp) match request-method
(config-cmap-sip-insp) match third-party registration
(config-cmap-sip-insp) match uri

(config-cmap-sip-insp) match content

To define SIP content checks, use the **match content** command. Use the **no** form of this command to remove the **match** statement from the class map.

[*line_number*] **match content** {**length gt** *number*} | {**type sdp** | *expression*}

no [*line_number*] **match content** {**length gt** *number*} | {**type sdp** | *expression*}

Syntax Description

[*line_number*]	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
length	Specifies the SIP message body length.
gt	Greater than operator.
number	Maximum size of a SIP message body that the ACE allows. Enter an integer from 0 to 65534 bytes. If the message body is greater than the configured value, the ACE performs the action that you configure in the policy map.
type	Specifies a content type check.
sdp	Specifies that the traffic must be of type Session Description Protocol (SDP) to match the class map.
expression	Regular expression that identifies the content type in the SIP message body that is required to match the class map. Enter a regular expression from 1 to 255 alphanumeric characters. The ACE supports the use of regular expressions for matching. See Table 2-5 for a list of the supported characters that you can use in regular expressions.

Command Modes

Class map SIP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

You can configure the ACE to perform SIP content checks based on the content length or content type. By default, the ACE allows all content types.

Examples

To configure the ACE to drop SIP packets that have content with a length greater than 4000 bytes in length, enter:

```
host1/Admin(config)# class-map type sip inspect match-all SIP_INSP_CLASS
host1/Admin(config-cmap-sip-insp)# match content length gt 200
```

```
host1/Admin(config)# policy-map type sip inspect all-match SIP_INSP_POLICY
host1/Admin(config-pmap-ins-sip)# class SIP_INSP_CLASS
host1/Admin(config-pmap-ins-sip-c)# deny
```

To remove the match statement from the class map, enter:

```
host1/Admin(config-cmap-sip-insp)# no match content length gt 200
```

Related Commands

(config-cmap-sip-insp) match called-party
(config-cmap-sip-insp) match calling-party
(config-cmap-sip-insp) match im-subscriber
(config-cmap-sip-insp) match message-path
(config-cmap-sip-insp) match request-method
(config-cmap-sip-insp) match third-party registration
(config-cmap-sip-insp) match uri

(config-cmap-sip-insp) match im-subscriber

To filter SIP traffic based on the Instant Messaging (IM) subscriber, use the **match im-subscriber** command. Use the **no** form of this command to remove the description from the class map.

[*line_number*] **match im-subscriber** *expression*

no [*line_number*] **match im-subscriber** *expression*

Syntax Description

[*line_number*]	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
expression	Calling party. Enter a regular expression from 1 to 255 alphanumeric characters. The ACE supports the use of regular expressions for matching.

Command Modes

Class map SIP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The ACE supports the use of regular expressions for matching. Expressions are stored in a header map in the form *header-name: expression*. Header expressions allow spaces if the spaces are escaped or quoted. See Table 2-5 for a list of the supported characters that you can use in regular expressions.

Examples

To filter SIP traffic based on the IM subscriber, John Q. Public, enter:

```
host1/Admin(config-cmap-sip-insp)# match im-subscriber John_Q_Public
```

To remove the match statement from the class map, enter:

```
host1/Admin(config-cmap-sip-insp)# no match im-subscriber John_Q_Public
```

Related Commands

(config-cmap-sip-insp) match called-party
(config-cmap-sip-insp) match calling-party
(config-cmap-sip-insp) match content
(config-cmap-sip-insp) match message-path
(config-cmap-sip-insp) match request-method
(config-cmap-sip-insp) match third-party registration
(config-cmap-sip-insp) match uri

(config-cmap-sip-insp) match message-path

To filter SIP traffic based on the message path, use the **match message-path** command. Use the **no** form of this command to remove the match statement from the class map.

[*line_number*] **match message-path** *expression*

no [*line_number*] **match message-path** *expression*

Syntax Description

[*line_number*]	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
expression	SIP proxy server. Enter a regular expression from 1 to 255 alphanumeric characters. The ACE supports the use of regular expressions for matching.

Command Modes

Class map SIP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

SIP inspection allows you to filter messages coming from or transiting through certain SIP proxy servers. The ACE maintains a list of unauthorized SIP proxy IP addresses or URIs in the form of regular expressions and then checks this list against the VIA header field in each SIP packet. The default action is to drop SIP packets with VIA fields that match the regex list.

The ACE supports the use of regular expressions for matching. Expressions are stored in a header map in the form *header-name: expression*. Header expressions allow spaces if the spaces are escaped or quoted. See Table 2-5 for a list of the supported characters that you can use in regular expressions.

Examples

To filter SIP traffic based on the message path 192.168.12.3:5060, enter:

```
host1/Admin(config-cmap-sip-insp)# match message-path 192.168.12.3:5060
```

To remove the match statement from the class map, enter:

```
host1/Admin(config-cmap-sip-insp)# no match message-path 192.168.12.3:5060
```

Related Commands

(config-cmap-sip-insp) match called-party
(config-cmap-sip-insp) match calling-party
(config-cmap-sip-insp) match content
(config-cmap-sip-insp) match im-subscriber
(config-cmap-sip-insp) match request-method
(config-cmap-sip-insp) match third-party registration
(config-cmap-sip-insp) match uri

(config-cmap-sip-insp) match request-method

To filter SIP traffic based on the request method, use the **match request-method** command. Use the **no** form of this command to remove the description from the class map.

[*line_number*] **match request-method** *method_name*

no [*line_number*] **match request-method** *method_name*

Syntax Description

[*line_number*]	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
method_name	Supported SIP method that uses one of the following keywords: • **ack** • **bye** • **cancel** • **info** • **invite** • **message** • **notify** • **options** • **prack** • **refer** • **register** • **subscribe** • **unknown** • **update** Use the **unknown** keyword to permit or deny unknown or unsupported SIP methods.

Command Modes

Class map SIP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To filter SIP traffic based on the INVITE request method, enter:

```
host1/Admin(config-cmap-sip-insp)# match request-method invite
```

To remove the match statement from the class map, enter:

```
host1/Admin(config-cmap-sip-insp)# no match request-method invite
```

Related Commands

(config-cmap-sip-insp) match called-party
(config-cmap-sip-insp) match calling-party
(config-cmap-sip-insp) match content
(config-cmap-sip-insp) match im-subscriber
(config-cmap-sip-insp) match message-path
(config-cmap-sip-insp) match third-party registration
(config-cmap-sip-insp) match uri

(config-cmap-sip-insp) match third-party registration

To filter SIP traffic based on third-party registrations or deregistrations, use the **match third-party-registration** command. Use the **no** form of this command to remove the match statement from the class map.

[*line_number*] **match third-party registration** *expression*

no [*line_number*] **match third-party registration** *expression*

Syntax Description

[*line_number*]	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
expression	Privileged user that is authorized for third-party registrations. Enter a regular expression from 1 to 255 alphanumeric characters.

Command Modes

Class map SIP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

SIP allows users to register other users on their behalf by sending REGISTER messages with different values in the From and To header fields. This process may pose a security threat if the REGISTER message is actually a DEREGISTER message. A malicious user could cause a Denial of Service (DoS) attack by deregistering all users on their behalf.

To prevent this security threat, the ACE administrator can specify a list of privileged users who can register or unregister someone else on their behalf. The ACE maintains the list as a regex table. If you configure this policy, the ACE drops REGISTER messages with mismatched From and To headers and a From header value that does not match any of the privileged user IDs.

The ACE supports the use of regular expressions for matching. Expressions are stored in a header map in the form *header-name: expression*. Header expressions allow spaces if the spaces are escaped or quoted. See Table 2-5 for a list of the supported characters that you can use in regular expressions.

Examples

To filter SIP traffic based on SIP registrations or deregistrations, enter:

```
host1/Admin(config-cmap-sip-insp)# match third-party-registration USER1
```

To remove the match statement from the class map, enter:

```
host1/Admin(config-cmap-sip-insp)# no match third-party-registration USER1
```

Related Commands

(config-cmap-sip-insp) match called-party
(config-cmap-sip-insp) match calling-party
(config-cmap-sip-insp) match content
(config-cmap-sip-insp) match im-subscriber
(config-cmap-sip-insp) match message-path
(config-cmap-sip-insp) match request-method
(config-cmap-sip-insp) match uri

(config-cmap-sip-insp) match uri

To filter SIP traffic based on URIs, use the **match uri** command. Use the **no** form of this command to remove the match statement from the class map.

[*line_number*] **match uri** {**sip** | **tel**} **length gt** *value*

no [*line_number*] **match uri** {**sip** | **tel**} **length gt** *value*

Syntax Description

[*line_number*]	(Optional) Line number that allows you to edit or delete individual **match** commands. Enter an integer from 2 to 1024 as the line number. You can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate a priority for the match statements.
sip	Specifies that the ACE validates the length of a SIP URI.
tel	Specifies that the ACE validates the length of a Tel URI.
length	Specifies the length of the SIP or Tel URI.

gt	Specifies the greater than operator.
value	Maximum value for the length of the SIP URI or Tel URI in bytes. Enter an integer from 0 to 254 bytes.

Command Modes

Class map SIP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

You can configure the ACE to validate the length of SIP URIs or Tel URIs. A SIP URI is a user identifier that a calling party (source) uses to contact the called party (destination). A Tel URI is a telephone number that identifies the endpoint of a SIP connection. For more information about SIP URIs and Tel URIs, see RFC 2534 and RFC 3966, respectively.

Examples

To instruct the ACE to filter traffic based on SIP URIs, enter:

```
host1/Admin(config-cmap-sip-insp)# match uri sip length gt 100
```

To remove the match statement from the class map, enter:

```
host1/Admin(config-cmap-sip-insp)# no match uri sip length gt 100
```

Related Commands

(config-cmap-sip-insp) match called-party
(config-cmap-sip-insp) match calling-party
(config-cmap-sip-insp) match content
(config-cmap-sip-insp) match im-subscriber
(config-cmap-sip-insp) match message-path
(config-cmap-sip-insp) match request-method
(config-cmap-sip-insp) match third-party registration

Class Map SIP Load Balancing Configuration Mode Commands

Class map SIP load balancing configuration mode commands allow you to create a Layer 7 SIP server load-balancing class map. To create a SIP load-balancing class map and access class map SIP load balancing configuration mode, use the **class-map type sip loadbalance** command. The prompt changes to (config-cmap-sip-lb). Use the **no** form of this command to remove a SIP load-balancing class map from the configuration.

class-map type sip loadbalance [**match-all** | **match-any**] *map_name*

no class-map type sip loadbalance [**match-all** | **match-any**] *map_name*

Syntax Description

match-all | **match-any**	(Optional) Determines how the ACE evaluates SIP network traffic when multiple match criteria exist in a class map. • **match-all**—(Default) Network traffic needs to satisfy all of the match criteria (implicit AND) to match the SIP load-balancing class map. • **match-any**—Network traffic needs to satisfy only one of the match criteria (implicit OR) to match the SIP load-balancing class map.
map_name	Unique identifier assigned to the SIP load-balancing class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To create a class map named SIP_L7_CLASS, enter:

```
host1/Admin(config)# class-map type sip loadbalance match-any SIP_L7_CLASS
host1/Admin(config-cmap-sip-lb)#
```

To remove the SIP load-balancing class map from the configuration, enter:

```
host1/Admin(config)# no class-map type sip loadbalance match-any SIP_L7_CLASS
```

Related Commands

(config) class-map
(config-cmap-sip-lb) description

(config-cmap-sip-lb) description

To provide a brief description of the SIP load-balancing class map, use the **description** command. Use the **no** form of this command to remove the description from the class map.

description *text*

no description

Syntax Description

text	Description of the class map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Class map SIP load balancing configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description for the SIP load-balancing class map, enter:

```
host1/Admin(config)# class-map type sip loadbalance match-any SIP_L7_CLASS
host1/Admin(config-cmap-sip-lb)# description SIP CLASS MAP
```

To remove the description from a SIP load-balancing class map, enter:

```
host1/Admin(config-cmap-sip-lb)# no description
```

Related Commands

This command has no related commands.

(config-cmap-sip-lb) match class-map

The nesting of class maps allows you to achieve complex logical expressions for Layer 7 server load balancing. To identify one SIP load-balancing class map as a matching criterion for another SIP load-balancing class map, use the **match class-map** command. Use the **no** form of this command to remove the nested class map from a SIP load-balancing class map.

[*line_number*] **match class-map** *name*

no [*line_number*] **match class-map** *name*

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. For example, you can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate any priority for the match statements. Enter a unique integer from 2 to 1024.
name	Name of an existing SIP load-balancing class map.

Command Modes

Class map SIP load balancing configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The **match class-map** command allows you to combine the use of the **match-any** and **match-all** keywords in the same class map. To combine **match-all** and **match-any** characteristics in a class map, create a class map that uses one **match** command (either **match-any** or **match-all**) and then use this class map as a match statement in a second class map that uses the other match type.

The ACE restricts the nesting of class maps to two levels to prevent you from including a nested class map under another class map.

Examples

To combine the characteristics of two class maps, one with **match-any** and one with **match-all** characteristics, into a single class map, enter:

```
host1/Admin(config)# class-map type sip loadbalance match-any CLASS3
host1/Admin(config-cmap-sip-lb)# 200 match sip header Host header-value XYZ
host1/Admin(config-cmap-sip-lb)# exit

host1/Admin(config)# class-map type sip loadbalance match-all CLASS4
host1/Admin(config-cmap-sip-lb)# 10 match class-map CLASS3
host1/Admin(config-cmap-sip-lb)# 20 match source-address 192.168.11.2
host1/Admin(config-cmap-sip-lb)# exit
```

To remove the nested class map from the SIP class map, enter:

```
host1/Admin(config)# class-map type sip loadbalance match-all CLASS4
host1/Admin(config-cmap-sip-lb)# no 10
```

Related Commands (config-cmap-sip-lb) description

(config-cmap-sip-lb) match sip header

To configure a class map to make SIP SLB decisions based on the name and value of a SIP header, use the **match sip header** command. Use the **no** form of this command to remove a SIP header match statement from the SIP load-balancing class map.

[*line_number*] **match sip header** *name* **header-value** *expression*

no [*line_number*] **match sip header** *name* **header-value** *expression*

Syntax Description

line_number	(Optional) Line number that you can use to edit or delete individual **match** commands. For example, you can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate any priority for the match statements. Enter a unique integer from 2 to 1024.
name	Name of the field in the SIP header. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. You can enter a text string with spaces provided that you enclose the entire string in quotation marks (“ ”). You can enter any header field name, including a standard SIP header field name or any user-defined header field name. For a list of standard SIP header field names, see Table 2-7. Because SIP is similar to HTTP/1.1, you can use any HTTP header listed in Table 2-6 if the SIP server supports it. For a complete list of SIP headers, see RFC 3261.
header-value *expression*	Header value expression string to compare against the value in the specified field in the SIP header. Enter a text string with a maximum of 255 alphanumeric characters. The ACE supports the use of regular expressions for header matching. Expressions are stored in a header map in the form *header-name: expression*. Header expressions allow spaces if the entire string that contains spaces is quoted. If you use a **match-all** class map, all headers in the header map must be matched. For a list of the supported characters that you can use in regular expressions, see Table 2-5.

Command Modes

Class map SIP load balancing configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The ACE can perform regular expression matching against the received packet data from a particular connection based on the SIP header expression. You can configure a maximum of nine SIP header field names per class map (the ACE always parses Call-ID).

When the ACE receives a SIP session request, the load-balancing decision is based on the first request message. All subsequent request and response message exchanges (with the same Call-ID) are forwarded to the same server. For this reason, when you configure header match criteria, ensure that the header is included in the first request message.

Table 2-7 lists the standard SIP header fields.

Table 2-7 Standard SIP Header Fields

Field Name	Description
Call-ID	Unique identifier that groups together a series of messages in a call.
Contact	SIP URI that can be used to contact the user agent.
From	Initiator of the SIP request, the source.
To	Desired recipient of the SIP request, the destination.
Via	Transport used for the transaction and where the response should be sent.

Examples

To configure a SIP load-balancing class map to load balance based on a SIP header named Session, enter:

```
host1/Admin(config)# class-map type sip loadbalance match-any L7SLBCLASS
host1/Admin(config-cmap-sip-lb)# 10 match sip header Session header-value abc123
```

To configure a SIP load-balancing class map to load balance based on a SIP header named Via, enter:

```
host1/Admin(config)# class-map type sip loadbalance match-any L7SLBCLASS
host1/Admin(config-cmap-sip-lb)# 20 match sip header Via header-value 192.*
```

To configure a SIP load-balancing class map to emulate a wildcard search to match the header value expression string, enter:

```
host1/Admin(config)# class-map type sip loadbalance match-any L7SLBCLASS
host1/Admin(config-cmap-sip-lb)# 30 match sip header To header-value .*@cisco.com
host1/Admin(config-cmap-sip-lb)# 40 match sip header To header-value .*@linksys.com
```

To remove SIP header match criteria from the L7SLBCLASS class map, enter:

```
host1/Admin(config-cmap-sip-lb)# no 10
host1/Admin(config-cmap-sip-lb)# no 20
```

Related Commands

(config-cmap-sip-lb) description

(config-cmap-sip-lb) match source-address

To configure the class map to make SIP SLB decisions based on a client source IP address, use the **match source-address** command. Use the **no** form of this command to remove the source IP address match statement from the class map.

[*line_number*] **match source-address** *ip_address* [*netmask*]

no [*line_number*] **match source-address** *ip_address* [*netmask*]

Syntax Description

line_number	(Optional) Line number that you can use to edit or delete individual **match** commands. For example, you can enter **no** *line_number* to delete long **match** commands instead of entering the entire line. The line numbers do not indicate any priority for the match statements. Enter a unique integer from 2 to 1024.
ip_address	Source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.2).
netmask	(Optional) Subnet mask of the IP address. Enter the netmask in dotted-decimal notation (for example, 255.255.255.0). The default is 255.255.255.255.

Command Modes

Class map SIP load balancing configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To specify that the SIP load-balancing class map match on source IP address 192.168.11.2 255.255.255.0, enter:

```
host1/Admin(config)# class-map type sip loadbalance match-any L7SLBCLASS
host1/Admin(config-cmap-sip-lb)# 50 match source-address 192.168.11.2 255.255.255.0
```

To remove the source IP address match statement from the class map, enter:

```
host1/Admin(config-cmap-sip-lb)# no 50
```

Related Commands

(config-cmap-sip-lb) description

Context Configuration Mode Commands

Context configuration mode commands allow you to configure attributes of virtual contexts. Each context that you create behaves like an independent device with its own policies, interfaces, domains, server farms, real servers, and administrators.

Each context, including the Admin context, has its own configuration file and local user database that are stored in the local disk partition in flash memory or that can be downloaded from an FTP, TFTP, or HTTP(S) server. The startup-config for each context is stored as the startup configuration file in flash memory.

In the Admin context, use the **changeto** command in Exec mode or the **do changeto** command in any configuration mode to move between contexts. Only users authenticated in the Admin context can use the **changeto** command. Other users that are authorized for more than one context must explicitly log in to each context.

To create a context and access context configuration mode, use the **context** command in configuration mode. The CLI prompt changes to (config-context). For information about the commands in context configuration mode, see the commands in this section.

Use the **no** form of this command to remove a context from the configuration.

context *name*

no context *name*

Syntax Description

name	Unique identifier of a virtual context. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

All commands in this mode require the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To create a context named C1 and access context configuration mode, enter:

```
host1/Admin(config)# context C1
host1/Admin(config-context)#
```

To delete the C1 context, enter:

```
host1/Admin(config)# no context C1
```

Related Commands

show context
show running-config

(config-context) allocate-interface

To assign one or more VLAN interfaces to the context, use the **allocate-interface** command. Use the **no** form of this command to remove the VLAN from the context configuration.

allocate-interface vlan *number_id*

no allocate-interface vlan *number_id*

Syntax Description

vlan *number_id*	Identifies the VLAN to assign to the user context. For the *number_id* argument, enter the number of an existing VLAN that you want to assign to the context as an integer from 2 to 4094.

Command Modes

Context configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

After you allocate the interface to a user context, you can configure the interface in that context.

When a VLAN is shared in multiple contexts, the interfaces must be on the same subnet. However, the interfaces that share the VLANs will have different MAC addresses. These different MAC addresses on the same VLAN classify traffic on multiple contexts. No routing can occur across contexts even if you configure shared VLANs.

The ACE allows you to configure one or more VLAN interfaces in any user context before you assign those VLAN interfaces to the associated user contexts through the **allocate-interface vlan** command in the Admin context. For more information about assigning interfaces to the ACE, see the *Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*.

You cannot deallocate a VLAN from a user context if the VLAN is currently in use on that context.

Examples

To allocate the VLAN interface identified as 100 to the currently active context, enter:

```
host1/Admin(config-context)# allocate-interface vlan 100
```

Related Commands

show context
(config) interface

(config-context) description

To enter a description for a user context, use the **description** command. Use the **no** form of this command to remove the context description from the configuration.

description *text*

no description

Syntax Description

text	Description for the user context. Enter a description as an unquoted text string with a maximum of 240 characters.

Command Modes

Context configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To provide a description of a user context, enter:

```
host1/Admin(config-context)# description context for accounting users
```

Related Commands

show context

(config-context) member

To associate a context with a resource class, use the **member** command. Use the **no** form of this command to remove a context from a resource class.

member *class*

no member *class*

Syntax Description

class	Name of an existing resource class. Enter the class name as an unquoted text string with a maximum of 64 alphanumeric characters.

Command Modes

Context configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You can associate a context with only one resource class. If you do not explicitly associate a context with a resource class, the ACE associates the context with the default resource class.

Examples

To disassociate a context from a resource class, enter:

```
host1/Admin(config-context)# no member RC1
```

Related Commands

show context
(config) resource-class

CSR Parameters Configuration Mode Commands

CSR parameters configuration mode commands allow you to define the distinguished name attributes for a Certificate Signing Request (CSR) parameter set. The ACE applies the CSR parameter set attributes during the CSR-generating process. The distinguished name attributes provide the Certificate Authority (CA) with the information that it needs to authenticate your site. The CA then applies the information that you provide in the CSR parameter set to your Secure Sockets Layer (SSL) certificate. Creating a CSR parameter set allows you to generate multiple CSRs with the same distinguished name attributes.

To create a new CSR parameter set (or modify an existing CSR parameter set) and access the CSR parameters configuration mode, use the **crypto csr-params** command. The CLI prompt changes to (config-csr-params). Use the **no** form of this command to remove an existing CSR parameter set.

crypto csr-params *csr_param_name*

no crypto csr-params *csr_param_name*

Syntax Description

csr_param_name	Name that designates a CSR parameter set. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the SSL feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

When you specify a CSR parameter set, you define the following distinguished name attributes:

- Common name—See the **(config-csr-params) common-name** command. This distinguished name attribute is required.
- Country name—See the **(config-csr-params) country** command. This distinguished name attribute is required.
- E-mail address—See the **(config-csr-params) email** command.
- Locality—See the **(config-csr-params) locality** command.
- Organization name (certificate subject)—See the **(config-csr-params) organization-name** command.
- Organization unit—See the **(config-csr-params) organization-unit** command.
- Serial number—See the **(config-csr-params) serial-number** command. This distinguished name attribute is required.
- State—See the **(config-csr-params) state** command. This distinguished name attribute is required.

If you do not define the required distinguished name attributes, the ACE displays an error message when you attempt top generate a CSR using the CSR parameter set.

You can create up to eight CSR parameter sets per context.

To generate a Certificate Signing Request (CSR) file using the CSR parameter set, use the **crypto generate csr** command in the Exec mode.

Examples

To create the CSR parameter set CSR_PARAMS_1, enter:

```
host1/Admin(config)# crypto csr-params CSR_PARAMS_1
host1/Admin(config-csr-params)
```

Related Commands

crypto generate csr
(config-csr-params) common-name
(config-csr-params) country
(config-csr-params) email
(config-csr-params) locality
(config-csr-params) organization-name
(config-csr-params) organization-unit
(config-csr-params) serial-number
(config-csr-params) state

(config-csr-params) common-name

To define the common name parameter in the Certificate Signing Request (CSR) parameter set, use the **common-name** command. Use the **no** form of this command to delete an existing common name from the CSR parameter set.

common-name *name*

no common-name

Syntax Description

name	Name that designates the common name in a CSR parameter set. Enter the common name as an unquoted alphanumeric string with no spaces or a quoted string with spaces and a maximum of 64 characters.

Command Modes

CSR parameters configuration mode

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The common name is a required distinguished name attribute. If you do not configure this attribute (and all other required attributes), the ACE displays an error message when you try to generate a CSR using the CSR parameter set.

The common name should be the domain name or individual hostname of the Secure Sockets Layer (SSL) site.

Examples

To specify the common name WWW.ABC123.COM, enter:

```
host1/Admin(config-csr-params)# common-name WWW.ABS123.COM
```

Related Commands

(config) crypto csr-params
(config-csr-params) country
(config-csr-params) email
(config-csr-params) locality
(config-csr-params) organization-name
(config-csr-params) organization-unit
(config-csr-params) serial-number
(config-csr-params) state

(config-csr-params) country

To define the country name parameter in the Certificate Signing Request (CSR) parameter set, use the **country** command. Use the **no** form of this command to delete an existing country name from the CSR parameter set.

country *name*

no country

Syntax Description

name	Name of the country where the Secure Sockets Layer (SSL) site resides. Enter the country name as an alphanumeric string from 1 to 2 characters.

Command Modes

CSR parameters configuration mode

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The country name is a required distinguished name attribute. If you do not configure this attribute (and all other required attributes), the ACE displays an error message when you try to generate a CSR using the CSR parameter set.

Examples

To specify the country US (United States), enter:

```
host1/Admin(config-csr-params)# country US
```

Related Commands

(config) crypto csr-params
(config-csr-params) common-name
(config-csr-params) email
(config-csr-params) locality
(config-csr-params) organization-name
(config-csr-params) organization-unit
(config-csr-params) serial-number
(config-csr-params) state

(config-csr-params) email

To define the e-mail address parameter in the Certificate Signing Request (CSR) parameter set, use the **email** command. Use the **no** form of this command to delete an existing e-mail address from the CSR parameter set.

email *address*

no email

Syntax Description

address	Address that designates the site e-mail address in a CSR parameter set. Enter an unquoted text string with no spaces and a maximum of 40 alphanumeric characters.

Command Modes

CSR parameters configuration mode

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The e-mail address is an optional distinguished name attribute.

Examples

To specify the e-mail address WEBADMIN@ABC123.COM, enter:

```
host1/Admin(config-csr-params)# email WEBADMIN@ABC123.COM
```

Related Commands

(config) crypto csr-params
(config-csr-params) common-name
(config-csr-params) country
(config-csr-params) locality
(config-csr-params) organization-name
(config-csr-params) organization-unit
(config-csr-params) serial-number
(config-csr-params) state

(config-csr-params) locality

To define the locality name parameter in the Certificate Signing Request (CSR) parameter set, use the **locality** command. Use the **no** form of this command to delete an existing locality from the CSR parameter set.

locality *name*

no locality

Syntax Description

name	Name that designates the locality (a county, for example) in a CSR parameter set. Enter an unquoted text string with a maximum of 40 alphanumeric characters including spaces.

Command Modes

CSR parameters configuration mode

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The locality name is an optional distinguished name attribute.

Examples

To specify the locality ATHENS, enter:

```
host1/Admin(config-csr-params)# locality ATHENS
```

Related Commands

(config) crypto csr-params
(config-csr-params) common-name
(config-csr-params) country
(config-csr-params) email
(config-csr-params) organization-name
(config-csr-params) organization-unit
(config-csr-params) serial-number
(config-csr-params) state

(config-csr-params) organization-name

To define the organization name parameter in the Certificate Signing Request (CSR) parameter set, use the **organization-name** command. Use the **no** form of this command to delete an existing organization name from the CSR parameter set.

organization-name *name*

no organization-name

Syntax Description

name	Name that designates the organization in a CSR parameter set. Enter the organization name as an unquoted alphanumeric string with a maximum of 64 characters including spaces.

Command Modes

CSR parameters configuration mode

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The organization name is an optional distinguished name attribute.

Examples

To specify the organization ABC123 SYSTEMS INC, enter:

```
host1/Admin(config-csr-params)# organization-name ABC123 SYSTEMS INC
```

Related Commands

(config) crypto csr-params
(config-csr-params) common-name
(config-csr-params) country
(config-csr-params) email
(config-csr-params) locality
(config-csr-params) organization-unit
(config-csr-params) serial-number
(config-csr-params) state

(config-csr-params) organization-unit

To define the organization unit parameter in the Certificate Signing Request (CSR) parameter set, use the **organization-unit** command. Use the **no** form of this command to delete an existing organization unit from the CSR parameter set.

organization-unit *unit*

no organization-unit

Syntax Description

unit	Name that designates the unit (within an organization) in a CSR configuration file. Enter the organization unit as an unquoted alphanumeric string with a maximum of 64 characters including spaces.

Command Modes

CSR parameters configuration mode

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The organization unit is an optional distinguished name attribute.

Examples

To specify the organization unit SSL ACCELERATOR, enter:

```
host1/Admin(config-csr-params)# organization-unit SSL ACCELERATOR
```

Related Commands

(config) crypto csr-params
(config-csr-params) common-name
(config-csr-params) country
(config-csr-params) email
(config-csr-params) locality
(config-csr-params) organization-name
(config-csr-params) serial-number
(config-csr-params) state

(config-csr-params) serial-number

To define the serial number parameter in the Certificate Signing Request (CSR) parameter set, use the **serial-number** command. Use the **no** form of this command to delete an existing serial number from the CSR parameter set.

serial-number *number*

no serial-number

Syntax Description

number	Number that designates the serial number in a CSR parameter set. Enter the serial number as an alphanumeric string from 1 to 16 characters.

Command Modes

CSR parameters configuration mode

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The serial number is a required distinguished name attribute. If you do not configure this attribute (and all other required attributes), the ACE displays an error message when you try to generate a CSR using the CSR parameter set.

The CA may choose to overwrite the serial number that you provide with its own serial number.

Examples

To specify the serial number 1001, enter:

```
(config-csr-params)# serial-number 1001
```

Related Commands

(config) crypto csr-params
(config-csr-params) common-name
(config-csr-params) country
(config-csr-params) email
(config-csr-params) locality
(config-csr-params) organization-name
(config-csr-params) organization-unit
(config-csr-params) state

(config-csr-params) state

To define the state name parameter in the Certificate Signing Request (CSR) parameter set, use the **state** command. Use the **no** form of this command to delete an existing state name from the CSR parameter set.

state *name*

no state

Syntax Description

name	Name that designates the state or province in a CSR configuration file. Enter an unquoted text string with a maximum of 40 alphanumeric characters including spaces.

Command Modes

CSR parameters configuration mode

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The state name is a required distinguished name attribute. If you do not configure this attribute (and all other required attributes), the ACE displays an error message when you try to generate a CSR using the CSR parameter set.

Examples

To specify the state GA (Georgia), enter:

```
host1/Admin(config-csr-params)# state GA
```

Related Commands

(config) crypto csr-params
(config-csr-params) common-name
(config-csr-params) country
(config-csr-params) email
(config-csr-params) locality
(config-csr-params) organization-name
(config-csr-params) organization-unit
(config-csr-params) serial-number

Domain Configuration Mode Commands

Domain configuration mode commands allow you to determine a user's domain (namespace in which the user operates). To create a domain and access domain configuration mode, use the **domain** command in configuration mode. The CLI prompt changes to (config-domain). For information about the commands in domain configuration mode, see the commands in this section.

Use the **no** form of this command to remove a domain from the configuration.

domain *name*

no domain *name*

Syntax Description

name	Unique identifier of a domain in a context. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

All commands in this mode require the context Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

A domain does not restrict the context configuration that you can display using the **show running-config** command. You can still display the running configuration for the entire context. However, you can restrict your access to the configurable objects within a context by adding to the domain only a limited subset of all the objects available to a context. To limit a user's ability to manipulate the objects in a domain, you can assign a role to that user. For more information about domains and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can configure KAL-AP TAGs as domains. For the domain load calculation, the ACE considers the Layer 3 class map, server farm, and real server objects. All other objects under the domain are ignored during the calculation.

Examples

To create a domain named D1 and access domain configuration mode, enter:

```
host1/Admin(config)# domain D1
host1/Admin(config-domain)#
```

To delete the D1 domain, enter:

```
host1/Admin(config)# no domain D1
```

Related Commands

show domain
show running-config

(config-domain) add-object

To associate a configuration object with a domain, use the **add-object** command. Use the **no** form of this command to remove an object added to the domain.

add-object {**access-list** {**ethertype** | **extended**} *name* | **action-list** *name* | **all** | **class-map** *name* | **interface** {**bvi** *number* | **vlan** *number*} | **object-group** *name* | **parameter-map** *name* | **policy-map** *name* | **probe** *name* | **rserver** *name* | **script** *name* | **serverfarm** *name* | **sticky** *name*}

no add-object {**access-list** {**ethertype** | **extended**} *name* | **action-list** *name* | **all** | **class-map** *name* | **interface** {**bvi** *number* | **vlan** *number*} | **object-group** *name* | **parameter-map** *name* | **policy-map** *name* | **probe** *name* | **rserver** *name* | **script** *name* | **serverfarm** *name* | **sticky** *name*}

Syntax Description

access-list *name*	Specifies an existing access control list that you want to associate with the domain.
ethertype	Specifies an existing EtherType access control list that you want to associate with the domain.
extended	Specifies an existing extended access control list that you want to associate with the domain.
action-list *name*	Specifies an existing action list that you want to associate with the domain.
all	Specifies that all configuration objects in the context are added to the domain.
class-map *name*	Specifies an existing class map for flow classification that you want to associate with the domain.
interface	Specifies an existing interface—either a Bridge Group Virtual Interface or a VLAN—that you want to associate with the domain.
bvi *number*	Specifies the existing Bridge Group Virtual Interface that you want to associate with the domain. Enter an integer from 1 to 4094.
vlan *number*	Specifies the existing VLAN that you want to associate with the domain. Enter an integer from 2 to 4094.
object-group *name*	Specifies an existing object group that you want to associate with the domain.
parameter-map *name*	Specifies an existing parameter map that you want to associate with the domain.
policy-map *name*	Specifies an existing policy map that you want to associate with the domain.
probe *name*	Specifies an existing real server probe (keepalive) that you want to associate with the domain.
rserver *name*	Specifies an existing real server that you want to associate with the domain.
script *name*	Specifies an existing script file (created with the ACE TCL scripting language) that you want to associate with the domain.
serverfarm *name*	Specifies an existing server farm that you want to associate with the domain.
sticky *name*	Specifies an existing sticky group that you want to associate with the domain to maintain persistence with a server.
name	Identifier of the specified object. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Domain configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To associate an interface called VLAN 10 with a domain, enter:

```
host1/Admin(config-domain)# add-object interface vlan 10
```

Related Commands

show domain

FT Group Configuration Mode Commands

FT group configuration mode commands allow you to configure fault-tolerant (FT) groups that consist of two contexts, each residing on a different ACE. FT groups are part of the ACE redundancy feature. For details about redundancy, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To create an FT group and access the FT group configuration mode, use the **ft group** command in configuration mode. The CLI prompt changes to (config-ft-group). For information about the commands in FT group configuration mode, see the commands in this section.

Use the **no** form of this command to remove an FT group from the configuration.

ft group *group_id*

no ft group *group_id*

Syntax Description

group_id	Unique identifier of an FT group. Enter an integer from 1 to 255.

Command Modes

Configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

All commands in this mode require the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To create an FT group with a group ID of 1 and access ft-group configuration mode, enter:

```
host1/Admin(config)# ft group 1
host1/Admin(config-ft-group)#
```

To delete the FT group, enter:

```
host1/Admin(config)# no ft group 1
```

Related Commands

show ft
show running-config

(config-ft-group) associate-context

To associate a context with a fault-tolerant (FT) group, use the **associate-context** command. You need to make this association for each of the two redundant contexts in an FT group. Use the **no** form of this command to remove a context from an FT group.

associate-context *name*

no associate-context *name*

Syntax Description

name	Identifier of the context that you want to associate with the FT group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

FT group configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Before you can remove a context from an FT group, you must first take the group out of service using the **no inservice** command. See the **(config-ft-group) inservice** command.

Examples

To associate a context with an FT group, enter:

```
host1/Admin(config-ft-group)# associate-context C1
```

Related Commands

show ft
(config) context

(config-ft-group) inservice

To place a fault-tolerant (FT) group in service, use the **inservice** command. Use the **no** form of this command to take the FT group out of service.

inservice

no inservice

Syntax Description

This command has no keywords or arguments.

Command Modes

FT group configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Before you place an FT group in service, be sure that you have associated one or two contexts with the FT group and properly configured the two peers.

Examples

To place an FT group in service, enter:

```
host1/Admin(config-ft-group)# inservice
```

Related Commands

This command has no related commands.

(config-ft-group) peer

To associate a peer ACE with a fault-tolerant (FT) group, use the **peer** command. Use the **no** form of this command to remove the peer association with the FT group.

peer *peer_id*

no peer *peer_id*

Syntax Description

peer_id	Identifier of an existing peer appliance. Enter 1 for the peer ID.

Command Modes

FT group configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The peer designation is used to denote the remote standby member of the FT group. A context in a redundant configuration can have only one peer context.

Examples

To associate a peer appliance with an FT group, enter:

```
host1/Admin(config-ft-group)# peer 1
```

Related Commands

show ft
(config) ft peer

(config-ft-group) peer priority

To configure the priority of a fault-tolerant (FT) group on the remote standby member, use the **peer priority** command. Use the **no** form of this command to restore the default priority of 100.

peer priority *number*

no peer priority *number*

Syntax Description

number	Priority of the FT group on the standby member. Enter an integer from 1 to 255. The default is 100.

Command Modes

FT group configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Configure a lower priority on the FT group member (context) that you want as the standby member.

Examples

To configure the priority of the FT group on the standby appliance with a value of 50, enter:

```
host1/Admin(config-ft-group)# peer priority 50
```

Related Commands

(config-ft-group) peer
(config-ft-group) preempt

(config-ft-group) preempt

To configure preemption after it has been disabled, use the **preempt** command. Use the **no** form of this command to disable preemption.

preempt

no preempt

Syntax Description

This command has no keywords or arguments.

Command Modes

FT group configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Preemption ensures that the group member with the higher priority always asserts itself and becomes the active member. By default, preemption is enabled.

If you disable preemption and a member with a higher priority is found after the other member has become active, the newly elected member becomes the standby member even though it has a higher priority.

Examples

To reenable preemption after its default setting was disabled, enter:

```
host1/Admin(config-ft-group)# preempt
```

Related Commands

show ft
(config-ft-group) priority

(config-ft-group) priority

To configure the priority of the active group member, use the **priority** command. Use the **no** form of this command to restore the default priority of 100.

priority *number*

no priority *number*

Syntax Description

number	Priority number for the active group member. Enter an integer from 1 to 255. The default is 100.

Command Modes

FT group configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You must configure the priority of a group on both peer appliances. Configure a higher priority for the group on the appliance where you want the active member to initially reside.

Examples

To set the priority of the FT group on the active member to a value of 150, enter:

```
host1/Admin(config-ft-group)# priority 150
```

Related Commands

show ft
(config-ft-group) preempt

FT Interface Configuration Mode Commands

FT interface configuration mode commands allows you to configure redundancy parameters for the fault-tolerant (FT) VLAN. The FT VLAN is a dedicated interface that the ACE uses exclusively for redundancy traffic (such as heartbeat, state, and replication packets). For more information about configuring redundancy on the ACE, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

To create an FT VLAN and access FT interface configuration mode, use the **ft interface vlan** command in configuration mode. The CLI prompt changes to (config-ft-intf). For information about the commands in FT interface configuration mode, see the following commands.

Use the **no** form of this command to remove an FT VLAN from the redundancy configuration.

ft interface vlan *vlan_id*

no ft interface vlan *vlan_id*

Syntax Description

vlan_id	Identifier of an existing VLAN that you want to use as the FT VLAN. Enter an integer from 2 to 4094.

Command Modes

Configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

All commands in this mode require the System feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To remove an FT VLAN from the redundancy configuration, first dissociate it from the FT peer using the **no** form of the **(config-ft-peer) ft-interface vlan** command and then enter the **no ft interface vlan** command in configuration mode.

Examples

To configure an FT VLAN and access FT group configuration mode, enter:

```
host1/Admin(config)# ft interface vlan 4000
host1/Admin(config-ft-intf)#
```

To delete the FT VLAN configuration, enter:

```
host1/Admin(config)# no ft interface vlan 4000
```

Related Commands

show ft
show interface
show running-config
(config-ft-peer) ft-interface vlan

(config-ft-intf) ip

To assign an IP address to the fault-tolerant (FT) VLAN, use the **ip** command. Use the **no** form of this command to remove the IP address from the configuration.

ip address *ip_address netmask*

no ip address *ip_address netmask*

Syntax Description

address *ip_address*	Specifies the IP address of the FT VLAN. Enter an IP address in dotted-decimal notation (for example, 192.168.12.1).
netmask	Subnet mask of the FT VLAN. Enter a subnet mask in dotted-decimal notation (for example, 255.255.255.0).

Command Modes

FT interface configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To configure an IP address for the FT VLAN, enter:

```
host1/Admin(config-ft-intf)# ip address 192.168.12.1 255.255.255.0
```

To remove an IP address from the FT VLAN, enter:

```
host1/Admin(config-ft-intf)# no ip address
```

Related Commands

show ft
show interface
(config-ft-intf) peer ip

(config-ft-intf) peer ip

To allow the local member of the fault-tolerant (FT) group to communicate with the remote peer, use the **peer ip** command to configure an IP address for the remote peer. Use the **no** form of this command to remove the IP address from the peer configuration.

peer ip address *ip_address netmask*

no peer ip address *ip_address netmask*

Syntax Description

address *ip_address*	Specifies the IP address of the remote peer. Enter an IP address in dotted-decimal notation (for example, 192.168.12.15).
netmask	Subnet mask of the remote peer. Enter a subnet mask in dotted-decimal notation (for example, 255.255.255.0).

Command Modes

FT interface configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To configure an IP address for the remote peer, enter:

```
host1/Admin(config-ft-intf)# peer ip address 192.168.12.15 255.255.255.0
```

To remove the IP address from the remote peer, enter:

```
host1/Admin(config-ft-intf)# no peer ip address 192.168.12.15 255.255.255.0
```

Related Commands

show interface
(config-ft-intf) ip

(config-ft-intf) shutdown

To disable the fault-tolerant (FT) VLAN, use the **shutdown** command. Use the **no** form of this command to enable the FT VLAN.

shutdown

no shutdown

Syntax Description

This command has no keywords or arguments.

Command Modes

FT interface configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When you create the FT VLAN, it is disabled by default. Use the **no** form of this command to enable the FT VLAN.

Examples

For example, to enable the FT VLAN, enter:

```
host1/Admin(config-ft-intf)# no shutdown
```

To disable the FT VLAN after you have enabled it, enter:

```
host1/Admin(config-ft-intf)# shutdown
```

Related Commands

show interface

FT Peer Configuration Mode Commands

Fault-tolerant (FT) peer configuration mode commands allow you to configure redundancy parameters for peer (standby) appliances. Each FT group in a redundant configuration consists of two ACE appliances: a local active appliance and a remote standby appliance or peer.

To configure an FT peer and access FT peer configuration mode, use the **ft peer** command in configuration mode. The CLI prompt changes to (config-ft-peer). For information about the commands in FT peer configuration mode, see the following commands.

Use the **no** form of this command to remove an FT group from the configuration.

ft peer *peer_id*

no ft peer *peer_id*

Syntax Description

peer_id	Unique identifier of the FT peer. Enter 1.

Command Modes

Configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

All commands in this mode require the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To configure an FT peer and access FT peer configuration mode, enter:

```
host1/Admin(config)# ft peer 1
host1/Admin(config-ft-peer)#
```

To delete the FT peer configuration, enter:

```
host1/Admin(config)# no ft peer 1
```

Related Commands

show ft
show running-config

(config-ft-peer) ft-interface vlan

To associate an existing fault-tolerant (FT) VLAN with a peer, use the **ft-interface vlan** command. Use the **no** form of this command to remove the FT VLAN from the peer configuration.

ft-interface vlan *vlan_id*

no ft-interface vlan *vlan_id*

Syntax Description

vlan_id	Identifier of an existing VLAN. Enter an integer from 2 to 4094.

Command Modes

FT peer configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To associate an existing FT VLAN with a peer, enter:

```
host1/Admin(config-ft-peer)# ft-interface vlan 200
```

Related Commands

show ft
(config) ft interface vlan

(config-ft-peer) heartbeat

To configure the heartbeat interval and count for verification timing between active and standby fault-tolerant (FT) peers, use the **heartbeat** command. Use the **no** form of this command to revert to the default heartbeat interval and count.

heartbeat {**count** *number* | **interval** *frequency*}

no heartbeat {**count** *number* | **interval** *frequency*}

Syntax Description

count *number*	Specifies the number of heartbeat intervals that must transpire with no heartbeat packet received by the standby member before the standby member determines that the active member is not available. Enter an integer from 10 to 50. The default is 10 heartbeat intervals.
interval *frequency*	Specifies the time period between heartbeats in milliseconds (ms). Enter an integer from 100 to 1000 ms. The default is 300 ms.

Command Modes

FT peer configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

If the standby member of the FT group does not receive a heartbeat packet from the active member, a time period equal to **count** *number* times **interval** *frequency* must elapse before a switchover between the active and standby members can occur.

Examples

To set a heartbeat count of 20, enter:

```
host1/Admin(config-ft-peer)# heartbeat count 20
```

To set a heartbeat interval of 200 milliseconds, enter:

```
host1/Admin(config-ft-peer)# heartbeat interval 200
```

Related Commands

show ft

(config-ft-peer) query-interface

To configure an alternate interface to allow the standby member to determine whether the active member is down or whether there is a connectivity problem with the fault-tolerant (FT) VLAN, use the **query-interface** command. A query interface helps prevent two redundant contexts from becoming active at the same time for the same FT group. Use the **no** form of this command to remove the query interface from the peer configuration.

query-interface vlan *vlan_id*

no query-interface vlan *vlan_id*

Syntax Description

vlan *vlan_id*	Specifies the identifier of an existing VLAN. Enter an integer from 2 to 4094.

Command Modes

FT peer configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Configuring a query interface allows you to assess the health of the active FT group member, but it increases failover time. You cannot delete a query interface if it is associated with a peer. You must dissociate the interface from the peer first, and then you can delete the query interface.

Examples

To configure a query interface, enter:

```
host1/Admin(config-ft-peer)# query-interface vlan 400
```

Related Commands

show ft
(config) ft interface vlan

FT Track Host Configuration Mode Commands

Fault-tolerant (FT) track host configuration mode commands allow you to configure tracking and failure detection for critical network gateways and hosts.

To create a process that tracks and detects failures for a gateway or host and accesses FT track host configuration mode, use the **ft track host** command in configuration mode. The CLI prompt changes to (config-ft-track-host). For information about the commands in FT track host configuration mode, see the following commands.

Use the **no** form of this command to delete a process that tracks and detects failures for a gateway or host.

ft track host *name*

no ft track host *name*

Syntax Description

name	Unique identifier of the tracking process for a gateway or a host. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the fault-tolerant feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To create a process that tracks and detects failures for a gateway or host and accesses FT track host configuration mode, enter:

```
host1/Admin(config)# ft track host TRACK_GATEWAY1
host1/Admin(config-ft-track-host)#
```

To delete the process that tracks and detects failures for a gateway or host, enter:

```
host1/Admin(config)# no ft track host TRACK_GATEWAY1
```

Related Commands

show ft
show running-config

(config-ft-track-host) peer priority

To assign a priority for multiple probes on the standby member of a fault-tolerant (FT) group, use the **peer priority** command. Use the **no** form of this command to reset the multiple-probe priority to the default value of 10 on the standby member.

peer priority *number*

no peer priority *number*

Syntax Description

number	Priority of the probes configured for the gateway or host on the standby member. Enter a priority value as an integer from 0 to 255. The default is 0. Higher values indicate higher priorities.

Command Modes

FT track host configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The **peer** command keyword indicates the standby member of an FT group.

Assign a priority value to multiple probes based on the relative importance of the gateway or host that the probes are tracking. If all the probes go down, the ACE decrements the priority of the FT group on the standby member by the value of the *number* argument. If the priority of the FT group on the active member falls below the priority of the FT group on the standby member, a switchover occurs where the active member becomes the standby member and the standby member becomes the active member.

Examples

To assign a priority for multiple probes on the standby member of an FT group, enter:

```
host1/Admin(config-ft-track-host)# peer priority 50
```

To reset the priority of multiple probes on the standby member of an FT group to the default value of 0, enter:

```
host1/Admin(config-ft-track-host)# no peer priority 50
```

Related Commands

(config-ft-track-host) priority

(config-ft-track-host) peer probe

To associate an existing probe with a gateway or host for tracking by the standby member of a fault-tolerant (FT) group, use the **peer probe** command. Use the **no** form of this command to dissociate the tracking probe from the tracking process on the standby member.

peer probe *name* **priority** *number*

no peer probe *name* **priority** *number*

Syntax Description

name	Identifier of an existing probe that you want to associate with a gateway or host for tracking.
priority *number*	(Optional) Specifies the priority of the probe. Enter an integer from 0 to 255. The default is 0. Higher values indicate higher priorities.

Command Modes

FT track host configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The **peer** command keyword indicates the standby member of an FT group.

Assign a priority value to the probe based on the relative importance of the gateway or host that the probe is tracking. If the probe goes down, the ACE decrements the priority of the FT group on the standby member by the value of the *number* argument. If the priority of the FT group on the active member falls below the priority of the FT group on the standby member, a switchover occurs where the active member becomes the standby member and the standby member becomes the active member.

Examples

To configure a probe with priority of 15 on the standby member of an FT group, enter:

```
host1/Admin(config-ft-track-host)# peer probe TCP_PROBE1 priority 15
```

To remove the tracking probe from the standby member, enter:

```
host1/Admin(config-ft-track-host)# no peer probe TCP_PROBE1
```

Related Commands

show probe
show running-config
(config) ft peer
(config) probe
(config-ft-track-host) probe

(config-ft-track-host) peer track-host

To configure the IP address of the gateway or host that you want to track on the standby member of a fault-tolerant (FT) group, use the **peer track-host** command. Use the **no** form of this command to remove the IP address of the gateway or host from the tracking process on the standby member configuration.

peer track-host *ip_address*

no peer track-host *ip_address*

Syntax Description

ip_address	IP address of the gateway or host that you want the standby FT group member to track. Enter the IP address in dotted-decimal notation (for example, 172.16.27.1).

Command Modes

FT track host configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The **peer** command keyword indicates the standby member of an FT group.

Examples

To configure the IP address of a gateway for tracking on the standby member of an FT group, enter:

```
host1/Admin(config-ft-track-host)# peer track-host 172.16.27.1
```

To remove the IP address of the tracked gateway from the standby member, enter:

```
host1/Admin(config-ft-track-host)# no peer track-host 172.16.27.1
```

Related Commands

show running-config
(config) ft peer
(config-ft-track-host) track-host

(config-ft-track-host) priority

To assign a priority for multiple probes on the active member of a fault-tolerant (FT) group, use the **priority** command. Use the **no** form of this command to reset the multiple-probe priority to the default value of 10 on the active member.

priority *number*

no priority *number*

Syntax Description

number	Priority of the probes configured for the gateway or host on the active member. Enter a priority value as an integer from 0 to 255. The default is 0. Higher values indicate higher priorities.

Command Modes

FT track host configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Assign a priority value for multiple probes based on the relative importance of the gateway or host that the probes are tracking. If all the probes go down, the ACE decrements the priority of the FT group on the active member by the value of the *number* argument. If the priority of the FT group on the active member falls below the priority of the FT group on the standby member, a switchover occurs where the active member becomes the standby member and the standby member becomes the active member.

Examples

To assign a priority for multiple probes on the active member of an FT group, enter:

```
host1/Admin(config-ft-track-host)# priority 100
```

To reset the priority of multiple probes on the active member of an FT group to the default value of 0, enter:

```
host1/Admin(config-ft-track-host)# no priority 100
```

Related Commands

(config-ft-track-host) peer priority

(config-ft-track-host) probe

To associate an existing probe with a gateway or host for tracking by the active member of a fault-tolerant (FT) group, use the **probe** command. Use the **no** form of this command to dissociate the tracking probe from the tracking process on the active member.

probe *name* **priority** *number*

no probe *name* **priority** *number*

Syntax Description

name	Identifier of an existing probe that you want to associate with a gateway or host for tracking.
priority *number*	(Optional) Specifies the priority of the probe on the active member of an FT group. Enter an integer from 0 to 255. The default is 0. Higher values indicate higher priorities.

Command Modes

FT track host configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Assign a priority value to the probe based on the relative importance of the gateway or host that the probe is tracking. If the probe goes down, the ACE decrements the priority of the FT group on the active member by the value of the *number* argument. If the priority of the FT group on the active member falls below the priority of the FT group on the standby member, a switchover occurs where the active member becomes the standby member and the standby member becomes the active member.

Examples

To configure a probe with a priority of 25 on the active member of an FT group, enter:

```
host1/Admin(config-ft-track-host)# probe TCP_PROBE1 priority 25
```

To remove the tracking probe from the active member, enter:

```
host1/Admin(config-ft-track-host)# no probe TCP_PROBE1
```

Related Commands

show probe
show running-config
(config) probe
(config-ft-track-host) peer probe

(config-ft-track-host) track-host

To configure the IP address of the gateway or host that you want to track on the active member of a fault-tolerant (FT) group, use the **track-host** command. Use the **no** form of this command to remove the IP address of the gateway or host from the tracking process on the active member.

track-host *ip_address*

no track-host *ip_address*

Syntax Description

ip_address	IP address of the gateway or host that you want the active FT group member to track. Enter the IP address in dotted-decimal notation (for example, 172.16.27.1).

Command Modes

FT track host configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To configure a gateway for tracking on the active member of an FT group, enter:

```
host1/Admin(config-ft-track-host)# track-host 172.16.27.1
```

To remove the gateway from the tracking process on the active member, enter:

```
host1/Admin(config-ft-track-host)# no track-host 172.16.27.1
```

Related Commands

show running-config
(config-ft-track-host) peer track-host

FT Track Interface Configuration Mode Commands

Fault-tolerant (FT) track interface configuration mode allows you to configure tracking and failure detection for critical interfaces.

To create a process that tracks and detects failures for critical interfaces and accesses FT track interface configuration mode, enter the **ft track interface** command in configuration mode. The CLI prompt changes to (config-ft-track-interface). For information about the commands in FT track interface configuration mode, see the following commands.

To delete the process that tracks and detects failures for an interface, use the **no** form of this command.

ft track interface *name*

no ft track interface *name*

Syntax Description

name	Unique identifier of the process that tracks and detects failures for a critical interface. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the fault-tolerant feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To create a process that tracks and detects failures for an interface and access FT track interface configuration mode, enter:

```
host1/Admin(config)# ft track interface TRACK_VLAN200
host1/Admin(config-ft-track-interface)#
```

To delete the process that tracks and detects failures for an interface, enter:

```
host1/Admin(config)# no ft track interface TRACK_VLAN200
```

Related Commands

show running-config

(config-ft-track-interface) peer priority

To assign a priority to the interface that the standby member is tracking, use the **peer priority** command. Use the **no** form of this command to reset the priority to the default value of 10.

peer priority *number*

no peer priority *number*

Syntax Description

number	Priority of the interface tracked by the standby member of a fault-tolerant (FT) group. Enter an integer from 0 to 255. The default is 0. Higher values indicate higher priorities.

Command Modes

FT track interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The **peer** command keyword indicates the standby member of an FT group.

Assign a priority value based on the relative importance of the interface that you are tracking on the standby member of an FT group. If the tracked interface goes down, the ACE decrements the priority of the FT group on the standby member by the value of the *number* argument. If the priority of the FT group on the active member falls below the priority of the FT group on the standby member, a switchover occurs where the active member becomes the standby member and the standby member becomes the active member.

Examples

To set a priority of 100 for the interface that you are tracking on the standby member, enter:

```
host1/Admin(config-ft-track-intf)# peer priority 100
```

To reset the priority of the interface to the default value of 0, enter:

```
host1/Admin(config-ft-track-intf)# no peer priority 100
```

Related Commands

(config-ft-track-interface) priority

(config-ft-track-interface) peer track-interface vlan

To configure the interface that you want the standby member to track, use the **peer track-interface vlan** command. Use the **no** form of this command to remove the interface.

peer track-interface vlan *vlan_id*

no peer track-interface vlan *vlan_id*

Syntax Description

vlan_id	Unique identifier of an existing VLAN that you want to track on the standby member of a fault-tolerant (FT) group. Enter an integer from 2 to 4094.

Command Modes

FT track interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The **peer** command keyword indicates the standby member of an FT group.

You cannot track the FT VLAN because it is reserved for the redundancy protocol.

Examples

To configure the VLAN 200 interface for tracking on the standby member, enter:

```
host1/Admin(config-ft-track-intf)# peer track-interface vlan 200
```

To remove VLAN 200 from the tracking process, enter:

```
host1/Admin(config-ft-track-intf)# no peer track-interface vlan 200
```

Related Commands

(config-ft-track-interface) track-interface vlan

(config-ft-track-interface) priority

To assign a priority to the interface that the active member is tracking, use the **priority** command. Use the **no** form of this command to reset the priority of the interface to the default value of 10.

priority *number*

no priority *number*

Syntax Description

number	Priority of the interface tracked by the active member of a fault-tolerant (FT) group. Enter an integer from 0 to 255. The default is 0. Higher values indicate higher priorities.

Command Modes

FT track interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Assign a priority value based on the relative importance of the interface that you are tracking on the active member of an FT group. If the tracked interface goes down, the ACE decrements the priority of the FT group on the active member by the value of the *number* argument. If the priority of the FT group on the active member falls below the priority of the FT group on the standby member, a switchover occurs where the active member becomes the standby member and the standby member becomes the active member.

Examples

To set a priority of 100 for the interface that you are tracking on the active member of an FT group, enter:

```
host1/Admin(config-ft-track-intf)# priority 100
```

To reset the priority of the interface to the default value of 0, enter:

```
host1/Admin(config-ft-track-intf)# no priority 100
```

Related Commands

(config-ft-track-interface) peer priority

(config-ft-track-interface) track-interface vlan

To configure the interface that you want the active member to track, use the **track-interface vlan** command. Use the **no** form of this command to remove the interface from the tracking process.

track-interface vlan *vlan_id*

no track-interface vlan *vlan_id*

Syntax Description

vlan_id	Unique identifier of an existing VLAN that you want to track on the active member of a fault-tolerant (FT) group. Enter an integer from 2 to 4094.

Command Modes

FT track interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To configure the VLAN 200 interface for tracking on the active member, enter:

```
host1/Admin(config-ft-track-intf)# track-interface vlan 200
```

To remove VLAN 200 from the tracking process, enter:

```
host1/Admin(config-ft-track-intf)# no track-interface vlan 200
```

Related Commands

show interface

Interface Configuration Mode Commands

Interface configuration mode commands allow you to configure a VLAN interface, a bridge-group virtual interface (BVI), an Ethernet port or a port-channel interface. To configure a bridge-group virtual interface (BVI), Ethernet port, port-channel interface, or VLAN interface, use the **interface** command. The CLI prompt changes to (config-if). Use the **no** form of this command to remove the interface from the context. For information about the commands in interface configuration mode, see the following commands.

interface {**bvi** *group_number* | **gigabitEthernet** *slot_number/port_number* | **port-channel** *channel_number* | **vlan** *number*}

no interface {**bvi** *group_number* | **gigabitEthernet** *slot_number/port_number* | **port-channel** *channel_number* | **vlan** *number*}

Syntax Description

bvi *group_number*	Creates a BVI for a bridge group and accesses interface configuration mode commands for the BVI. The *group_number* argument is the bridge-group number configured on a VLAN interface.
gigabitEthernet *slot_number/port_number*	Specifies one of the four Ethernet ports on the rear panel of the ACE. • *slot_number*—The physical slot on the ACE containing the Ethernet ports. This selection is always 1, the location of the daughter card in the ACE. The daughter card includes the four Layer 2 Ethernet ports to perform Layer 2 switching. • *port_number*—The physical Ethernet port on the ACE. Valid selections are 1 through 4, which specifies one of the four Ethernet ports (1, 2, 3, or 4) associated with the slot 1 (daughter card) selection.
port-channel *channel_number*	Specifies the channel number assigned to this port-channel interface. Valid values are from 1 to 255.
vlan *number*	Assigns the VLAN to the context and accesses interface configuration mode commands for the VLAN. The *number* argument is the number for a VLAN assigned to the ACE.

Command Modes

Configuration mode

BVI and VLAN interface—Admin and user contexts

Ethernet port and port-channel interface—Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

All commands in this mode require the interface feature in your user role. In addition, the Ethernet port and port-channel interface command functions require the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The four Ethernet ports provide physical Ethernet ports to connect servers, PCs, routers, and other devices to the ACE. You can configure the four Ethernet ports to provide an interface for connecting to 10-Mbps, 100-Mbps, or 1000-Mbps networks. Each Layer 2 Ethernet port supports autonegotiate, or full-duplex or half-duplex operation on an Ethernet LAN, and can carry traffic within a designated VLAN.

You can group physical ports together on the ACE to form a logical Layer 2 interface called the EtherChannel (or port-channel). All the ports belonging to the same port-channel must be configured with same values; for example, port parameters, VLAN membership, trunk configuration. Only one port-channel in a channel group is allowed, and a physical port can belong to only to a single port-channel interface.

You can configure one or more VLAN interfaces in any user context before you assign those VLAN interfaces to the associated user contexts through the **(config-context) allocate-interface** command in the Admin context.

The ACE supports a maximum of 4,093 VLAN interfaces with a maximum of 1,024 shared VLANs.

The ACE supports a maximum of 4,094 BVI interfaces.

The ACE supports a maximum of 8,192 interfaces per system that include VLANs, shared VLANs, and BVI interfaces.

Examples

To assign VLAN interface 200 to the Admin context and access interface configuration mode, enter:

```
host1/Admin(config)# interface vlan 200
host1/Admin(config-if)#
```

To remove a VLAN, enter:

```
host1/Admin(config)# no interface vlan 200
```

To create a BVI for bridge group 15, enter:

```
host1/Admin(config)# interface bvi 15
host1/Admin(config-if)#
```

To delete a BVI for bridge group 15, enter:

```
host1/Admin(config)# no interface bvi 15
```

Related Commands

show arp
show interface
show ip
show running-config
show vlans

(config-if) access-group

To apply an access control list (ACL) to the inbound or outbound direction of a VLAN interface and make the ACL active, use the **access-group** command. Use the **no** form of this command to remove an ACL from an interface.

access-group {**input** | **output**} *acl_name*

no access-group {**input** | **output**} *acl_name*

Syntax Description

input	Specifies the inbound direction of the interface to which you want to apply the ACL.
output	Specifies the outbound direction of the interface to which you want to apply the ACL.
acl_name	Identifier of an existing ACL that you want to apply to an interface.

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You must apply ACLs to a VLAN interface to allow the traffic to pass on an interface. You can apply one ACL of each type (extended and EtherType) to both directions of the interface. For connectionless protocols, you need to apply the ACL to the source and destination interfaces if you want traffic to pass in both directions. For example, you can allow Border Gateway Protocol (BGP) in an ACL in transparent mode, and you need to apply the ACL to both interfaces.

A bridge-group VLAN supports extended ACLs for IP traffic and EtherType ACLs for non-IP traffic. For non-IP traffic, you can configure an EtherType ACL. EtherType ACLs support Ethernet V2 frames. You can configure the ACE to pass one or any of the following non-IP EtherTypes: Multiprotocol Label Switching (MPLS), IP version 6 (ipv6), and bridge protocol data units (BDPUs).

The **output** option is not allowed for EtherType ACLs.

To apply an ACL globally to all interfaces in a context, use the **(config) access-group** command.

Examples

To apply an ACL named INBOUND to the inbound direction of an interface, enter:

```
host1/Admin(config)# interface vlan100
host1/Admin(config-if)# access-group input INBOUND
```

To remove an ACL from an interface, enter:

```
host1/Admin(config-if)# no access-group input INBOUND
```

Related Commands

show access-list
(config) access-group
(config) access-list extended

(config-if) alias

To configure an IP address that is shared between active and standby appliances for a bridge-group virtual interface (BVI) or VLAN interface, use the **alias** command. Use the **no** form of this command to delete an alias IP address.

alias *ip_address mask*

no alias *ip_address mask*

Syntax Description

ip_address	IP address of the interface. Enter the IP address in dotted-decimal notation (for example, 172.16.27.1).
mask	Subnet mask of the interface. Enter the subnet mask in dotted-decimal notation (for example, 255.255.255.0).

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You must configure redundancy (fault tolerance) on the ACE for the alias IP address to work. For more information on redundancy, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

For stealth firewalls, an ACE balances traffic among unique VLAN alias IP address interfaces on another ACE that provides paths through stealth firewalls. You configure a stealth firewall so that all traffic moving in both directions across that VLAN moves through the same firewall.

For details about firewall load balancing (FWLB), see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To configure an alias IP address and mask, enter:

```
host1/Admin(config-if)# alias 12.0.0.81 255.0.0.0
```

To remove an alias IP address, enter:

```
host1/Admin(config-if)# no alias 192.168.12.15 255.255.255.0
```

Related Commands

show interface

(config-if) arp

To add a static ARP entry in the ARP table for a VLAN interface, use the **arp** command. Use the **no** form of this command to remove a static ARP entry.

arp *ip_address mac_address*

no arp *ip_address mac_address*

Syntax Description

ip_address	IP address for an ARP table entry. Enter the IP address in dotted-decimal notation (for example, 172.16.27.1).
mac_address	MAC address for the ARP table entry. Enter the MAC address in dotted-hexadecimal notation (for example, 00.02.9a.3b.94.d9).

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Static ARPs for bridged interfaces are configured on the specific interface.

Examples

To allow ARP responses from the router at 10.1.1.1 with the MAC address 00.02.9a.3b.94.d9, enter:

```
host1/Admin(config-if)# arp 10.1.1.1 00.02.9a.3b.94.d9
```

To remove a static ARP entry, use the **no arp** command. For example, enter:

```
host1/Admin(config-if)# no arp 10.1.1.1 00.02.9a.3b.94.d9
```

Related Commands

show arp

(config-if) arp inspection

To enable the ACE to dynamically check the source MAC address in an Ethernet header against the sender's MAC address in an ARP payload for every ARP packet received by the ACE, use the **arp inspection** command. Use the **no** form of this command to remove a static ARP entry.

arp inspection validate src-mac [**flood** | **no-flood**]

no arp *ip_address mac_address*

Syntax Description

validate src-mac	Instructs the ACE to check the source MAC address in an Ethernet header against the sender's MAC address in an ARP payload for every ARP packet received by the ACE
flood	(Optional) Enables ARP forwarding for the interface and forwards ARP packets with nonmatching source MAC addresses to all interfaces in the bridge group. This is the default option when you enable dynamic ARP inspection.
no-flood	(Optional) Disables ARP forwarding for the interface and drops ARP packets with nonmatching source MAC addresses.

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The ACE does not learn or update the ARP or MAC tables for packets with different MAC addresses. By default, dynamic ARP inspection is disabled. If you enable this feature, the default option is **flood**.

Use this feature for interoperability with third-party firewalls (for example, CheckPoint).

If ARP inspection fails, then the ACE does not perform source MAC validation. For details about ARP inspection, see the **(config) arp** command.

Regardless of whether you enter the **flood** or the **no-flood** option, if the source MAC address of the ARP packet does not match the MAC address of the Ethernet header, then the source MAC validation fails and the ACE increments the Smac-validation Failed counter of the **show arp** command.

Examples

To enable the ACE to check the source MAC address in an Ethernet header against the sender's MAC address in an ARP payload for every ARP packet received by the ACE and to forward (flood) the packets, enter:

```
host1/Admin(config-if)# arp inspection validate src-mac
```

To restore the behavior of the ACE to the default of not validating source MAC addresses, enter the following command:

```
host1/Admin(config-if)# no arp inspection validate src-mac
```

Related Commands

show arp

(config-if) bridge-group

To assign the VLAN to a bridge group, use the **bridge-group** command. Use the **no** form of this command to remove the bridge group from the VLAN.

bridge-group *number*

no bridge-group

Syntax Description

number	Bridge-group number. Enter an integer from 1 to 4094.

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

In bridge mode, you can configure two interface VLANs into a group and bridge packets between them. All interfaces are in one broadcast domain and packets from one VLAN are switched to the other VLAN. The ACE bridge mode supports only two L2 VLANs per bridge group. In this mode, VLANs do not have configured IP addresses.

To enable the bridge-group VLANs, you must configure a bridge-group virtual interface (BVI) that represents a corresponding bridge group.

Examples

To assign bridge group 15 to the VLAN, enter:

```
host1/Admin(config-if)# bridge-group 15
```

To remove the bridge group from the VLAN, enter:

```
host1/Admin(config-if)# no bridge-group
```

Related Commands

show interface

(config-if) carrier-delay

To add a configurable delay at the physical port level to address issues with transition time, based on the variety of peers, use the **carrier-delay** command. Use the **no** form of the command to remove the carrier delay for the Ethernet port.

carrier-delay *seconds*

no carrier-delay *seconds*

Syntax Description

seconds	The carrier transition delay in seconds. Valid values are 0 to 120 seconds. The default is 0 (no carrier delay).

Command Modes

Interface configuration mode

Admin context only

Command History

Release	Modification
A1(8)	This command was introduced.

Usage Guidelines

If you connect an ACE to a Catalyst 6500 series switch, your configuration on the Catalyst may include the Spanning Tree Protocol (STP). However, the ACE does not support STP. In this case, you may find that the Layer 2 convergence time is much longer than the physical port up time. For example, the physical port would normally be up within 3 seconds, but STP moving to the forward state may need approximately 30 seconds. During this transitional time, although the ACE declares the port to be up, the traffic will not pass.

The **carrier-delay** command adds a configurable delay at the physical port level to address this transition time, based on the variety of peers.

Examples

To add a configurable delay of 60 seconds at the physical port level for Ethernet port 3, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/3
host1/Admin(config-if)# carrier-delay 60
```

To remove the carrier delay for the Ethernet port, enter:

```
host1/Admin(config-if)# no carrier-delay 60
```

Related Commands

show interface

(config-if) channel-group

To map the physical Ethernet port to a port channel when configuring Layer 2 EtherChannels, use the **channel-group** command. Use the **no** form of the command to remove the channel group assigned to the Ethernet port.

channel-group *channel_number*

no channel-group *channel_number*

Syntax Description

channel_number	Channel number assigned to this channel group. Valid values are from 1 to 255.

Command Modes

Interface configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You can group physical ports together on the ACE to form a logical Layer 2 interface called the EtherChannel (or port-channel). The **channel-group** command configures the Ethernet port in a port-channel group and automatically creates the port-channel logical interface.

It is not necessary to configure a port-channel interface before assigning a physical Ethernet port to a channel group through the **channel-group** command. A port-channel interface is created automatically when the channel group receives its first physical interface, if it is not already created.

Examples

To create a channel group with a channel number of 255, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/3
host1/Admin(config)# channel-group 255
```

To remove the channel group assigned to the Ethernet port, enter:

```
host1/Admin(config-if)# no channel-group 255
```

Related Commands

show interface

(config-if) description

To provide a description for a bridge-group virtual interface (BVI) or VLAN interface, use the **description** command. Use the **no** form of this command to delete the description.

description *text*

no description

Syntax Description

text	Description for the interface. Enter an unquoted text string that contains a maximum of 240 characters including spaces.

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To provide the description of POLICY MAP 3 FOR INBOUND AND OUTBOUND TRAFFIC, enter:

```
host1/admin(config-if)# description POLICY MAP3 FOR INBOUND AND OUTBOUND TRAFFIC
```

To remove the description for the interface, enter:

```
host1/admin(config-if)# no description
```

Related Commands

show interface

(config-if) duplex

To configure an Ethernet port for full- or half-duplex operation, use the **duplex** command in interface configuration mode. The default configuration for an ACE interface is autonegotiate. Use the **no** form of this command to revert to autonegotiation operation.

duplex {**full** | **half**}

no duplex

Syntax Description

full	Configures the specified Ethernet port for full-duplex operation, which allows data to travel in both directions at the same time.
half	Configures the specified Ethernet port for half-duplex operation. A half-duplex setting ensures that data travels only in one direction at any given time.

Command Modes

Interface configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

If you configure the Ethernet port speed to **auto** on a 10/100/1000-Mbps Ethernet port, both speed and duplex are autonegotiated. The ACE prevents you from making a duplex setting when you configure the speed of an Ethernet port to **auto**. The **speed** command must be a non-auto setting of 10, 100, or 1000 Mbps to be able to configure the duplex setting for the Ethernet port.

Examples

To set the duplex mode to full on Ethernet port 3, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/3
host1/Admin(config-if)# duplex full
```

To restore the default setting of autonegotiate for an Ethernet port, enter:

```
host1/Admin(config-if)# no duplex
```

Related Commands

(config-if) speed

(config-if) fragment chain

To configure the maximum number of fragments that belong to the same packet that the ACE accepts for reassembly for a VLAN interface, use the **fragment chain** command. Use the **no** form of this command to reset the default value.

fragment chain *number*

no fragment chain

Syntax Description

number	Maximum number of fragments that belong to the same packet. Enter an integer from 1 to 256. The default is 24.

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To configure a fragment chain limit of 126, enter:

```
host1/C1(config-if)# fragment chain 126
```

To reset the maximum number of fragments in a packet to the default of 24, enter:

```
host1/C1(config-if)# no fragment chain
```

Related Commands

show fragment
(config-if) fragment min-mtu
(config-if) fragment timeout

(config-if) fragment min-mtu

To configure the minimum fragment size that the ACE accepts for reassembly for a VLAN interface, use the **fragment min-mtu** command. Use the **no** form of this command to reset the default value.

fragment min-mtu *number*

no fragment min-mtu

Syntax Description

number	Minimum fragment size. Enter an integer from 28 to 9216 bytes. The default is 576 bytes.

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To configure a minimum fragment size of 1024, enter:

```
host1/C1(config-if)# fragment min-mtu 1024
```

To reset the minimum fragment size to the default value of 576 bytes, enter:

```
host1/C1(config-if)# no fragment min-mtu
```

Related Commands

show fragment
(config-if) fragment chain
(config-if) fragment timeout

(config-if) fragment timeout

To configure a reassembly timeout for a VLAN interface, use the **fragment timeout** command. Use the **no** form of this command to reset the default value.

fragment timeout *seconds*

no fragment timeout

Syntax Description

seconds	Reassembly timeout in seconds. Enter an integer from to 1 to 30. The default is 5.

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The IP reassembly timeout specifies the period of time after which the ACE abandons the fragment reassembly process if it does not receive any outstanding fragments for the current fragment chain (fragments that belong to the same packet).

Examples

To configure an IP reassembly timeout of 15 seconds, enter:

```
host1/C1(config-if)# fragment timeout 15
```

To reset the fragment timeout to the default value of 5 seconds, enter:

```
host1/C1(config-if)# no fragment timeout
```

Related Commands

show fragment
(config-if) fragment chain
(config-if) fragment min-mtu

(config-if) ft-port vlan

To configure one of the Ethernet ports or a port-channel interface on the ACE for fault tolerance using a dedicated FT VLAN for communication between the members of an FT group, use the **ft-port vlan** command in interface configuration mode. Use the **no** form of this command to remove the FT VLAN function from an Ethernet port or port-channel interface.

ft-port vlan *number*

no ft-port vlan *number*

Syntax Description

number	Unique identifier for the FT VLAN. Valid values are from 2 to 4094.

Command Modes

Interface configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Peer ACE appliances communicate with each other over a dedicated FT VLAN. These redundant peers use the FT VLAN to transmit and receive heartbeat packets and state and configuration replication packets.

On both peer ACE appliances, you must configure the same Ethernet port or the same port-channel interface as the FT VLAN port. For example, if you configure ACE appliance 1 to use Ethernet port 4 as the FT VLAN port, then be sure to configure ACE appliance 2 to use Ethernet port 4 as the FT VLAN port.

It is not necessary to create an FT VLAN before designating an Ethernet port or port-channel interface as the FT VLAN port.

When you specify the **ft-port vlan** command, the ACE modifies the associated Ethernet port or port-channel interface to a trunk port.

We recommend that you enable QoS on the FT VLAN port to provide higher priority for FT traffic (see the **(config-if) qos trust cos** command).

For details on configuring redundant ACE appliances, including an FT VLAN, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.

Examples

To configure FT VLAN identifier 60 for Ethernet port 3, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/3
host1/Admin(config-if)# ft-port vlan 60
```

To remove the FT VLAN from the Ethernet port, enter:

```
host1/Admin(config-if)# no ft-port vlan 60
```

Related Commands

show interface

(config-if) icmp-guard

To enable the ICMP security checks in the ACE, use the **icmp-guard** command. This feature is enabled by default. Use the **no** form of this command to disable the ICMP security checks.

icmp-guard

no icmp-guard

Syntax Description

This command has no keywords or arguments.

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

By default, the ACE provides several ICMP security checks by matching ICMP reply packets with request packets and using mismatched packets to detect attacks. Also, the ACE forwards ICMP error packets only if a connection record pertaining to the flow for which the error packet was received exists.

Caution If you disable the ACE ICMP security checks, you may expose your ACE and your data center to potential security risks. After you enter the **no icmp-guard** command, the ACE no longer performs Network Address Translation (NAT) translations on the ICMP header and payload in error packets, which potentially can reveal real host IP addresses to attackers.

If you want to operate your ACE as a load balancer only, use the **no icmp-guard** command to disable the ACE ICMP security checks. You must also disable TCP normalization by using the **no normalization** command. For details about operating your ACE for load balancing only, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To enable the ACE ICMP security checks after you have disabled them, enter:

```
host1/Admin(config)# interface vlan 200
host1/Admin(config-if)# icmp-guard
```

To disable ACE ICMP security checks, enter:

```
host1/Admin(config-if)# no icmp-guard
```

Related Commands

(config-if) normalization

(config-if) ip address

To assign an IP address to a bridge-group virtual interface (BVI) or VLAN interface, use the **ip address** command. Use the **no** form of this command to remove an IP address from an interface.

ip address *ip_address mask*

no ip address

Syntax Description

address	IP address and mask for the interface. Enter an IP address in dotted-decimal notation (for example, 192.168.12.1).
mask	Subnet mask of the interface. Enter the subnet mask in dotted-decimal notation (for example, 255.255.255.0).

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When you assign an IP address to an interface, the ACE automatically makes the interface routed.

You must configure static ARP entries for bridged interfaces on the specific interface.

In a single context, you must configure each interface address on a unique subnet; the addresses cannot overlap. However, the IP subnet can overlap an interface in different contexts.

You must configure a unique IP address across multiple contexts on a shared VLAN. On a nonshared VLAN, the IP address can be the same.

No routing occurs across contexts even when shared VLANs are configured.

Examples

To set the IP address of 192.168.1.1 255.255.255.0 for VLAN interface 200, enter:

```
host1/Admin(config)# interface vlan 200
host1/Admin(config-if)# ip address 192.168.1.1 255.255.255.0
```

To remove the IP address for the VLAN, enter:

```
host1/Admin(config-if)# no ip address
```

Related Commands

show arp
show interface
show ip

(config-if) ip df

To configure how the ACE handles an IP packet that has its Don't Fragment (DF) bit set on a VLAN interface, use the **ip df** command. Use the **no** form of this command to instruct the ACE to ignore the DF bit.

ip df {**clear** | **allow**}

no ip df

Syntax Description

clear	Clears the DF bit and permits the packet. If the packet is larger than the next-hop maximum transmission unit (MTU), the ACE fragments the packet.
allow	Permits the packet with the DF bit set. This is the default. If the packet is larger than the next-hop MTU, the ACE discards the packet and sends an ICMP unreachable message to the source host.

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Occasionally, an ACE may receive a packet that has its DF bit set in the IP header. This flag tells network routers and the ACE not to fragment the packet and to forward it in its entirety.

Examples

To clear the DF bit and permit the packet, enter:

```
host1/Admin(config-if)# ip df clear
```

To instruct the ACE to ignore the DF bit, enter:

```
host1/Admin(config-if)# no ip df
```

Related Commands

This command has no related commands.

(config-if) ip dhcp relay enable

To accept Dynamic Host Configuration Protocol (DHCP) requests on a VLAN interface, use the **ip dhcp relay enable** command. Use the **no** form of this command to disable DHCP on the interface.

ip dhcp relay enable

no ip dhcp relay enable

Syntax Description

This command has no keywords or arguments.

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The DHCP relay starts forwarding packets to the DHCP server address specified in the **ip dhcp relay server** command for the associated interface or context.

Examples

To enable the DHCP relay on the interface, enter:

```
host1/Admin(config-if)# ip dhcp relay enable
```

To disable the DHCP relay on the interface, enter:

```
host1/Admin(config-if)# no ip dhcp relay enable
```

Related Commands

(config-if) ip dhcp relay enable
(config-if) ip dhcp relay server

(config-if) ip dhcp relay server

To set the IP address of a Dynamic Host Configuration Protocol (DHCP) server to which the DHCP relay agent forwards client requests on a VLAN interface, use the **ip dhcp relay server** command. Use the **no** form of this command to remove the IP address of the DHCP server.

ip dhcp relay server *ip_address*

no ip dhcp relay server *ip_address*

Syntax Description

ip_address	IP address of the DHCP server. Enter the address in dotted-decimal IP notation (for example, 192.168.11.1).

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To specify the IP address for the DHCP relay server, enter:

```
host1/Admin(config-if)# ip dhcp relay server 192.168.20.1
```

To remove the IP address of the DHCP server, enter:

```
host1/Admin(config-if)# no ip dhcp relay server 192.168.20.1
```

Related Commands

This command has no related commands.

(config-if) ip options

To configure how the ACE handles IP options and to perform specific actions when an IP option is set in a packet for a VLAN interface, use the **ip options** command. Use the **no** form of this command to instruct the ACE to ignore the IP option.

ip options {**allow** | **clear** | **clear-invalid** | **drop**}

no ip options

Syntax Description

allow	Allows the packet with the IP options set.
clear	Clears the specified option from the packet and allows the packet.
clear-invalid	Clears all IP options from the packet if the ACE encounters one or more invalid or unsupported IP options and allows the packet. This option is the default.
drop	Causes the ACE to discard the packet.

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To allow packets with IP options set, enter:

```
host1/Admin(config-if)# ip options allow
```

To reset the ACE to its default of clearing all IP options if the appliance encounters one or more invalid or unsupported IP options, enter:

```
host1/Admin(config-if)# no ip options
```

Related Commands

This command has no related commands.

(config-if) ip ttl minimum

To set the packet time-to-live (TTL) hops in the IP header on a VLAN interface, use the **ip ttl minimum** command. By default, the ACE does not rewrite the TTL value of a packet. Use the **no** form of this command to reset the default behavior.

ip ttl minimum *number*

no ip ttl minimum

Syntax Description

number	Minimum number of hops that a packet can take to reach its destination. Enter an integer from 1 to 255 seconds.

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Each router along the packet's path decrements the TTL by one. If the packet's TTL equals 0 before the packet reaches its destination, the packet is discarded.

If the TTL value of the incoming packet is lower than the configured value, the ACE rewrites the TTL with the configured value. Otherwise, the ACE transmits the packet with its TTL unchanged or discards the packet if the TTL equals zero.

Examples

To set the TTL hops to 15, enter:

```
host1/Admin(config-if)# ip ttl minimum 15
```

To instruct the ACE to ignore the TTL value, enter:

```
host1/Admin(config-if)# no ip ttl minimum
```

Related Commands

This command has no related commands.

(config-if) ip verify reverse-path

To enable reverse-path forwarding (RPF) based on the source IP address for a VLAN interface, use the **ip verify reverse-path** command. By default, URPF is disabled on the interface. Use the **no** form of this command to reset the default behavior.

ip verify reverse-path

no ip verify reverse-path

Syntax Description

This command has no keywords or arguments.

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Unicast reverse-path forwarding (URPF) helps to mitigate problems caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by allowing the ACE to discard IP packets that lack a verifiable source IP address. This feature enables the ACE to filter both ingress and egress packets to verify addressing and route integrity. The route lookup is typically based on the destination address, not the source address.

When you enable URPF, the ACE discards packets if no route is found or if the route does not match the interface on which the packet arrived.

You cannot use this command when RPF based on the source MAC address for a VLAN interface is enabled through the **(config-if) mac-sticky enable** command.

Examples

To enable RPF, enter:

```
host/Admin(config-if)# ip verify reverse-path
```

To disable RPF, enter:

```
host/Admin(config-if)# no ip verify reverse-path
```

Related Commands

(config-if) mac-sticky enable

(config-if) mac address autogenerate

To enable the autogeneration of a MAC address on a VLAN interface, use the **mac address autogenerate** command. Use the **no** form of this command to disable MAC address autogeneration.

mac address autogenerate

no mac address autogenerate

Syntax Description

This command has no keywords or arguments.

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

By default, the ACE does not allow traffic from one context to another context over a transparent firewall. The ACE assumes that VLANs in different contexts are in different Layer-2 domains, unless it is a shared VLAN. Thus the ACE allocates the same MAC address to them.

When using a firewall service module (FWSM) to bridge traffic between two contexts on the ACE, two Layer-3 VLANs must be assigned to the same bridge domain. To support this configuration, these VLAN interfaces require different MAC addresses.

When you issue the **mac address autogenerate** command, the ACE assigns a MAC address from the bank of MAC address for shared VLANs. If you issue the **no mac address autogenerate** command, the interface retains this address. To revert to a MAC address for an unshared VLAN, you must delete the interface and then readd it.

Examples

To enable MAC address autogeneration on the VLAN, enter:

```
host1/Admin(config-if)# mac address autogenerate
```

To disable MAC address autogeneration on the VLAN, enter:

```
host1/Admin(config-if)# no mac address autogenerate
```

Related Commands

This command has no related commands.

(config-if) mac-sticky enable

To enable the mac-sticky feature for a VLAN interface, use the **mac-sticky** command. The mac-sticky feature ensures that the ACE sends return traffic to the same upstream device through which the connection setup from the original client was received. By default, the mac-sticky feature is disabled on the ACE. Use the **no** form of this command to disable the mac-sticky feature, resetting the default behavior of the ACE performing a route lookup to select the next hop to reach the client.

mac-sticky enable

no mac-sticky enable

Syntax Description

This command has no keywords or arguments.

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When you use this command to enable the mac-sticky feature, the ACE uses the source MAC address from the first packet of a new connection to determine the device to send the return traffic. This guarantees that the ACE sends the return traffic for load-balanced connections to the same device originating the connection. By default, the ACE performs a route lookup to select the next hop to reach the client.

This feature is useful when the ACE receives traffic from Layer-2/Layer-3 adjacent stateful devices, like firewalls and transparent caches, guaranteeing that it sends return traffic to the correct stateful device that sourced the connection without any requirement for source NAT. For more information on firewall load balancing, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

You cannot use this command when RPF based on the source IP address for a VLAN interface is enabled through the **(config-if) ip verify reverse-path** command.

Examples

To enable the mac-sticky feature, enter:

```
host/Admin(config-if)# mac-sticky enable
```

To disable the mac-sticky feature, enter:

```
host/Admin(config-if)# no mac-sticky enable
```

Related Commands

(config-if) ip verify reverse-path

(config-if) mtu

To specify the maximum transmission unit (MTU) for a VLAN interface, use the **mtu** command. This command allows you to set the data size that is sent on a connection. Use the **no** form of this command to reset the MTU block size to the default of 1500 for Ethernet interfaces.

mtu *bytes*

no mtu

Syntax Description

bytes	Number of bytes in the MTU; valid values are from 64 to 9216 bytes. The default is 1500.

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The default MTU is a 1500-byte block for Ethernet interfaces. This value is sufficient for most applications, but you can pick a lower number if network conditions require it. The ACE fragments packets that are larger than the MTU value before sending them to the next hop.

Examples

To specify the MTU data size of 1000 for an interface, enter:

```
host1/admin(config-if)# mtu 1000
```

To reset the MTU block size to the default value of 1500 for Ethernet interfaces, enter:

```
host1/admin(config-if)# no mtu
```

Related Commands

show interface

(config-if) nat-pool

To create a pool of IP addresses for dynamic Network Address Translation (NAT) for a VLAN interface, use the **nat-pool** command. Use the **no** form of this command to remove a NAT pool from the configuration.

nat-pool *nat_id ip_address1* [*ip_address2*] **netmask** *mask* [**pat**]

no nat-pool *nat_id ip_address1* [*ip_address2*] **netmask** *mask* [**pat**]

Syntax Description

nat_id	Identifier of the NAT pool of global IP addresses. Enter an integer from 1 to 2147483647.
ip_address1	Single IP address, or if also using the *ip_address2* argument, the first IP address in a range of global addresses used for NAT. Enter an IP address in dotted-decimal notation (for example, 172.27.16.10).
ip_address2	(Optional) Highest IP address in a range of global IP addresses used for NAT. Enter an IP address in dotted-decimal notation (for example, 172.27.16.109).
netmask *mask*	Specifies the subnet mask for the IP address pool. Enter a mask in dotted-decimal notation (for example, 255.255.255.0). If you do not specify a network mask for the global IP addresses in the pool, the ACE, by default, uses the network mask of the interface to which the pool is attached.
pat	(Optional) Specifies that the ACE perform Port Address Translation (PAT) in addition to NAT.

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Dynamic NAT uses a pool of global IP addresses that you specify. You can define either a single global IP address for a group of servers with PAT to differentiate between them or a range of global IP addresses when using dynamic NAT only. To use a single IP address or a range of addresses, you assign an identifier to the address pool. You then associate the NAT pool with a global interface that is different from the interface that you use to filter and receive NAT traffic.

If a packet egresses an interface that you have not configured for NAT, the ACE transmits the packet untranslated.

If the ACE runs out of IP addresses in a NAT pool, it can switch over to a PAT rule, if configured. For example, you can configure the following:

```
nat-pool 1 10.1.100.10 10.1.100.99 netmask 255.255.255.255
nat-pool 1 10.1.100.100 10.1.100.100 netmask 255.255.255.255 pat
```

Examples

To configure a NAT pool that consists of a range of 100 global IP addresses with PAT, enter:

```
host1/C1(config-if)# nat-pool 1 172.27.16.10 172.27.16.109 netmask 255.255.255.0 pat
```

Related Commands

show nat-fabric
(config-pmap-lb-c) nat dynamic

(config-if) normalization

To enable TCP normalization, use the **normalization** command. This feature is enabled by default. Use the **no** form of this command to disable TCP normalization.

normalization

no normalization

Syntax Description

This command has no keywords or arguments.

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

By default, TCP normalization is enabled.

Caution

If you disable TCP normalization, you may expose your ACE and your data center to potential security risks. TCP normalization helps protect the ACE and the data center from attackers by enforcing strict security policies that are designed to examine traffic for malformed or malicious segments.

To operate your ACE for load balancing only, disable TCP normalization by entering the **no normalization** command. You must also disable the ACE Internet Control Message Protocol (ICMP) security checks by using the **no icmp-guard** command. For details about operating your ACE as a load balancer only, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Disabling TCP normalization affects only Layer 4 traffic. TCP normalization is always enabled for Layer 7 traffic.

Use the **no normalization** command when you encounter the following two types of asymmetric flows, which would otherwise be blocked by the normalization checks that the ACE performs:

- ACE sees only the client-to-server traffic. For example, for a TCP connection, the ACE sees the SYN from the client, but not the SYN-ACK from the server. In this case, apply the **no normalization** command to the client-side VLAN.

- ACE sees only the server-to-client traffic. For example, for a TCP connection, the ACE receives a SYN-ACK from the server without having received the SYN from the client. In this case, apply the **no normalization** command to the server-side VLAN.

With TCP normalization disabled, the ACE still sets up flows for the asymmetric traffic described above and makes entries in the connection table.

Examples

To enable TCP normalization after you have disabled it, enter:

```
host1/Admin(config)# interface vlan 200
host1/Admin(config-if)# normalization
```

To disable TCP normalization, enter:

```
host1/Admin(config-if)# no normalization
```

Related Commands

(config-if) icmp-guard

(config-if) peer ip address

To configure the IP address of a standby appliance for the bridge-group virtual interface (BVI) or VLAN interface, use the **peer** command. Use the **no** form of this command to delete the IP address of the peer appliance.

peer ip address *ip_address mask*

no peer ip address

Syntax Description

ip_address	IP address of the peer appliance. Enter the address in dotted-decimal IP notation (for example, 192.168.11.1).
mask	Subnet mask of the peer appliance. Enter the subnet mask in dotted-decimal notation (for example, 255.255.255.0).

Command Modes

Interface configuration mode for BVI and VLAN interfaces

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When you configure redundancy, configuration mode on the standby appliance is disabled by default and changes on an active appliance are automatically synchronized on the standby appliance. However, interface IP addresses on the active and standby appliances must be unique. To ensure that the addresses on the interfaces are unique, the interface IP address on the active appliance is synchronized on the

standby appliance as the peer IP address. To configure an interface IP address on the standby appliance, use the **peer ip address** command. The peer IP address on the active appliance is synchronized on the standby appliance as the interface IP address.

You must configure a unique IP address across multiple contexts on a shared VLAN. On a nonshared VLAN, the IP address can be the same.

Examples

To configure an IP address and mask for the peer appliance, enter:

```
host1/Admin(config-if)# peer ip address 11.0.0.81 255.0.0.0
```

To delete the IP address for the peer ACE appliance, enter:

```
host1/Admin(config-if)# no peer ip address
```

Related Commands

show interface

(config-if) port-channel load-balance

To set the load-distribution method among the ports in the EtherChannel bundle, use the **port-channel load-balance** command. Use the **no** form of the command to remove the load-distribution method.

port-channel load-balance {**dst-ip** | **dst-mac** | **dst-port** | **src-dst-ip** | **src-dst-mac** | **src-dst-port** | **src-ip** | **src-mac** | **src-port**}

no port-channel load-balance {**dst-ip** | **dst-mac** | **dst-port** | **src-dst-ip** | **src-dst-mac** | **src-dst-port** | **src-ip** | **src-mac** | **src-port**}

Syntax Description

dst-ip	Loads the distribution on the destination IP address
dst-mac	Loads the distribution on the destination MAC address
dst-port	Loads the distribution on the destination TCP or UDP port
src-dst-ip	Loads the distribution on the source or destination IP address
src-dst-mac	Loads the distribution on the source or destination MAC address
src-dst-port	Loads the distribution on the source or destination port
src-ip	Loads the distribution on the source IP address
src-mac	Loads the distribution on the source MAC address
src-port	Loads the distribution on the TCP or UDP source port

Command Modes

Interface configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

An EtherChannel balances the traffic load across the links in the EtherChannel by reducing part of the binary pattern formed from the addresses in the frame to a numerical value that selects one of the links in the channel. EtherChannel load balancing can use MAC addresses or IP addresses, Layer 4 port numbers, source addresses, destination addresses, or both source and destination addresses.

Use the option that provides the load-balance criteria with the greatest variety in your configuration. For example, if the traffic on an EtherChannel is going to a single MAC address only and you use the destination MAC address as the basis of EtherChannel load balancing, the EtherChannel always chooses the same link in the EtherChannel.

Examples

To configure an EtherChannel to balance the traffic load across the links using source or destination IP addresses, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/1
host1/Admin(config-if)# port-channel load-balance src-dst-ip
```

Related Commands

This command has no related commands.

(config-if) qos trust cos

To enable Quality of Service (QoS) for a configured physical Ethernet port that is based on VLAN Class of Service (CoS) bits, use the **qos trust cos** command. Use the **no** form of the command to disable QoS for the Ethernet port.

qos trust cos

no qos trust cos

Syntax Description

This command has no keywords or arguments.

Command Modes

Interface configuration mode

Admin context only

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

QoS is configured at the physical port level. When you enable QoS on a trusted port, traffic is mapped into different ingress queues based on their VLAN CoS bits. If there are no VLAN CoS bits, or QoS is not enabled on the port (untrusted port), the traffic is then mapped into the lowest priority queue.

You can enable QoS for an Ethernet port configured for fault tolerance (see **(config-if) ft-port vlan**). In this case, heartbeat packets are always tagged with COS bits set to 7 (a weight of High). We recommend that you enable QoS on the FT VLAN port to provide higher priority for FT traffic.

QoS is configurable only for a physical Ethernet port and is not VLAN interface-based.

Examples

To enable QoS for Ethernet port 3, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/3
host1/Admin(config-if)# qos trust cos
```

To disable QoS for the Ethernet port, enter:

```
host1/Admin(config-if)# no qos trust cos
```

Related Commands

show interface

(config-if) remove-eth-pad

To enable an internal length check and remove any trailer bytes appended to the end of an Ethernet IP frame coming into the ACE, use the **remove-eth-pad** command. This check is performed for each interface and is disabled by default. Use the **no** form of the command to disable an internal length check and the removal of trailer bytes.

remove-eth-pad

no remove-eth-pad

Syntax Description

This command has no keywords or arguments.

Command Modes

Interface configuration mode

Admin context only

Command History

Release	Modification
A3(2.3)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To enable an internal length check and remove any trailer bytes appended to the end of an Ethernet IP frame coming into the ACE, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/3
host1/Admin(config-if)# remove-eth-pad
```

To disable an internal length check and the removal of trailer bytes, enter:

```
host1/Admin(config-if)# no remove-eth-pad
```

Related Commands

show interface

(config-if) service-policy input

To apply a previously created policy map and attach the traffic policy to the input direction of a VLAN interface, use the **service-policy input** command Use the **no** form of this command to remove a service policy.

service-policy input *policy_name*

no service-policy input *policy_name*

Syntax Description

policy_name	Name of a previously defined policy map, configured with a previously created **policy-map** command. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When you enter the **service-policy** command in configuration mode, the policy maps that are applied globally in a context are applied on all interfaces that exist in the context.

A policy activated on an interface overwrites any specified global policies for overlapping classifications and actions.

The ACE allows only one policy of a specific feature type to be activated on a given interface.

Examples

To apply the L4SLBPOLICY policy map to an interface, enter:

```
host1/C1(config-if)# service-policy input L4SLBPOLICY
```

To remove the L4SLBPOLICY policy map from the interface, enter:

```
host1/C1(config-if)# no service-policy input L4SLBPOLICY
```

Related Commands

show service-policy
(config) service-policy

(config-if) shutdown

To disable a bridge-group virtual interface (BVI) or VLAN interface, use the **shutdown** command. Use the **no** form of this command to enable the interface.

shutdown

no shutdown

Syntax Description

This command has no keywords or arguments.

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When you create an interface, the interface is in the shutdown state until you enable it. If you disable or reenable the interface within a context, only that context interface is affected.

To enable a bridge-group virtual interface (BVI), Ethernet port, port-channel interface, VLAN interface, or VLAN trunking, use the **no shutdown** command in interface configuration mode. This puts the interface in the Up administrative state.

To disable a bridge-group virtual interface (BVI), Ethernet port, port-channel interface, VLAN interface, or VLAN trunking, use the **shutdown** command in interface configuration mode. This puts the interface in the Down administrative state.

Examples

To disable an interface, enter:

```
host1/Admin(config-if)# shutdown
```

To enable an interface for use, enter:

```
host1/Admin (config-if)# no shutdown
```

Related Commands

show interface
show running-config

(config-if) speed

To configure the Ethernet port speed for a setting of 10, 100, or 1000 Mbps, use the **speed** command in interface configuration mode. The default speed for an ACE interface is autonegotiate. Use the **no** form of the command to return to the default Ethernet port speed setting.

speed {**1000M** | **100M** | **10M** | **auto**}

no speed

Syntax Description

1000M	Initiates 1000-Mbps operation.
100M	Initiates 100-Mbps operation.
10M	Initiates 10-Mbps operation.
auto	Enables the ACE to autonegotiate with other devices for speeds of 10, 100, or 1000 Mbps. If you set the Ethernet port speed to **auto**, the ACE automatically sets the duplex mode to auto. This is the default setting.

Command Modes

Interface configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

By default, the ACE automatically uses the autonegotiate setting for Ethernet port speed and duplex mode parameters to allow the ACE to negotiate the speed and duplex mode between ports. If you manually configure the port speed and duplex modes, follow these guidelines:

- The ACE prevents you from making a duplex setting when you configure the speed of an Ethernet port to **auto**. The **speed** command must be a non-auto setting of 10, 100, or 1000 Mbps to be able to configure the duplex setting for the Ethernet port.
- If you configure an Ethernet port speed to a value other than **auto** (for example, 10, 100, or 1000 Mbps), ensure that you configure the connecting port to match. Do not configure the connecting port to negotiate the speed through the **auto** keyword.
- The ports on both ends of a link must have the same setting. The link will not come up if the port at each end of the connecting interface has a different setting.
- If you enter the **no speed** command, the ACE automatically configures both the speed and duplex settings to **auto**.

The ACE cannot automatically negotiate interface speed and duplex mode if you configure the connecting interface to a value other than **auto**.

If you configure the Ethernet port speed to **auto**, the ACE automatically sets the duplex mode to **auto**.

Examples

To set the speed to 1000 Mbps on Ethernet port 3, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/3
host1/Admin(config-if)# speed 1000M
```

To restore the default setting of autonegotiate for an Ethernet port, enter:

```
host1/Admin(config-if)# no speed
```

Related Commands

(config-if) duplex

(config-if) switchport access vlan

To configure an access port to a specific VLAN for either an Ethernet interface or a Layer 2 EtherChannel interface, use the **switchport access vlan** command in interface configuration mode. Use the **no** form of the command to reset the access mode to the default VLAN 1.

switchport access vlan *number*

no switchport access vlan *number*

Syntax Description

number	VLAN number that you want to configure as the IEEE 802.1Q native VLAN when operating in trunking mode. Valid values are from 1 to 4094. The default is VLAN 1.

Command Modes

Interface configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

On the ACE, ports are assigned to a single VLAN. These ports are referred to as access ports and provide a connection for end users or node devices, such as a router or server. By default, all devices are assigned to VLAN 1, known as the default VLAN.

You can configure a trunk on a single Ethernet port or on a port-channel interface (EtherChannel).

It is not necessary to create a VLAN interface before configuring an access VLAN. To configure a VLAN interface and access its mode to configure its attributes, use the **interface vlan** command in configuration mode for the context.

When you assign a VLAN as the access port for a specific Ethernet port or port-channel interface, the VLAN is reserved and cannot be configured as a VLAN trunk. A VLAN access port and a VLAN trunk cannot coexist for the same Ethernet port or port-channel interface. If you specify both configurations for the same Ethernet port or port-channel interface, the most recent configuration will overwrite the older configuration.

If you have QoS enabled for a physical Ethernet port (see the **"(config-if) qos trust cos"** command) that has been designated as an FT VLAN port (see the **"(config-if) ft-port vlan"** command), do not configure this Ethernet port as a VLAN access port. In this configuration, the QoS setting for redundancy traffic, such as heartbeat packets or TCP tracking probes, may not be handled properly by the ACE and FT traffic may be dropped when there is network congestion.

Examples

To configure VLAN 101 as an access port for Ethernet port 4, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/4
host1/Admin(config-if)# switchport access vlan 101
```

To configure VLAN 101 as an access port for EtherChannel 255, enter:

```
host1/Admin(config)# interface port-channel 255
host1/Admin(config-if)# switchport access vlan 101
```

To reset the access mode to the default VLAN 1, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/4
host1/Admin(config-if)# no switchport access vlan 101
```

Related Commands (config) interface

(config-if) switchport trunk allowed vlan

To specify which VLANs are to be allocated to a trunk link, use the **switchport trunk allowed vlan** command in interface configuration mode. To remove a VLAN from the trunk link, use the **no** form of the command.

switchport trunk allowed vlan *vlan_list*

no switchport trunk allowed vlan *vlan_list*

Syntax Description

vlan_list	The allowed VLANs that transmit this interface in tagged format when in trunking mode. The *vlan_list* argument can be one of the following: • Single VLAN number • Range of VLAN numbers separated by a hyphen • Specific VLAN numbers separated by commas Valid entries are 1 through 4094. Do not enter any spaces between the dash-specified ranges or the comma-separated numbers in the *vlan_list* argument.

Command Modes

Interface configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You cannot remove VLAN 1. If you remove VLAN 1 from a trunk, the trunk interface continues to send and receive management traffic in VLAN 1.

You can selectively allocate individual VLANs to a trunk link. All added VLANs are active on a trunk link, and as long as the VLAN is available for use, traffic for that VLAN is carried across the trunk link.

It is not necessary to create a VLAN interface before you allocate a VLAN to an Ethernet port or port-channel interface (EtherChannel). To configure a VLAN interface and access its mode to configure its attributes, use the **interface vlan** command in configuration mode for the context.

If you configure a VLAN on a trunk, you cannot configure the VLAN as the access port for a specific Ethernet port or port-channel interface. A VLAN access port and a VLAN trunk cannot coexist for the same Ethernet port or port-channel interface. If you specify both configurations for the same Ethernet port or port-channel interface, the most recent configuration will overwrite the older configuration.

When allocating VLANs to ports, overlapping is not allowed. For example, if you associate VLAN 10 with Ethernet port 1, you cannot associate VLAN 10 with another Ethernet port.

If you have QoS enabled for a physical Ethernet port (see the **"(config-if) qos trust cos"** command) that has been designated as an FT VLAN port (see the **"(config-if) ft-port vlan"** command), do not configure the FT VLAN as an 802.1Q native VLAN. In this configuration, the QoS setting for redundancy traffic, such as heartbeat packets or TCP tracking probes, may not be handled properly by the ACE and FT traffic may be dropped when there is network congestion.

Examples

To add VLANs 101, 201, and 250 through 260 to the defined list of VLANs currently set for Ethernet port 4, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/4
host1/Admin(config-if)# switchport trunk allowed vlan 101,201,250-260
```

To remove VLANs 101 through 499 from the defined list of VLANs currently set for Ethernet port 4, enter:

```
host1/Admin(config)# interface gigabitEthernet 1/4
host1/Admin(config-if)# no switchport trunk allowed vlan 101-499
```

Related Commands

(config) interface

(config-if) switchport trunk native vlan

To set the IEEE 802.1Q native VLAN for a trunk, use the **switchport trunk native vlan** command in interface configuration mode. Use the no form of the command to revert to the default of VLAN 1.

switchport trunk native vlan *number*

no switchport trunk native vlan *number*

Syntax Description

number	VLAN number that you want to configure as the 802.1Q native VLAN when operating in trunking mode. Valid values are from 1 to 4094. The default is VLAN 1.

Command Modes

Interface configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You can only have one assigned native VLAN.

The native VLAN is the VLAN that is assigned to all ports in the ACE. By default, all interfaces are in VLAN 1 on the ACE, and VLAN 1 is the native VLAN. Depending on your network needs, you may change the native VLAN to be other than VLAN 1.

When configuring 802.1Q trunking, you must match the native VLAN across the link. Because the native VLAN is untagged, you must keep the native VLAN the same on each side of the trunk line. The native VLAN must match on both sides of the trunk link for 802.1Q; otherwise, the link will not work.

It is not necessary to create a VLAN interface setting the 802.1Q native VLAN for a trunk. To configure a VLAN interface and access its mode to configure its attributes, use the **interface vlan** command in configuration mode for the context.

Examples

To specify VLAN 3 as the 802.1Q native VLAN for the trunk, enter:

```
host1/Admin(config)# interface port-channel 255
host1/Admin(config-if)# switchport trunk native vlan 3
```

To revert to the default of VLAN 1, enter:

```
host1/Admin(config-if)# no switchport trunk native vlan
```

Related Commands

(config) interface

(config-if) syn-cookie

To configure SYN-cookie-based DoS protection, use the **syn-cookie** command. Use the **no** form of this command to remove SYN-cookie DoS protection from the interface.

syn-cookie *number*

no syn-cookie

Syntax Description

number	Embryonic connection threshold above which the ACE applies SYN-cookie DoS protection. Enter an integer from 2 to 65535.

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

Please keep in mind the following guidelines when you use the SYN cookie feature:

- If the server drops the SYN that is sent by the ACE, the ACE resets the connection using the embryonic timeout. It does not retry the SYN packet.
- A SYN cookie supports only the MSS TCP option. The ACE ignores all other TCP options, even if there are problems with those other options.
- The ACE returns an MSS of 536 to the client, which is the RFC-specified default.
- If you use a parameter map to specify the minimum and maximum MSS values, the ACE ignores those values.
- Disabling normalization and using a SYN cookie concurrently may result in unpredictable behavior.
- The ACE does not generate any syslogs for a SYN cookie, even if the number of embryonic connections exceeds the configured threshold, which may indicate a SYN-flood attack.
- If you are configuring the SYN cookie feature on a bridged VLAN with non-loadbalanced flows, you must configure static routes for non-loadbalanced destinations that do not reside in the same subnet as the bridge-group virtual interface (BVI).

  For example, assuming the following configuration:

  - BVI IP address is 192.168.1.1
  - Gateway1 IP address 192.168.1.2 to reach external network 172.16.1.0
  - Gateway2 IP address 192.168.1.3 to reach external network 172.31.1.0

  Configure the following static routes:

  - ip route 172.16.1.0 255.255.255.0 192.168.1.2
  - ip route 172.31.1.0 255.255.255.0 192.168.1.3

Examples

To configure SYN-cookie DoS protection for servers in a data center connected to VLAN 100, enter:

```
host1/C1(config)# interface vlan 100
host1/C1(config-if)# syn-cookie 4096
```

To remove SYN-cookie DoS protection from the interface, enter:

```
host1/C1(config-if)# no syn-cookie
```

Related Commands

show interface
show running-config

(config-if) udp

To enable the UDP booster feature for applications that require very high UDP connection rates, use the **udp** command in interface configuration mode. The syntax of this command is as follows:

udp {**ip-source-hash** | **ip-destination-hash**}

no udp

Syntax Description

ip-source-hash	Instructs the ACE to hash the source IP address of UDP packets that hit a source-hash VLAN interface prior to performing a connection match. Configure this keyword on a client-side interface.
ip-destination-hash	Instructs the ACE to hash the destination IP address of UDP packets that hit a destination-hash VLAN interface prior to performing a connection match. Configure this keyword on a server-side interface.

Command Modes

Interface configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

For the UDP booster feature to work, you must configure both command keywords on their respective interfaces.

Do not configure this feature with NAT or with any Layer 7 feature, for example, per-packet UDP load balancing (also called UDP fast-age) using the **loadbalance vip udp-fast-age** command. Otherwise, unexpected results may occur.

For detailed information concerning this feature and its configuration, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To configure the UDP booster feature on the client VLAN 100, enter:

```
host1/C1(config)# interface vlan 100
host1/C1(config-if)# udp ip-source-hash
```

To configure the UDP booster feature on the server VLAN 200, enter:

```
host1/C1(config)# interface vlan 200
host1/C1(config-if)# udp ip-destination-hash
```

To remove the UDP booster feature from an interface, enter:

```
host1/C1(config-if)# no udp
```

Related Commands

show interface
show running-config

KAL-AP UDP Configuration Mode Commands

The ACE supports secure KAL-AP for MD5 encryption of data between the ACE and the Global Site Selector (GSS). To configure secure KAL-AP on the ACE, access KAL-AP UDP configuration mode using the **kalap udp** command. The CLI prompt changes to (config-kalap-udp). Use the **no** form of this command to return to configuration mode (or use the **exit** command).

kalap udp

no kalap udp

Syntax Description

This command has no keywords or arguments.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The ACE supports secure KAL-AP for MD5 encryption of data between the ACE and the GSS. For encryption, you must configure a shared secret as a key for authentication between the GSS and the ACE context.

Examples

To enter KAL-AP UDP configuration mode, enter:

```
host1/Admin(config)# kalap udp
host1/Admin(config-kalap-udp)#
```

Related Commands

show kalap udp load
show running-config
(config-kalap-udp) ip address

(config-kalap-udp) ip address

To enable secure KAL-AP, you configure the VIP address to the GSS and the shared secret using the **ip address** command. Use the **no** form of this command to remove the VIP address and the shared secret from the configuration.

ip address *ip_address* **encryption md5** *secret*

no ip address *ip_address*

Syntax Description

ip_address	VIP address for the GSS. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
secret	Shared secret between the GSS and the ACE. Enter the shared secret as a case-sensitive string with no spaces and a maximum of 31 alphanumeric characters.

Command Modes

KAL-AP UDP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The ACE supports secure KAL-AP for MD5 encryption of data between the ACE and the Global Site Selector (GSS). For encryption, you must configure a shared secret as a key for authentication between the GSS and the ACE context.

Examples

To enable secure KAL-AP and configure the VIP address for the GSS and the shared secret, enter:

```
host1/Admin(config)# kalap udp
host1/Admin(config-kalap-udp)# ip address 10.1.0.1 encryption md5 andromeda
```

To disable secure KAL-AP, enter:

```
host1/Admin(config-kalap-udp)# no ip address 10.1.0.1
```

Related Commands

show kalap udp load
show running-config
(config) kalap udp

LDAP Configuration Mode Commands

LDAP configuration mode commands allow you to configure multiple Lightweight Directory Access Protocol (v3) (LDAP) servers as a named AAA server group. You specify the IP address of one or more previously configured LDAP servers that you want added to or removed from a AAA server group with configuration parameters such as the user profile attribute, the base DN, and the filter to use in the search request.

For details about creating an LDAP server group, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

To create an LDAP server group and access the LDAP server configuration mode, use the **aaa group server ldap** command in configuration mode. The CLI prompt changes to (config-ldap). Use the **no** form of this command to remove an LDAP server group.

aaa group server ldap *group_name*

no aaa group server ldap *group_name*

Syntax Description

ldap	Specifies an LDAP directory server group.
group_name	Name for the group of LDAP servers. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

All commands in this mode require the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

A server group is a list of server hosts. The ACE allows you to configure multiple AAA servers as a named server group. You group the different AAA server hosts into distinct lists. The ACE searches for the server hosts in the order in which you specify them within a group. You can configure a maximum of 10 server groups for each context in the ACE.

You can configure LDAP server groups at any time, but you must enter the **aaa authentication login** command to apply the groups to the AAA service.

Examples To create an LDAP server group, enter:

```
host1/Admin(config) aaa group server ldap LDAP_Server_Group1
host1/Admin(config-ldap)# server 172.16.56.76
host1/Admin(config-ldap)# server 172.16.56.77
host1/Admin(config-ldap)# server 172.16.56.78
```

Related Commands **(config) aaa authentication login**

(config-ldap) attribute user-profile

To specify the user profile attribute that the Lightweight Directory Access Protocol (LDAP) server group uses, use the **attribute user-profile** command. Use the **no** form of this command to delete a user profile attribute from the LDAP server group.

attribute user-profile *text*

no attribute user-profile *text*

Syntax Description

text	User profile. The user profile is an unquoted text string of a maximum of 63 alphanumeric characters without spaces.

Command Modes LDAP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines The user profile attribute type is a mandatory configuration for an LDAP server group. Without this setting, the user profile attribute cannot be retrieved by the LDAP server.

The user profile attribute type is a private attribute. In this case, the LDAP server database should use the same attribute type for the user profile. The LDAP client (the ACE) sends the search request with this attribute type as the attribute that it wants to download. If the lookup was successful, the search response contains this attribute value. The attribute value should contain a string that represents the user role and domain pair for this particular context.

Examples To configure a user profile attribute for the LDAP server group, enter:

```
host1/Admin(config)# aaa group server ldap LDAP_Server_Group1
host1/Admin(config-ldap)# attribute user-profile usrprof
```

Related Commands **(config) aaa group server**

(config-ldap) baseDN

To configure the base distinguished name (DN) that you want to use to perform search operations in the LDAP directory tree, use the **baseDN** command. A baseDN can take a form such as dc=your,dc=domain, where the base DN uses the DNS domain name as its basis and is split into the domain components. Use the **no** form of this command to delete a configured baseDN for the LDAP server group.

baseDN *text*

no baseDN *text*

Syntax Description

text	Distinguished name of the search base. The baseDN name is a quoted text string of a maximum of 63 alphanumeric characters without spaces.

Command Modes

LDAP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The base DN is a mandatory configuration for an LDAP server group. Without this setting, a user cannot be authenticated.

Examples

To configure the base DN for the LDAP server group, enter:

```
host1/Admin(config)# aaa group server ldap LDAP_Server_Group1
host1/Admin(config-ldap)# baseDN "dc=sns,dc=cisco,dc=com"
```

To delete the configured base DN, enter:

```
host1/Admin(config-ldap)# no baseDN "dc=sns,dc=cisco,dc=com"
```

Related Commands

(config) aaa group server

(config-ldap) filter search-user

To configure a search request sent by the Lightweight Directory Access Protocol (LDAP) client to the server to find the user's node in the Directory Information Tree (DIT), use the **filter search-user** command. The $user and $contextid are substituted with actual values when sending the request. Use the **no** form of this command to delete the search request from the LDAP server group.

filter search-user *text*

no filter search-user *text*

Syntax Description

text	Search request. The search filter is a quoted text string of a maximum of 63 alphanumeric characters without spaces.

Command Modes

LDAP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The search filter is a mandatory configuration for an LDAP server group. Without this setting, a user cannot be authenticated.

The search filter should follow the format defined in RFC 2254. The LDAP client sends the search request with the configured search filter after replacing the $userid and $contextid with the userid that the client is trying to authenticate and the associated virtual context name.The ACE allows $userid and $contextid to be used as placeholders for user ID and context ID.

Examples

To configure a search request for the LDAP server group, enter:

```
host1/Admin(config)# aaa group server ldap LDAP_Server_Group1
host1/Admin(config-ldap)# filter search-user "(&(objectclass=person)
(&(cn=$userid)(cid=$contextid)))"
```

To delete the search request, enter:

```
host1/Admin(config-ldap)# no filter search-user
"(&(objectclass=person)(&(cn=$userid)(cid=$contextid)))"
```

Related Commands

(config) aaa group server

(config-ldap) server

To specify the IP address of one or more previously configured Lightweight Directory Access Protocol (LDAP) servers that you want added to or removed from the AAA server group, use the **server** command. Use the **no** form of this command to remove the server from the AAA server group.

server *ip_address*

no server *ip_address*

Syntax Description

ip_address	IP address of the LDAP server. Enter the address in dotted-decimal IP notation (for example, 192.168.11.1).

Command Modes

LDAP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You can add multiple LDAP servers to the AAA server group by entering multiple **server** commands while in this mode. The same server can belong to multiple server groups.

Examples

To add one or more servers to an LDAP server group, enter:

```
host1/Admin(config)# aaa group server ldap LDAP_Server_Group1
host1/Admin(config-ldap)# server 172.16.56.76
host1/Admin(config-ldap)# server 172.16.56.79
host1/Admin(config-ldap)# server 172.16.56.82
```

To remove a server from the LDAP server group, enter:

```
host1/Admin(config-ldap)# no server 172.16.56.76
```

Related Commands

(config) aaa group server

Line Configuration Mode Commands

Line configuration mode commands allow you to configure the virtual terminal line settings. To configure the virtual terminal line settings and access line configuration mode, use the **line vty** command in configuration mode. The CLI prompt changes to (config-line). For information about the commands in line configuration mode, see the following commands.

Use the **no** form of the **line vty** command to reset the line configuration mode parameter to its default setting.

line vty

no line vty

Syntax Description

This command has no keywords or arguments.

Command Modes

Configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode have no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To enter the line configuration mode, enter:

```
host1/Admin(config)# line vty
host1/Admin(config-line)#
```

Related Commands

clear line
show line

(config-line) session-limit

T o configure the maximum number of terminal sessions per line, use the **session-limit** command. Use the **no** form of this command to disable a setting for the configured virtual terminal line.

session-limit *number*

no session-limit *number*

Syntax Description

number	Maximum number of terminal sessions per line. Enter an integer from 1 to 251.

Command Modes

Line configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

For example, to configure a virtual terminal line, enter:

```
host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
host1/Admin(config)#
host1/Admin(config)# line vty
host1/Admin(config-line)# session-limit 23
```

To disable a setting for the configured virtual terminal line, enter:

```
host1/Admin(config-line)# no session-limit 23
```

Related Commands

clear line
show line
(config) line vty

Object Group Configuration Mode Commands

Object groups allow you to simplify the creation of multiple access control list (ACL) entries in an ACL. By grouping like objects together, you can use an object group in an ACL entry instead of having to enter an ACL entry for each object separately.

To create an object group and access object group configuration mode, use the **object-group** command. The CLI prompt changes to (config-objgrp-netw or config-objgrp-serv) depending upon whether you create a network or service object group. Use the **no** form of this command to delete an existing object group.

object-group [**network** | **service**] *name*

no object-group [**network** | **service**] *name*

Syntax Description

network	Specifies a group of hosts or subnet IP addresses.
service	Specifies a group of TCP or UDP port specifications or ICMP types.
name	Unique identifier of the object group. Enter the object group name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Action list modify configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

You can create either network or service object groups. After you create these groups, you can use a single ACL entry to allow trusted hosts to make specific service requests to a group of public servers.

If you add new members to an existing object group that is already in use by an entry in a large ACL, recommitting the ACL can take a long time, depending on the size of the ACL and the object group. In some cases, making this change can cause the ACE to devote over an hour to committing the ACL, during which time you cannot access the terminal. We recommend that you first remove the ACL entry that refers to the object group, make your change, and then add the ACL entry back into the ACL.

Examples

To create a network object group, enter:

```
host1/Admin(config)# object-group network NET_OBJ_GROUP1
host1/Admin(config-objgrp-netw)#
```

To create a service object group, enter:

```
host1/Admin(config)# object-group service SERV_OBJ_GROUP1
host1/Admin(config-objgrp-serv)#
```

Related Commands
(config-objgrp-netw) description
(config-objgrp-netw) host
(config-objgrp-netw) ip_address netmask

(config-objgrp-netw) description

To add an optional description to a network object group, use the **description** command. Use the **no** form of this command to remove a description from a network object group.

description *text*

no description *text*

Syntax Description

text	(Optional) Description of the network object group. Enter the description as an unquoted, alphanumeric, text string from 1 to 240 characters.

Command Modes

Network object group configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description to the network object group, enter:

```
host1/Admin(config-objgrp-netw)# description intranet network object group
```

To remove a description from the network object group, enter:

```
host1/Admin(config-objgrp-netw)# no description intranet network object group
```

Related Commands
(config) object-group
(config-objgrp-netw) host
(config-objgrp-netw) ip_address netmask

(config-objgrp-netw) host

To associate a host IP address with a network object group, use the **host** command. Use the **no** form of this command to remove a host from the network object group.

host *ip_address*

no host *ip_address*

Syntax Description

ip_address	Host IP address associated with the network object group. Enter an IP address in dotted-decimal notation (for example, 192.168.12.15).

Command Modes

Network object group configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To associate host IP address 192.168.12.15 with a network object group, enter:

```
host1/Admin(config-objgrp-netw)# host 192.168.12.15
```

To remove host IP address 192.168.12.15 from the network object group, enter:

```
host1/Admin(config-objgrp-netw)# no host 192.168.12.15
```

Related Commands

(config) object-group
(config-objgrp-netw) description
(config-objgrp-netw) ip_address netmask

(config-objgrp-netw) *ip_address netmask*

To associate a network IP address with a network object group, use the *ip_address* command. Use the **no** form of this command to remove an IP address or host from the network object group.

ip_address netmask

no *ip_address netmask*

Syntax Description

ip_address	IP address assigned to the network object group. Enter an IP address in dotted-decimal notation (for example, 192.168.12.15).
netmask	Network mask applied to the IP address. Enter a network mask in dotted decimal notation (for example, 255.255.255.0).

Command Modes

Network object group configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add the IP address 192.168.12.15 and network mask 255.255.255.0 to a network object group, enter:

```
host1/Admin(config-objgrp-netw)# 192.168.12.15 255.255.255.0
```

To remove an IP address from the network object group, enter:

```
host1/Admin(config-objgrp-netw)# no 192.168.12.15 255.255.255.0
```

Related Commands

(config) object-group
(config-objgrp-netw) description
(config-objgrp-netw) host

(config-objgrp-serv) description

To add an optional description to a service object group, use the **description** command. Use the **no** form of this command to remove a description from a service object group.

description *text*

no description *text*

Syntax Description

text	(Optional) Description of the service object group. Enter the description as an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Service object group configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description to the service object group, enter:

```
host1/Admin(config-objgrp-serv)# description intranet service object group
```

To remove a description from the service object group, enter:

```
host1/Admin(config-objgrp-serv)# no description intranet service object group
```

Related Commands

(config) object-group
(config-objgrp-serv) protocol

(config-objgrp-serv) *protocol*

To associate a protocol and port designation with a service object group, use the *protocol* command. Use the **no** form of this command to remove the protocol and port designation from a service object group.

protocol [**source** *operator port1* [*port2*]] [*operator port3* [*port4*]] [**icmp-type** *type* **code** *operator code1 code2*]

no *protocol* [**source** *operator port1* [*port2*]] [*operator port3* [*port4*]] [**icmp-type** *type* **code** *operator code1 code2*]

Syntax Description

protocol	Name or number of an IP protocol. Enter a protocol name or an integer from 1 to 255 that represents an IP protocol number. See Table 2-8.
source	Specifies a source port for TCP, TCP-UDP, or UDP. To specify a destination port, use the *operator* argument with no keyword.
operator	(Optional) Operand used to compare source and destination port numbers for TCP and UDP protocols, and message codes for ICMP. To specify a destination port, use the *operator* argument with no keyword.The operators are as follows: • **lt**—Less than. • **gt**—Greater than. • **eq**—Equal to. • **neq**—Not equal to. • **range**—An inclusive range of port values or ICMP message codes. If you enter this operator, enter a second port number value or second ICMP message code to define the upper limit of the range.
port1 [*port2*]	TCP or UDP source name or port number from which you permit or deny services access. Enter a port name or an integer from 0 to 65535. To enter an inclusive range of ports, enter two port numbers. *Port2* must be greater than or equal to *port1*. See Table 2-9 for a list of well-known TCP keywords and port numbers and Table 2-10 for a list of well-known UDP key words and port numbers.
port3 [*port4*]	TCP or UDP destination name or port number to which you permit or deny services access. To enter an optional inclusive range of ports, enter two port numbers. *port4* must be greater than or equal to *port3*. See Table 2-9 for a list of well-known TCP keywords and port numbers and Table 2-10 for a list of well-known UDP keywords and port numbers.
icmp-type *type*	(Optional) If you entered ICMP as the protocol, specifies the type of ICMP messaging. Enter either an integer corresponding to the ICMP code number or one of the ICMP types listed in Table 2-11.
code	(Optional) Specifies that a numeric operator and ICMP code follows.
code1 [*code2*]	ICMP code number that corresponds to an ICMP type. See Table 2-11. If you entered the **range** operator, enter a second ICMP code value to define the upper limit of the range.

Table 2-8 Supported Protocol Keywords and Numbers

Protocol Name	Protocol Number	Description
ah	**51**	Authentication Header
eigrp	**88**	Enhanced IGRP
esp	**50**	Encapsulated Security Payload
gre	**47**	Generic Routing Encapsulation
icmp	**1**	Internet Control Message Protocol
igmp	**2**	Internet Group Management Protocol
ip	**any**	Internet Protocol
ip-in-ip	**4**	IP-in-IP Layer 3 Tunneling Protocol
ospf	**89**	Open Shortest Path First
pim	**103**	Protocol Independent Multicast
tcp	**6**	Transmission Control Protocol
tcp-udp	**6 and 17**	TCP and UDP
udp	**17**	User Datagram Protocol

Table 2-9 Well-Known TCP Port Numbers and Keywords

Keyword	Port Number	Description
aol	**5190**	America-Online
bgp	**179**	Border Gateway Protocol
chargen	**19**	Character Generator
citrix-ica	**1494**	Citrix Independent Computing Architecture Protocol
cmd	**514**	Same as exec, with automatic authentication
ctiqbe	**2748**	Computer Telephony Interface Quick Buffer Encoding
daytime	**13**	Daytime
discard	**9**	Discard
domain	**53**	Domain Name System
echo	**7**	Echo
exec	**512**	Exec (RSH)
finger	**79**	Finger
ftp	**21**	File Transfer Protocol
ftp-data	**20**	FTP data connections
gopher	**70**	Gopher
h323	**1720**	H.323 call signaling
hostname	**101**	NIC hostname server

Table 2-9 Well-Known TCP Port Numbers and Keywords (continued)

Keyword	Port Number	Description
http	**80**	Hypertext Transfer Protocol
https	**443**	HTTP over TLS/SSL
ident	**113**	Ident Protocol
imap4	**143**	Internet Message Access Protocol, version 4
irc	**194**	Internet Relay Chat
kerberos	**88**	Kerberos
klogin	**543**	Kerberos Login
kshell	**544**	Kerberos Shell
ldap	**389**	Lightweight Directory Access Protocol
ldaps	**636**	LDAP over TLS/SSL
login	**513**	Login (rlogin)
lotusnotes	**1352**	IBM Lotus Notes
lpd	**515**	Printer Service
matip-a	**350**	Mapping of Airline Traffic over Internet Protocol Type A
netbios-ssn	**139**	NetBIOS Session Service
nntp	**119**	Network News Transport Protocol
pcanywhere-data	**5631**	PC Anywhere data
pim-auto-rp	**496**	PIM Auto-RP
pop2	**109**	Post Office Protocol v2
pop3	**110**	Post Office Protocol v3
pptp	**1723**	Point-to-Point Tunneling Protocol, RFC 2637
rtsp	**554**	Real-Time Streaming Protocol
sip	**5060**	Session Initiation Protocol
skinny	**2000**	Cisco Skinny Client Control Protocol (SCCP)
smtp	**25**	Simple Mail Transfer Protocol
sqlnet	**1521**	Structured Query Language Network
ssh	**22**	Secure Shell
sunrpc	**111**	Sun Remote Procedure Call
tacacs	**49**	Terminal Access Controller Access Control System
talk	**517**	Talk
telnet	**23**	Telnet
time	**37**	Time

Table 2-9 Well-Known TCP Port Numbers and Keywords (continued)

Keyword	Port Number	Description
uucp	**540**	Unix-to-Unix Copy Program
whois	**43**	Nicname
www	**80**	World Wide Web (HTTP)

Table 2-10 Well-Known UDP Keywords and Port Numbers

Keyword	Port Number	Description
biff	**512**	Mail notification
bootpc	**68**	Bootstrap Protocol client
bootps	**67**	Bootstrap Protocol server
discard	**9**	Discard
dnsix	**195**	DNSIX Security protocol auditing (dn6-nlm-aud)
domain	**53**	Domain Name System
echo	**7**	Echo
isakmp	**500**	Internet Security Association Key Management Protocol
kerberos	**88**	Kerberos
mobile-ip	**434**	Mobile IP registration
nameserver	**42**	Host Name Server
netbios-dgm	**138**	NetBIOS datagram service
netbios-ns	**137**	NetBIOS name service
netbios-ssn	**139**	NetBIOS Session Service
ntp	**123**	Network Time Protocol
pcanywhere-status	**5632**	PC Anywhere status
radius	**1812**	Remote Authentication Dial-in User Service
radius-acct	**1813**	RADIUS Accounting
rip	**520**	Routing Information Protocol
snmp	**161**	Simple Network Management Protocol
snmptrap	**162**	SNMP Traps
sunrpc	**111**	Sun Remote Procedure Call
syslog	**514**	System Logger
tacacs	**49**	Terminal Access Controller Access Control System
talk	**517**	Talk
tftp	**69**	Trivial File Transfer Protocol

Table 2-10 Well-Known UDP Keywords and Port Numbers (continued)

Keyword	Port Number	Description
time	**37**	Time
who	**513**	Who service (rwho)
wsp	**9200**	Connectionless Wireless Session Protocol
wsp-wtls	**9202**	Secure Connectionless WSP
wsp-wtp	**9201**	Connection-based WSP
wsp-wtp-wtls	**9203**	Secure Connection-based WSP
xdmcp	**177**	X Display Manager Control Protocol

Table 2-11 ICMP Types

ICMP Code Number	ICMP Type
0	**echo-reply**
3	**unreachable**
4	**source-quench**
5	**redirect**
6	**alternate-address**
8	**echo**
9	**router-advertisement**
10	**router-solicitation**
11	**time-exceeded**
12	**parameter-problem**
13	**timestamp-request**
14	**timestamp-reply**
15	**information-request**
16	**information-reply**
17	**mask-request**
18	**mask-reply**
30	**traceroute**
31	**conversion-error**
32	**mobile-redirect**

Command Modes

Service object group configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

For example, to add the TCP protocol to a service object group, enter:

```
host1/Admin(config-objgrp-serv)# 6
```

Enter additional service object group protocols as required.

To remove the TCP protocol from a service object group, enter:

```
host1/Admin(config-objgrp-prot)# no 6
```

For example, to create a service object group for TCP, UDP, and ICMP, enter:

```
ISM/Admin(config)# object-group service TCP_UDP_ICMP
ISM/Admin(config-objgrp-serv)# tcp source eq domain eq hostname
ISM/Admin(config-objgrp-serv)# udp source eq radius eq radius-acct
ISM/Admin(config-objgrp-serv)# icmp echo code eq 0
```

To remove the ICMP protocol from the above service object group, enter:

```
host1/Admin(config-objgrp-prot)# no icmp echo code eq 0
```

Related Commands

(config) object-group
(config-objgrp-serv) description

Optimize Configuration Mode Commands

The optimize mode includes a set of commands that allow you to globally configure application acceleration and optimization operation on the ACE. To remove an optimize mode selection, use the **no** form of the command. For details about using the commands in the optimize mode, see the *Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide*.

To access the optimize mode, enter the **optimize** command. The CLI prompt changes to (config-optimize).

optimize

no optimize

Syntax Description

This command has no keywords or arguments.

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To access the optimize mode, enter:

```
host1/Admin(config)# optimize
host1/Admin(config-optimize)#
```

Related Commands

show optimization-global

(config-optimize) appscope-log

To configure the ACE to upload the application acceleration and optimization statistical log information to the optional Cisco AVS 3180A Management Station, use the **appscope-log** command. Use the **no** form of this command to disable sending statistical log information to a Management Station.

appscope-log

no appscope-log

Syntax Description

This command has no keywords or arguments.

Command Modes

Optimize mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The statistical log file contains an entry for each ACE optimization request to the server and is used for statistical analysis by the optional Cisco AVS 3180A Management Station. The ACE collects statistical log data and then sends it to the Management Station for loading into the management station database. For details about the optional Cisco AVS 3180A Management Station database, management, and reporting features, including AppScope reporting, see the *Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide*.

To enable the AppScope feature, use the **appscope** command in action list optimization configuration mode. See the (config-actlist-optm) appscope command.

For each ACE request, information about the statistical log is written to the statlog.*nnn* file, where *nnn* is a three-digit number. Each entry in the statlog file is written in an XML-like syntax, where each element is opened with an angle-bracketed tag, and closed with a similar tag, and can contain several fields with nested elements.

Note Statistical log information from active ACE nodes is carried by the syslog-ng daemon to the Cisco AVS 3180A Management Console and written to a file under the avs-log/syslog/ directory. The file is <optm-id>_<virtual-context-id>, which is unique across all ACE nodes.

To specify the host (the syslog server on the Management Station) that receives the syslog messages sent by the ACE, use the **logging host** configuration command. See the (config) logging host command. This command allows you to identify the IP address of the Management Station that will be used as the syslog server. You can specify that the host uses either UDP or TCP to send messages to the syslog server.

Examples

To specify that the information about statistical log is to be sent to a Management Station at 192.168.10.1 using TCP, enter:

```
host1/Admin(config)# optimize
host1/Admin(config-optimize)# appscope-log
host1/Admin(config-optimize)# exit
host1/Admin(config)# logging host 192.168.10.1 tcp
```

To disable sending information about the statistical log information to an AVS 3180A Management Station, enter:

```
host1/Admin(config-optimize)# no appscope-log
```

Related Commands

(config-actlist-optm) appscope
(config-parammap-optmz) appscope optimize-rate-percent
(config-parammap-optmz) parameter-summary parameter-value-limit
(config-parammap-optmz) request-grouping-string

(config-optimize) concurrent-connections limit

To define the concurrent connection limit at which optimization will be disabled for all new connections that are received by the ACE, use the **concurrent-connections limit** command. Use the **no** form of this command to return to the default conncurrent connection limit of 1000.

concurrent-connections limit *connection_limit*

no concurrent-connections limit

Syntax Description

connection_limit	Maximum concurrent connection limit. Enter an integer from 100 to 9500. The default is 1000.

Command Modes

Optimize mode

Admin and user contexts

Command History

Release	Modification
A1(8)	This command was introduced.

Usage Guidelines

When you use the ACE to perform a specific set of application acceleration and optimization functions, and the ACE reaches the maximum of 10,000 concurrent connections, the appliance stops accepting any additional concurrent connections until the count drops below 10,000. You can define the limit at which all new connections are directly sent to the real server without the ACE performing application acceleration and optimization. This user-defined limit bypasses application acceleration and optimization requests on a connection until the concurrent connection count is less than the allowed specified maximum of 9,500 concurrent connections.

The ACE will always perform application acceleration and optimization for FlashForward URLs, AppScope URLs, and base file URLs in a new connection even if you have specified a concurrent connection limit.

Note The **show stats loadbalance** command in Exec mode displays the optimized connection counter (maximum and concurrent) and the unoptimized connection counter for all application acceleration connections.

Examples To specify a concurrent connection limit of 5000, enter:

```
host1/Admin(config)# optimize
host1/Admin(config-optimize)# concurrent-connections limit 5000
```

To return to the default conncurrent connection limit of 1000, enter:

```
host1/Admin(config-optimize)# no concurrent-connections limit
```

Related Commands This command has no related commands.

(config-optimize) debug-level

To enable HTTP optimization logging and control the maximum level for system log messages sent to the host (the syslog server on the optional Cisco AVS 3180A Management Station), use the **debug-level** command. Use the **no** form of the command to disable the debug function for HTTP optimization.

debug-level *severity_level*

no debug-level *severity_level*

Syntax Description

severity_level	Maximum level for system log messages sent to a syslog server. The severity level that you specify indicates that you want syslog messages at that level and messages lower than that level. For example, if the specified level is 3, the syslog displays level 3, 2, 1, and 0 messages. The severity level that you specify indicates that you want to log messages at that level and below. Allowable entries are as follows: • **0**—emergencies (system unusable messages) • **1**—alerts (take immediate action) • **2**—critical (critical condition) • **3**—errors (error message) • **4**—warnings (warning message) • **5**—notifications (normal but significant condition) • **6**—informational (information message) • **7**—debugging (debug messages)

Command Modes Optimize mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The **debug-level** command limits the HTTP optimization logging messages sent to a syslog server based on severity.

To specify the host (the syslog server on the optional Management Station) that receives the syslog messages sent by the ACE, use the **logging host** configuration command. See the (config) logging host command. You can specify that the host uses either UDP or TCP to send messages to the syslog server.

Examples

To enable HTTP optimization logging and send informational system message logs to the syslog server, enter:

```
host1/Admin(config)# debug-level 6
```

To disable the debug function for HTTP optimization, enter:

```
host1/Admin(config)# no debug-level
```

Related Commands

(config-parammap-optmz) appscope optimize-rate-percent
(config-parammap-optmz) parameter-summary parameter-value-limit
(config-parammap-optmz) request-grouping-string

Parameter Map Connection Configuration Mode Commands

Parameter map connection configuration mode commands allow you to define a connection-type parameter map. After you create the connection parameter map, you can configure TCP, IP, and other settings for the map. To create the connection parameter map and access parameter map connection configuration mode, use the **parameter-map type connection** command in configuration mode. The prompt changes to (config-parammap-conn). Use the **no** form of this command to remove the parameter map from the configuration.

parameter-map type connection *name*

no parameter-map type connection *name*

Syntax Description

name	Name assigned to the parameter map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the connection feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

After you create and configure a parameter map, you must associate the parameter map with a policy map to activate it. For details, see the **(config-pmap-c) connection advanced-options** command in the "Policy Map Configuration Mode Commands" section.

Examples

To create a connection parameter map called TCP_MAP, enter:

```
host1/Admin(config)# parameter-map type connection TCP_MAP
host1/Admin(config-parammap-conn)#
```

To delete the connection parameter map, enter:

```
host1/Admin(config)# no parameter-map type connection TCP_MAP
```

Related Commands

(config) parameter-map type
(config-pmap-c) connection advanced-options
show parameter-map

(config-parammap-conn) description

To add a description for the parameter map, use the **description** command. Use the **no** form of this command to remove the description from the parameter map.

description *text_string*

no description

Syntax Description

text_string	Description for the action list. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Parameter map connection configuration mode

Admin and user contexts

Command History

Release	Modification
A3(2.3)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description for the connection parameter map, enter:

```
host1/Admin(config)# parameter-map type connection TCP_MAP
host1/Admin(config-parammap-conn)# description TCP CONNECTION PARAMETER MAP
```

To remove the description from the connection parameter map, enter:

```
host1/Admin(config-parammap-conn)# no description
```

Related Commands

show parameter-map

(config-parammap-conn) exceed-mss

To configure the ACE to allow segments that exceed the maximum segment size (MSS), use the **exceed-mss** command. Use the **no** form of this command to reset the ACE to its default of discarding segments that exceed the MSS.

exceed-mss {**allow** | **drop**}

no exceed-mss

Syntax Description

allow	Permits segments that exceed the maximum segment size.
drop	Discards segments that exceed the maximum segment size. This is the default.

Command Modes

Parameter map connection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To configure the ACE to allow segments that exceed the MSS, enter:

```
host1/Admin(config-parammap-conn)# exceed-mss allow
```

To configure the ACE to discard segments that exceed the MSS, enter:

```
host1/Admin(config-parammap-conn)# exceed-mss drop
```

To reset the ACE behavior to the default of discarding segments that exceed the MSS, enter:

```
host1/Admin(config-parammap-conn)# no exceed-mss allow
```

Related Commands

(config-parammap-conn) set tcp mss
show parameter-map

(config-parammap-conn) nagle

To enable Nagle's algorithm, use the **nagle** command. By default, this command is disabled. Nagle's algorithm instructs a sender to buffer any data to be sent until all outstanding data has been acknowledged or until there is a full segment of data to send. Use the **no** form of this command to disable Nagle's algorithm.

nagle

no nagle

Syntax Description

This command has no keywords or arguments.

Command Modes

Parameter map connection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Nagle's algorithm automatically concatenates a number of small buffer messages that are transmitted over the TCP connection. This process increases throughput by decreasing the number of segments that need to be sent over the network. However, the interaction between Nagle's algorithm and the TCP delay acknowledgment may increase latency in your TCP connection. You should disable Nagle's algorithm if you notice delays in your TCP connection.

Examples

To enable Nagle's algorithm, enter:

```
host1/Admin(config-parammap-conn)# nagle
```

To disable Nagle's algorithm, enter:

```
host1/Admin(config-parammap-conn)# no nagle
```

Related Commands

show parameter-map

(config-parammap-conn) random-sequence-number

To enable TCP sequence number randomization, use the **random-sequence-number** command. This feature is enabled by default. Use the **no** form of this command to disable sequence number randomization.

random-sequence-number

no random-sequence-number

Syntax Description

This command has no keywords or arguments.

Command Modes

Parameter map connection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Randomizing TCP sequence numbers makes it more difficult for a hacker to guess or predict the next sequence number in a TCP connection.

Examples

To enable sequence number randomization, enter:

```
host1/Admin(config-parammap-conn)# random-sequence-number
```

To disable sequence number randomization, enter:

```
host1/Admin(config-parammap-conn)# no random-sequence-number
```

Related Commands

show parameter-map

(config-parammap-conn) rate-limit

To limit the connection rate or the bandwidth rate of a policy, use the **rate-limit** command. Use the **no** form of this command to return the behavior of the ACE to the default of not limiting the policy bandwidth rate.

rate-limit {**connection** *number1* | **bandwidth** *number2*}

no rate-limit {**connection** *number1* | **bandwidth** *number2*}

Syntax Description

connection *number1*	Specifies the connection-rate limit for a policy in connections per second. Enter an integer from 0 to 350000. There is no default value.
bandwidth *number2*	Specifies the bandwidth-rate limit for a policy in bytes per second. Enter an integer from 0 to 300000000. There is no default value.

Command Modes

Parameter map connection configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

In addition to preserving system resources by limiting the total number of active connections to a real server, the ACE allows you to limit the connection rate and the bandwidth rate of a policy map. The connection rate is the number of connections per second that match the policy. The bandwidth rate is the number of bytes per second that match the policy. The ACE applies these rate limits to each class map that you associate with the policy at the virtual server level.

When the connection-rate limit or the bandwidth-rate limit is reached, the ACE blocks any further traffic that matches that policy until the connection rate or bandwidth rate drops below the configured limit. By default, the ACE does not limit the connection rate or the bandwidth rate of a policy.

You can also limit the connection rate and the bandwidth rate of a real server in a server farm. For details, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*

Examples

To limit the connection rate of a policy to 100000 connections per second, enter:

```
host1/Admin(config-parammap-conn)# rate-limit connection 100000
```

To return the behavior of the ACE to the default of not limiting the policy connection rate, enter:

```
host1/Admin(config-parammap-conn)# no rate-limit connection 100000
```

To limit the policy bandwidth rate to 5000000 bytes per second, enter:

```
host1/Admin(config-parammap-conn)# rate-limit bandwidth 50000000
```

To return the behavior of the ACE to the default of not limiting the policy bandwidth rate, enter:

```
host1/Admin(config-parammap-conn)# no rate-limit bandwidth 50000000
```

Related Commands show parameter-map

(config-parammap-conn) reserved-bits

To configure how an ACE handles segments with the reserved bits set in the TCP header, use the **reserved-bits** command. Use the **no** form of this command to reset the ACE to its default of clearing reserved bits set in the TCP header of a segment.

reserved-bits {**allow** | **clear** | **drop**}

no reserved-bits

Syntax Description

allow	Permits segments with the reserved bits set in the TCP header.
clear	Clears the reserved bits in the TCP header and allows the segment. This is the default.
drop	Discards segments with reserved bits set in the TCP header.

Command Modes

Parameter map connection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The six reserved bits in the TCP header are for future use and have a value of 0.

Examples

To configure the ACE to allow segments with the reserved bits set in the TCP header, enter:

```
host1/Admin(config-parammap-conn)# reserved-bits allow
```

To reset the ACE to its default of clearing reserved bits set in the TCP header of a segment, enter:

```
host1/Admin(config-parammap-conn)# no reserved-bits allow
```

Related Commands show parameter-map

(config-parammap-conn) set ip tos

To set the type of service (ToS) for packets in a particular traffic class, use the **set ip tos** command. Use the **no** form of this command to instruct the ACE to not rewrite the IP ToS value.

set ip tos *number*

no set ip tos

Syntax Description

number	Packet ToS value. Enter an integer from 0 to 255.

Command Modes

Parameter map connection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The ToS for a packet determines how the network handles the packet and balances its precedence, delay, throughput, and reliability. This information resides in the IP header.

For details about the ToS byte, see RFCs 791, 1122, 1349, and 3168.

Examples

To set a packet's ToS value to 20, enter:

```
host1/Admin(config-parammap)# set ip tos 20
```

To instruct the ACE to ignore the ToS of a packet, enter:

```
host1/Admin(config-parammap)# no set ip tos
```

Related Commands show parameter-map

(config-parammap-conn) set tcp ack-delay

To configure an ACK delay, use the **set tcp ack-delay** command. You can configure the ACE to delay sending the ACK from a client to a server. Some applications delay the ACK for best performance. To reset the ACK delay timer to the default value of 200 ms, use the **no** form of this command.

set tcp ack-delay *number*

no set tcp ack-delay

Syntax Description

number	Delay time for sending an ACK from a client to a server. Enter an integer from 0 to 400 ms. The default is 200 ms.

Command Modes

Connection parameter-map configuration mode

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Delaying the ACK can help reduce congestion by sending one ACK for multiple segments rather than sending an ACK for each segment.

Examples

To delay sending an ACK for 400 ms, enter:

```
host1/Admin(config-parammap-conn)# set tcp ack-delay 400
```

To reset the ACK delay timer to the default of 200 ms, enter:

```
host1/Admin(config-parammap-conn)# no set tcp ack-delay
```

Related Commands

show parameter-map

(config-parammap-conn) set tcp buffer-share

To set the maximum receive or transmit buffer share size for each TCP and UDP connection, use the **set tcp buffer-share** command. Use the **no** form of this command to reset the buffer limit to the default of 32768 bytes.

set tcp buffer-share *number*

no set tcp buffer-share

Syntax Description

number	Maximum size of the receive or transmit buffer share in bytes for each TCP and UDP connection. Enter an integer from 8192 to 262143. The default is 32768 bytes.

Command Modes

Parameter map connection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(2.2)	This command now allows you to configure the buffer limit for UDP connections. Previously, the buffer limit was configurable only for TCP connections.

Usage Guidelines

To improve throughput and overall performance, the ACE checks the number of buffered bytes on a TCP and UDP connection against the configured buffer setting before accepting new receive or transmit data. By default, the maximum size of the receive or transmit buffer for each TCP or UDP connection is 32768 bytes. For large bandwidth and delay network connections, you may want to increase the default buffer size to improve your network performance.

Examples

To specify a maximum receive buffer share size of 16384 bytes, enter:

```
host1/Admin(config-parammap-conn)# set tcp buffer-share 16384
```

To reset the buffer limit to the default of 65535 bytes, enter:

```
host1/Admin(config-parammap-conn)# no set tcp buffer-share
```

Related Commands

show parameter-map

(config-parammap-conn) set tcp mss

To set a range of values for the TCP maximum segment size (MSS), use the **set tcp mss** command. Use the **no** form of this command to reset the minimum MSS to the default of 0 bytes and the maximum MSS to the default of 1460.

set tcp mss min *number1* **max** *number2*

no set tcp mss

Syntax Description

min *number1*	Specifies the smallest segment size in bytes that the ACE will accept. Enter an integer from 0 to 65535. The default is 0 bytes. If the ACE receives a segment smaller than the configured minimum size, the appliance discards the segment.
max *number2*	Specifies the largest segment size in bytes that the ACE will accept. Enter an integer from 0 to 65535. The default is 1460 bytes. If the ACE receives a segment larger than the configured maximum size, the appliance discards the segment.

Command Modes

Parameter map connection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The MSS is the largest amount of TCP data that the ACE accepts in one segment. To prevent the transmission of many smaller segments or very large segments that may require fragmentation, you can set the minimum and maximum acceptable sizes of the MSS.

Both the host and the server can set the MSS when they first establish a connection. If either maximum value exceeds the value that you set with the **set tcp mss max** command, then the ACE overrides the maximum value and inserts the value that you set. If either maximum value is less than the value that you set with the **set tcp mss min** command, then the ACE overrides the maximum value and inserts the minimum value (the minimum value is actually the smallest maximum allowed). For example, if you set a maximum value of 1200 bytes and a minimum value of 400 bytes, when a host requests a maximum value of 1300 bytes, then the ACE alters the packet to request 1200 bytes (the maximum). If another host requests a maximum value of 300 bytes, then the ACE alters the packet to request 400 bytes (the minimum).

If the host or server does not request an MSS, the ACE assumes that the RFC 793 default value of 536 bytes is in effect.

Examples

To set the minimum acceptable MSS value to 768 bytes and the maximum acceptable MSS value to 1500, enter:

```
host1/Admin(config-parammap-conn)# set tcp mss min 768 max 1500
```

To reset the minimum MSS to the default of 0 bytes and the maximum MSS to the default of 1460, enter:

```
host1/Admin(config-parammap-conn)# no set tcp mss
```

Related Commands

(config-parammap-conn) exceed-mss
show parameter-map

(config-parammap-conn) set tcp syn-retry

To set the maximum number of attempts that the ACE can take to transmit a TCP segment, use the **set tcp syn-retry** *number* command. Use the **no** form of this command to reset the maximum number of TCP SYN retires to the default of 4.

set tcp syn-retry *number*

no set tcp syn-retry

Syntax Description

number	Number of SYN retries. Enter an integer from 1 to 15. The default is 4.

Command Modes

Parameter map connection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To set the maximum number of attempts that the ACE takes to transmit a TCP segment to 3, enter:

```
host1/Admin(config-parammap-conn)# set tcp syn-retry 3
```

To reset the maximum number of TCP SYN retries to the default of 4, enter:

```
host1/Admin(config-parammap-conn)# no set tcp syn-retry
```

Related Commands

show parameter-map

(config-parammap-conn) set tcp timeout

To configure a timeout for TCP embryonic connections (connections that result from an incomplete three-way handshake) and half-closed connections (connections where the client has sent a FIN and the server has not responded), use the **set tcp timeout** command. Use the **no** form of this command to reset TCP timeout values to their default settings.

set tcp timeout {**embryonic** *seconds* | **half-closed** *seconds*}

no set tcp timeout {**embryonic** | **half-closed**}

Syntax Description

embryonic	Specifies the timeout for embryonic connections.
seconds	Time in seconds after which the ACE times out an embryonic connection. Enter an integer from 0 to 4294967295. The default is 5 seconds. A value of 0 specifies that the ACE never time out an embryonic connection.
half-closed	Specifies the timeout for half-closed connections.
seconds	Time in seconds after which the ACE times out a half-closed connection. Enter an integer from 0 to 4294967295. The default is 3600 seconds (1 hour). A value of 0 specifies that the ACE never time out a half-closed TCP connection.

Command Modes

Parameter map connection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The **set tcp timeout embryonic** command affects only Layer 4 flows and not Layer 7 flows.

Examples

To set the TCP timeout for embryonic connections to 24 seconds, enter:

```
host1/Admin(config-parammap-conn)# set tcp timeout embryonic 24
```

To reset the TCP half-closed connection timeout to the default of 600 seconds, enter:

```
host1/Admin(config-parammap-conn)# no set tcp timeout half-closed
```

Related Commands

show parameter-map

(config-parammap-conn) set tcp wan-optimization

To control how the ACE applies TCP optimizations to packets on a connection associated with a Layer 7 policy map using a round-trip time (RTT) value, use the **set tcp wan-optimization** command. Use the **no** form of this command to restore ACE behavior to the default of not optimizing TCP connections.

set tcp wan-optimization rtt *number*

no set tcp wan-optimization rtt *number*

Syntax Description

number	RTT value. Enter an integer from 0 to 65535. The default is 65535.

Command Modes

Parameter map connection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command allows you to control how the ACE applies TCP optimizations to packets on a connection associated with a Layer 7 policy map using the following RTT values:

- For a value of 0, the ACE applies TCP optimizations to packets for the life of a connection.
- For a value of 65535 (the default), the ACE performs normal operations (no optimizations) for the life of a connection.
- For values from 1 to 65534, the ACE applies TCP optimizations to packets based on the client RTT to the ACE as follows:
  - If the actual client RTT is less than the configured RTT, the ACE performs normal operations for the life of the connection.
  - If the actual client RTT is greater than or equal to the configured RTT, the ACE performs TCP optimizations on the packets for the life of a connection.

TCP optimizations include the following connection parameter-map configuration mode operations:

- Nagle optimization algorithm
- Slow-start connection behavior
- Acknowledgement (ACK) delay timer
- Window-scale factor
- Retry settings

Examples

To set the RTT to 0 to apply TCP optimizations to packets for the life of a connection, enter:

```
host1/C1(config-parammap-conn)# set tcp wan-optimization rtt 0
```

To restore the ACE behavior to the default of not optimizing TCP connections, enter:

```
host1/C1(config-parammap-conn)# no set tcp wan-optimization rtt
```

Related Commands show parameter-map

(config-parammap-conn) set tcp window-scale

To configure a TCP window-scale factor for network paths with high-bandwidth, long-delay characteristics, use the **set tcp window-scale** command. Use the **no** form of this command to reset the window-scale factor to its default setting.

set tcp window-scale *number*

no set tcp window-scale

Syntax Description

number	Window-scale factor. Enter an integer from 0 to 14. The default is 0.

Command Modes

Parameter map connection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The TCP window scaling feature adds support for the Window Scaling option in RFC 1323. We recommend increasing the window size to improve TCP performance in network paths with large bandwidth, long-delay characteristics. This type of network is called a long fat network (LFN).

The window scaling extension expands the definition of the TCP window to 32 bits and then uses a scale factor to carry this 32-bit value in the 16-bit window field of the TCP header. You can increase the window size to a maximum scale factor of 14. Typical applications use a scale factor of 3 when deployed in LFNs.

Examples

To set the TCP window-scale factor to 3, enter:

```
host1/Admin(config-parammap-conn)# set tcp window-scale 3
```

To reset the TCP window-scale factor to the default of 0, enter:

```
host1/Admin(config-parammap-conn)# no set tcp window-scale
```

Related Commands show parameter-map

(config-parammap-conn) set timeout inactivity

To configure the connection inactivity timer, use the **set timeout inactivity** command. Use the **no** form of this command to reset the timeout inactivity values to the default ICMP, TCP, and UDP settings.

set timeout inactivity *seconds*

no set timeout inactivity

Syntax Description

inactivity	Specifies the timeout for idle TCP connections.
seconds	Time period after which the ACE disconnects idle established connections. Enter an integer from 0 to 1638050. A value of 0 specifies that the ACE never time out a TCP connection. Default settings are as follows: • ICMP—2 seconds • TCP—3600 seconds (1 hour) • UDP—120 seconds (2 minutes)

Command Modes

Parameter map connection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The ACE uses the connection inactivity timer to disconnect established ICMP, TCP, and UDP connections that have remained idle for the duration of the specified timeout period.

The ACE rounds up the configured timeout value to the nearest 30-second interval.

Examples

To specify that the ACE disconnect idle established TCP connections after 2400 seconds, enter:

```
host1/Admin(config-parammap-conn)# set timeout inactivity 2400
```

To reset the ICMP, TCP, and UDP inactivity timeout to the default values, enter:

```
host1/Admin(config-parammap-conn)# no set timeout inactivity
```

Related Commands

show parameter-map

(config-parammap-conn) slowstart

To enable the slow start algorithm, use the **slowstart** command. This feature is disabled by default. Use the **no** form of this command to disable the slow start algorithm after it has been enabled.

slowstart

no slowstart

Syntax Description

This command has no keywords or arguments.

Command Modes

Parameter map connection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The slow start algorithm is a congestion avoidance method in which TCP increases its window size as ACK handshakes arrive. It operates by observing that the rate at which new segments should be injected into the network is the rate at which the acknowledgments are returned by the host at the other end of the connection. For further details about the TCP slow start algorithm, see RFC 2581 and RFC 3782.

Examples

To enable the slow start algorithm, enter:

```
host1/Admin(config-parammap-conn)# slowstart
```

To disable the slow start algorithm, enter:

```
host1/Admin(config-parammap-conn)# no slowstart
```

Related Commands

show parameter-map

(config-parammap-conn) syn-data

To set the ACE to discard SYN segments with data, use the **syn-data** command. Use the **no** form of this command to reset the ACE to its default of allowing SYN segments that contain data.

syn-data {**allow** | **drop**}

no syn-data

Syntax Description

allow	Permits the SYN segments that contain data and flags them for data processing. This is the default.
drop	Discards the SYN segments that contain data.

Command Modes

Parameter map connection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Occasionally, the ACE may receive a SYN segment that contains data. You can configure the ACE to either discard the segment or flag the segment for data processing.

Examples

To instruct the ACE to discard segments that contain data, enter:

```
host1/Admin(config-parammap-conn)# syn-data drop
```

To reset the ACE to its default of allowing SYN segments that contain data, enter:

```
host1/Admin(config-parammap-conn)# no syn-data
```

Related Commands

show parameter-map

(config-parammap-conn) tcp-options

To specify a range of TCP options not explicitly supported by the ACE, or allow or clear explicitly supported TCP options specified in a SYN segment, use the **tcp-options** command. Use the **no** form of this command to remove a TCP option range from the configuration or reset the ACE to its default of clearing the specific TCP options.

tcp-options {**range** *number1 number2* {**allow** | **drop**}} | {**selective-ack** | **timestamp** | **window-scale** {**allow** | **clear** | **drop**}}

no tcp-options {**range** *number1 number2* {**allow** | **drop**}} | {**selective-ack** | **timestamp** | **window-scale** {**allow** | **clear** | **drop**}}

Syntax Description

range *number1 number2*	Specifies the TCP options not explicitly supported by the ACE using a range of option numbers. The arguments are as follows: • *number1*—Specifies the lower limit of the TCP option range. Enter either 6 or 7 or an integer from 9 to 255. See the "Usage Guidelines" section for the available TCP options. • *number2*—Specifies the upper limit of the TCP option range. Enter 6 or 7 or an integer from 9 to 255. See the "Usage Guidelines" section for the available TCP options.
allow	Allows any segment with the specified option set.
drop	Causes the ACE to discard any segment with the specified option set.
selective-ack	Allows the ACE to inform the sender about all segments that it received. The sender needs to retransmit the lost segments, rather than wait for a cumulative acknowledgement or retransmit segments unnecessarily. Selective ACK (SACK) can reduce the number of retransmitted segments and increase throughput under some circumstances.
timestamp	Measures the round-trip time (RTT) of a TCP segment between two nodes on a network. Time stamps are always sent and echoed in both directions.
window-scale	Allows the ACE to use a window-scale factor that increases the size of the TCP send and receive buffers. The sender specifies a window-scale factor in a SYN segment that determines the send and receive window size for the duration of the connection.
clear	Clears the specified option from any segment that has it set and allows the segment. This is the default action on the explicitly supported options.

Command Modes

Parameter map connection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Using the **tcp-options** command, the ACE permits you to allow or clear the following explicitly supported TCP options specified in a SYN segment:

- Selective Acknowledgement (SACK)
- Time stamp
- Window Scale

You can specify this command multiple times to configure different options and actions. If you specify the same option with different actions, the ACE uses the order of precedence to decide which action to use.

The order of precedence for the actions in this command is as follows:

1. Drop
2. Clear
3. Allow

Table 2-12 lists the TCP options not explicitly supported by the ACE.

Table 2-12 Unsupported TCP Options

Kind	Length	Meaning	Reference
6	6	Echo (obsoleted by option 8)	RFC 1072
7	6	Echo Reply (obsoleted by option 8)	RFC 1072
9	2	Partial Order Connection Permitted	RFC 1693
10	3	Partial Order Service Profile	RFC 1693
11		CC	RFC 1644
12		CC.NEW	RFC 1644
13		CC.ECHO	RFC 1644
14	3	TCP Alternate Checksum Request	RFC 1146
15	N	TCP Alternate Checksum Data	RFC 1146
16		Skeeter	[Knowles]
17		Bubba	[Knowles]
18	3	Trailer Checksum Option	[Subbu & Monroe]
19	18	MD5 Signature Option	RFC 2385
20		SCPS Capabilities	[Scott]
21		Selective Negative Acknowledgements (SNACK)	[Scott]
22		Record Boundaries	[Scott]
23		Corruption experienced	[Scott]

Table 2-12 Unsupported TCP Options (continued)

Kind	Length	Meaning	Reference
24		SNAP	[Sukonnik]
25		Unassigned (released 12/18/00)	
26		TCP Compression Filter	[Bellovin]

Table 2-13 lists the TCP options explicitly supported by the ACE.

Table 2-13 Supported TCP Options

Kind	Length	Meaning	Reference
0	-	End of Option List	RFC 793
1	-	No Operation	RFC 793
3	3	WSOPT—Window Scale	RFC 1323
4	2	Selective Acknowledgement (SACK) Permitted	RFC 2018
5	N	SACK	RFC 2018
8	10	Time Stamp Option (TSOPT)	RFC 1323

Examples

To allow the segment with the SACK option set, enter:

```
host1/Admin(config-parammap-conn)# tcp-options selective-ack allow
```

To reset the behavior of the ACE to the default of clearing the SACK option and allowing the segment, enter:

```
host1/Admin(config-parammap-conn)# no tcp-options selective-ack allow
```

You can specify a range of options for each action. If you specify overlapping option ranges with different actions, the ACE uses the order of precedence described in the “Usage Guidelines” section to decide which action to perform for the specified options.

For example, to specify a range of options for each action, enter:

```
host1/Admin(config-parammap-conn)# tcp-options range 6 7 allow
host1/Admin(config-parammap-conn)# tcp-options range 9 18 clear
host1/Admin(config-parammap-conn)# tcp-options range 19 26 drop
```

To remove the TCP option ranges from the configuration, enter:

```
host1/Admin(config-parammap-conn)# no tcp-options range 6 7 allow
host1/Admin(config-parammap-conn)# no tcp-options range 9 18 clear
host1/Admin(config-parammap-conn)# no tcp-options range 19 26 drop
```

Related Commands

show parameter-map

(config-parammap-conn) urgent-flag

To set the Urgent Pointer policy, use the **urgent-flag** command. Use the **no** form of this command to return to the default setting of clearing the Urgent flag.

urgent-flag {**allow** | **clear**}

no urgent-flag

Syntax Description

allow	Permits the status of the Urgent flag. This is the default. If the Urgent flag is set, the offset in the Urgent Pointer that indicates the location of the urgent data is valid. If the Urgent flag is not set, the offset in the Urgent Pointer is invalid.
clear	Sets the Urgent flag to 0, which invalidates the offset in the Urgent Pointer.

Command Modes

Parameter map connection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

If the Urgent control bit (flag) is set in the TCP header, it indicates that the Urgent Pointer is valid. The Urgent Pointer contains an offset that indicates the location of the segment that follows the urgent data in the payload. Urgent data is data that should be processed as soon as possible, even before normal data is processed. The ACE permits you to allow or clear the Urgent flag. If you clear the Urgent flag, you invalidate the Urgent Pointer.

The ACE clears the Urgent flag for any traffic above Layer 4. If you have enabled server connection reuse (see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*), the ACE does not pass the Urgent flag value to the server.

Examples

To clear the Urgent flag, enter:

```
host1/Admin(config-parammap-conn)# urgent-flag clear
```

To reset the ACE to its default of allowing the Urgent flag, enter:

```
host1/Admin(config-parammap-conn)# no urgent-flag
```

Related Commands

show parameter-map

Parameter Map DNS Configuration Mode Commands

Parameter map DNS configuration mode commands allow you to define a DNS-type parameter map. After you create the DNS parameter map, you can configure a query timeout for the map. To create the DNS parameter map and access parameter map DNS configuration mode, use the **parameter-map type dns** command in configuration mode. The prompt changes to (config-parammap-dns). Use the **no** form of this command to remove the parameter map from the configuration.

parameter-map type dns *name*

no parameter-map type dns *name*

Syntax Description

name	Name assigned to the parameter map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The commands in this mode require the connection feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

After you create and configure a parameter map, you must associate the parameter map with a policy map to activate it. For details, see the **(config-pmap-c) appl-parameter dns advanced-options** command in the "Policy Map Configuration Mode Commands" section.

Examples

To create a DNS-type parameter map called TCP_MAP, enter:

```
host1/Admin(config)# parameter-map type dns TCP_MAP
host1/Admin(config-parammap-dns)#
```

To delete the DNS-type parameter map, enter:

```
host1/Admin(config)# no parameter-map type dns TCP_MAP
```

Related Commands

(config) parameter-map type
(config-pmap-c) appl-parameter dns advanced-options
show parameter-map

(config-parammap-dns) description

To add a description for the parameter map, use the **description** command. Use the **no** form of this command to remove the description from the parameter map.

description *text_string*

no description

Syntax Description

text_string	Description for the action list. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Parameter map DNS configuration mode

Admin and user contexts

Command History

Release	Modification
A3(2.3)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description for the parameter map, enter:

```
host1/Admin(config)# parameter-map type dns TCP_MAP
host1/Admin(config-parammap-dns)# description DNS-TYPE PARAMETER MAP
```

To remove the description from the parameter map, enter:

```
host1/Admin(config-parammap-dns)# no description
```

Related Commands

show parameter-map

(config-parammap-dns) timeout query

To configure the ACE to time out DNS queries that have no matching server response, use the **timeout query** command. Use the **no** form of this command to reset the ACE behavior to the default of timing out DNS queries when the underlying UDP connection times out.

timeout query {*number*}

no timeout query {*number*}

Syntax Description

number	Specifies the length of time in seconds that the ACE keeps the query entries without answers in the hash table before timing them out. Enter an integer from 2 to 120 seconds. The default is 10 seconds.

Command Modes

Parameter map DNS configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To configure the ACE to time out DNS query entries with no corresponding server responses after 20 seconds, enter:

```
host1/Admin(config-parammap-dns)# timeout query 20
```

To reset the ACE behavior to the default of timing out DNS queries without server responses when the underlying UDP connection times out, enter:

```
host1/Admin(config-parammap-dns)# no timeout query 20
```

Related Commands

show parameter-map

Parameter Map Generic Configuration Mode Commands

Parameter map generic configuration mode commands allow you to define a generic-type parameter map. After you create the generic parameter map, you can configure related parameters for the map. To create the generic parameter map and access parameter map generic configuration mode, use the **parameter-map type generic** command in configuration mode. The prompt changes to (config-parammap-generic). Use the **no** form of this command to remove the parameter map from the configuration.

parameter-map type generic *name*

no parameter-map type generic *name*

Syntax Description

name	Name assigned to the parameter map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The commands in this mode require the connection feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

After you create and configure a parameter map, you must associate the parameter map with a policy map to activate it. For details, see the **(config-pmap-c) appl-parameter generic advanced-options** command in the "Policy Map Configuration Mode Commands" section.

Examples

To create a generic parameter map called TCP_MAP, enter:

```
host1/Admin(config)# parameter-map type generic TCP_MAP
host1/Admin(config-parammap-generi)#
```

To delete the generic parameter map, enter:

```
host1/Admin(config)# no parameter-map type generic TCP_MAP
```

Related Commands

(config) parameter-map type
(config-pmap-c) appl-parameter generic advanced-options
show parameter-map

(config-parammap-generi) case-insensitive

To enable case-insensitive matching for generic matching only, use the **case-insensitive** command. With case-insensitive matching enabled, uppercase and lowercase letters are considered the same. By default, the ACE CLI is case sensitive. Use the **no** form of this command to reset the ACE to its default of case-sensitive generic matching.

case-insensitive

no case-insensitive

Syntax Description

This command has no keywords or arguments.

Command Modes

Parameter map generic configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

When enabled, case insensitivity applies to generic protocol regular expression matches.

Examples

To enable case-insensitive-matching, enter:

```
host1/Admin(config-parammap-generi)# case-insensitive
```

To reenable case-sensitive matching, enter:

```
host1/Admin(config-parammap-generi)# no case-insensitive
```

Related Commands

show parameter-map

(config-parammap-generi) description

To add a description for the parameter map, use the **description** command. Use the **no** form of this command to remove the description from the parameter map.

description *text_string*

no description

Syntax Description

text_string	Description for the action list. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Parameter map generic configuration mode

Admin and user contexts

Command History

Release	Modification
A3(2.3)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description for the parameter map, enter:

```
host1/Admin(config)# parameter-map type generic TCP_MAP
host1/Admin(config-parammap-generi)# description GENERIC-TYPE PARAMETER MAP
```

To remove the description from the parameter map, enter:

```
host1/Admin(config-parammap-generi)# no description
```

Related Commands

show parameter-map

(config-parammap-generi) set max-parse-length

You can set the maximum number of bytes to parse for generic protocols by using the **set max-parse-length** command in generic parameter-map configuration mode. The syntax of this command is as follows:

set max-parse-length *bytes*

no set max-parse-length *bytes*

Syntax Description

bytes	Maximum number of bytes to parse. Enter an integer from 1 to 65535. The default is 2048 bytes.

Command Modes

Parameter map generic configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To set the maximum parse length for generic protocols, enter the following command:

```
host1/Admin(config-parammap-generi)# set max-parse-length 8192
```

To reset the maximum parse length for generic protocols to the default value of 2048, enter the following command:

```
host1/Admin(config-parammap-generi)# no set max-parse-length
```

Related Commands

show parameter-map

Parameter Map HTTP Configuration Mode Commands

Parameter map HTTP configuration mode commands allow you to specify an HTTP-type parameter map and define its settings. To create an HTTP-type parameter map and access parameter map HTTP configuration mode, use the **parameter-map type http** command in configuration mode. The prompt changes to (config-parammap-http). Use the **no** form of this command to remove an HTTP-type parameter map from the configuration.

parameter-map type http *name*

no parameter-map type http *name*

Syntax Description

name	Name assigned to the parameter map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the connection feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

After you create and configure a parameter map, you must associate the parameter map with a policy map to activate it. For details, see the **(config-pmap-c) appl-parameter http advanced-options** command in the "Policy Map Configuration Mode Commands" section.

Examples

To create an HTTP-type parameter map called HTTP_MAP, enter:

```
host1/Admin(config)# parameter-map type http HTTP_MAP
host1/Admin(config-parammap-http)#
```

To delete the HTTP-type parameter map, enter:

```
host1/Admin(config)# no parameter-map type http HTTP_MAP
```

Related Commands

(config) parameter-map type
(config-pmap-c) appl-parameter http advanced-options
show parameter-map

(config-parammap-http) case-insensitive

To enable case-insensitive matching for HTTP matching only, use the **case-insensitive** command. With case-insensitive matching enabled, uppercase and lowercase letters are considered the same. By default, the ACE CLI is case sensitive. Use the **no** form of this command to reset the ACE to its default of case-sensitive HTTP matching.

case-insensitive

no case-insensitive

Syntax Description

This command has no keywords or arguments.

Command Modes

Parameter map HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When enabled, case insensitivity applies to the following:

- HTTP header names and values
- HTTP cookie names and values
- URL strings
- HTTP deep inspection

Examples

To enable case-insensitive-matching, enter:

```
host1/Admin(config-parammap-http)# case-insensitive
```

To reenable case-sensitive matching, enter:

```
host1/Admin(config-parammap-http)# no case-insensitive
```

Related Commands

show parameter-map

(config-parammap-http) description

To add a description for the parameter map, use the **description** command. Use the **no** form of this command to remove the description from the parameter map.

description *text_string*

no description

Syntax Description

text_string	Description for the action list. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Parameter map HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(2.3)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description for the parameter map, enter:

```
host1/Admin(config)# parameter-map type http HTTP_MAP
host1/Admin(config-parammap-http)# description HTTP-TYPE PARAMETER MAP
```

To remove the description from the parameter map, enter:

```
host1/Admin(config-parammap-http)# no description
```

Related Commands

show parameter-map

(config-parammap-http) compress

To define the parameters that the ACE uses when compressing HTTP traffic, use the **compress** command. Use the **no** form of this command to remove the HTTP compression.

compress {**mimetype** *type/subtype* | **minimum-size** *size* | **user-agent** *string*}

no compress {**mimetype** *type/subtype* | **minimum-size** *size* | **user-agent** *string*}

Syntax Description

mimetype *type/subtype*	Specifies the Multipurpose Internet Mail Extension (MIME) type to compress. The default is text/.* which includes all text MIME types, such as text/html, text/plain, and so on.
minimum-size *size*	Specifies the threshold at which compression occurs. The ACE compresses files that are the specified minimum size or larger. The default is 512 bytes.
user-agent *string*	Specifies the text string in the request to match. The ACE does not compress the response to a request when the request contains the specified user agent string. The default is none.

Command Modes

Parameter map HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To specify compression of all image MIME types, enter:

```
host1/Admin(config-parammap-http)# compress mimetype image/.*
```

To specify the user agent string .*Konqueror.*, enter:

```
host1/Admin(config-parammap-http)# compress user-agent .*Konqueror.*
```

Related Commands

(config-pmap-lb-c) compress

(config-parammap-http) header modify per-request

To instruct the ACE to modify headers (insert, delete, or rewrite) on every HTTP request or response without the additional effect of performing load balancing on each new HTTP request caused by the **persistence-rebalance** command, use the **header modify per-request** command. Use the **no** form of this command to reset the ACE to its default of case-sensitive HTTP matching.

header modify per-request

no header modify per-request

Syntax Description

This command has no keywords or arguments.

Command Modes

Parameter map HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has an effect only when **persistence-rebalance** is disabled. The **header modify per-request** command also causes the ACE to perform URL location header rewrite on every HTTP response if the **ssl url rewrite location** command is enabled. For more information about SSL URL rewrite, see the *Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide*.

Examples

To instruct the ACE to perform header modification on every HTTP request or response, enter the following command:

```
host1/Admin(config-parammap-http)# header modify per-request
```

To return the ACE behavior to the default of modifying headers only on the first HTTP request or response, enter the following command:

```
host1/Admin(config-parammap-http)# no header modify per-request
```

Related Commands

show parameter-map
(config) action-list type modify http
(config-actlist-modify) header delete
(config-actlist-modify) header insert
(config-actlist-modify) header rewrite
(config-actlist-modify) ssl url rewrite location
(config-parammap-http) persistence-rebalance
(config-pmap-lb-c) insert-http
(config-pmap-lb-m) insert-http

(config-parammap-http) length-exceed

To configure how the ACE handles URLs or cookies that exceed the maximum parse length, use the **length** command. Use the **no** form of this command to reset the ACE to its default of stopping load balancing and discarding a packet when its URL or cookie exceeds the maximum parse length.

length-exceed {**continue** | **drop**}

no length-exceed

Syntax Description

continue	Specifies that the ACE continue load balancing when the maximum parse length is exceeded.
drop	Specifies that the ACE stop load balancing when the maximum parse length is exceeded. This is the default.

Command Modes

Parameter map HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When you specify the **continue** keyword, the **(config-parammap-http) persistence-rebalance** command is disabled if the total length of all cookies, HTTP headers, and URLs exceeds the maximum parse-length value.

Examples

To continue load balancing when the maximum parse length is exceeded, enter:

```
host1/Admin(config-parammap-http)# length-exceed continue
```

To reset the ACE to its default of stopping load balancing and discarding a packet when its URL or cookie exceeds the maximum parse length, enter:

```
host1/Admin(config-parammap-http)# no length-exceed
```

Related Commands

show parameter-map
(config-parammap-http) persistence-rebalance

(config-parammap-http) persistence-rebalance

To enable the ACE to check each GET request on a TCP connection and to load balance the request only if it matches a load-balancing class map that is different from the load-balancing class map matched by the previous request, use the **persistence-rebalance** command. By default, HTTP persistence is disabled. Use the **no** form of this command to reset persistence to the default setting of disabled.

persistence-rebalance

no persistence-rebalance

Syntax Description

This command has no keywords or arguments.

Command Modes

Parameter map HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

With persistence rebalance enabled, when successive GET requests result in load balancing that chooses the same class in the same policy, the ACE sends the requests to the real server that was used for the last GET request. This behavior prevents the ACE from load balancing every request and recreating the server-side connection on every GET request, producing less overhead and better performance. If a request matches a different policy, then the ACE rebalances the server-side connection.

When persistence rebalance is disabled, the ACE load balances the first GET request on a new connection to a real server. The ACE sends successive requests on that same connection to the same server that serviced the first request because the ACE does not parse the Layer 7 information that is present in the request. In this case, load balancing is not involved after the initial load-balancing decision is made.

Another effect of persistence rebalance is that header insertion and cookie insertion, if enabled, occur for every request instead of only the first request.

If a real server is enabled with the NTLM Microsoft authentication protocol, we recommend that you leave persistence rebalance disabled. NTLM is a security measure that is used to perform authentication with Microsoft remote access protocols. When a real server is enabled with NTLM, every connection to the real server must be authenticated; typically, each client user will see a pop-up window prompting for a username and password. Once the connection is authenticated, all subsequent requests on the same connection will not be challenged. However, when the server load balancing function is enabled and configured with persistence rebalance, a subsequent request may point to a different real server causing a new authentication handshake.

The **persistence-rebalance** command is not compatible with generic protocol parsing.

Examples

To enable persistence rebalance, enter:

```
host1/Admin(config-parammap-http)# persistence-rebalance
```

To reset persistence rebalance to the default setting of disabled, enter:

```
host1/Admin(config-parammap-http)# no persistence-rebalance
```

Related Commands

show parameter-map
(config-pmap-lb-c) insert-http
(config-sticky-cookie) cookie insert

(config-parammap-http) server-conn reuse

To configure TCP server reuse, use the **server-conn reuse** command. TCP server reuse allows the ACE to reduce the number of open connections on a server by allowing connections to persist and be reused by multiple client connections. Use the **no** form of this command to disable TCP server reuse.

server-conn reuse

no server-conn reuse

Syntax Description

This command has no keywords or arguments.

Command Modes

Parameter map HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The ACE maintains a pool of TCP connections that can be reused if the client connection and the server connection share the same TCP options. For information about how the ACE handles TCP options, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*. For proper operation of this feature, follow these TCP server reuse configuration recommendations and restrictions:

- Ensure that the ACE maximum segment size (MSS) is the same as the server MSS.
- Configure Port Address Translation (PAT) on the interface that is connected to the real server. PAT prevents collisions when a client stops using a server connection and then that connection is reused by another client. Without PAT, if the original client tries to reuse the original server connection, it is no longer available. For details about configuring PAT, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.
- Configure the same TCP options that exist on the TCP server.
- Ensure that all real servers within a server farm have identical configurations.

Another effect of TCP server reuse is that header insertion and cookie insertion, if enabled, occur for every request instead of only the first request.

Examples

To enable TCP server reuse, enter:

```
host1/Admin(config-parammap-http)# server-conn reuse
```

To disable TCP server reuse, enter:

```
host1/Admin(config-parammap-http)# no server-conn reuse
```

Related Commands

show parameter-map
(config-parammap-http) persistence-rebalance
(config-pmap-lb-c) insert-http
(config-sticky-cookie) cookie insert

(config-parammap-http) set content-maxparse-length

To set the maximum number of bytes to parse in HTTP content, use the **set content-maxparse-length** command. Use the **no** form of this command to reset the maximum parse length to the default of 4096 bytes.

set content-maxparse-length *bytes*

no set content maxparse-length

Syntax Description

bytes	Maximum number of bytes to parse in HTTP content. Enter an integer from 1 to 65535. The default is 4096 bytes.

Command Modes

Parameter map HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To set the maximum parse length to 8192, enter:

```
host1/Admin(config-parammap-http)# set content-maxparse-length 8192
```

To reset the maximum parse length to the default of 4096 bytes, enter:

```
host1/Admin(config-parammap-http)# no set content-maxparse-length
```

Related Commands

show parameter-map

(config-parammap-http) set header-maxparse-length

To set the maximum number of bytes to parse for cookies, HTTP headers, and URLs, use the **set header-maxparse-length** command. Use the **no** form of this command to reset the HTTP header maximum parse length to the default of 2048 bytes.

set header-maxparse-length *bytes*

no set-header maxparse-length

Syntax Description

bytes	Maximum number of bytes to parse for the total length of all cookies, HTTP headers, and URLs. Enter an integer from 1 to 65535. The default is 2048 bytes.

Command Modes

Parameter map HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To set the HTTP header maximum parse length to 8192, enter:

```
host1/Admin(config-parammap-http)# set header-maxparse-length 8192
```

To reset the HTTP header maximum parse length to the default of 2048 bytes, enter:

```
host1/Admin(config-parammap-http)# no set header-maxparse-length
```

Related Commands

show parameter-map

(config-parammap-http) set secondary-cookie-delimiters

To define a list of ASCII-character delimiter strings that you can use to separate the cookies in a URL string, use the **set secondary-cookie-delimiters** command. Use the **no** form of this command to reset the delimiter string list to the default of /?&#+.

set secondary-cookie-delimiters *text*

no set secondary-cookie-delimiters

Syntax Description

text	Delimiter string. Enter an unquoted text string with no spaces and a maximum of four characters. The order of the delimiters in the list does not matter. The default list of delimiters is /&#+.

Command Modes

Parameter map HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Cookies and their delimiters appear in GET request lines. In the following example of a GET request line, the ampersand (&) that appears between name-value pairs is the secondary cookie delimiter. The question mark (?) begins the URL query and is not configurable.

```
GET /default.cgi?user=me&hello=world&id=2 HTTP/1.1
```

Examples

To set the delimiter string list to the characters !@#$, enter:

```
host1/Admin(config-parammap-http)# set secondary-cookie-delimiters !@#$
```

To reset the delimiter string list to the default of /?&#+, enter:

```
host1/Admin(config-parammap-http)# no set secondary-cookie-delimiters
```

Related Commands

show parameter-map

(config-parammap-http) set secondary-cookie-start

To define the ASCII-character string at the start of a secondary cookie in a URL or ignore any start string of a secondary cookie in the URL and consider the secondary cookie part of the URL, use the **set secondary-cookie-start** command. Use the **no** form of this command to reset the secondary cookie start string to the default setting of ?.

The syntax of this command is as follows:

set secondary-cookie-start {**none** | *text*}

set secondary-cookie-start

Syntax Description

none	The secondary cookie start is not configured or the ACE ignores any start string of a secondary cookie in the URL and considers the secondary cookie as part of the URL. When you configure the **none** keyword to consider the entire URL query string as part of a URL, the commands that rely on the URL query, such as the **match cookie secondary** and **predictor hash cookie secondary** commands, do not work. Do not configure these commands under the same real server.
text	The start string of the secondary cookie. Enter a maximum of two characters. The default start character is ?.

Command Modes

Parameter map HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(2.3)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To define the secondary cookie start string, enter:

```
host1/Admin(config-parammap-http)# set secondary-cookie-start ?!
```

To reset the secondary cookie start string to the default setting of ?, enter:

```
host1/Admin(config-parammap-http)# no set secondary-cookie-start
```

Related Commands

show parameter-map

Parameter Map Optimization Configuration Mode Commands

Parameter map optimization configuration mode commands allow you to create an optimization HTTP-type parameter map and define its application acceleration settings. To create an optimization HTTP-type parameter map and access parameter map optimization configuration mode, use the **parameter-map type optimization http** command in configuration mode. The prompt changes to (config-parammap-optmz). Use the **no** form of the command to remove an optimization HTTP-type parameter map from the configuration.

parameter-map type optimization http *map_name*

no parameter-map type optimization http *map_name*

Syntax Description

map_name	Enter a unique name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

An optimization HTTP parameter map can be optionally specified in an optimization HTTP policy map to identify the association between an optimization HTTP action list and the parameter map. The optimization HTTP action list defines what to do, while the optimization HTTP parameter map defines the specific details about how to accomplish the application acceleration action. For details, see the "Policy Map Management Configuration Mode Commands" section.

Examples

To create an optimization HTTP-type parameter map, enter:

```
host1/Admin(config)# parameter-map type optimization http OPTIMIZE_PARAM_MAP
host1/Admin(config-parammap-optmz)#
```

To remove a Layer 7 optimization parameter map from the configuration, enter:

```
host1/Admin(config)# no parameter-map type optimization http OPTIMIZE_PARAM_MAP
```

Related Commands

(config) parameter-map type
(config) action-list type optimization http
show parameter-map

(config-parammap-optmz) appscope optimize-rate-percent

To control the AppScope features that measure application acceleration performance by the optional Cisco AVS 3180A Management Station, use the **appscope optimize-rate-percent** command. Use the **no** form of the command to revert to the default AppScope performance rate settings.

appscope optimize-rate-percent *value* **passthru-rate-percent** *value*

no appscope optimize-rate-percent *value* **passthru-rate-percent** *value*

Syntax Description

value	Percentage of all requests (or sessions) to be sampled for performance with acceleration (optimization) applied. All applicable optimizations for the class will be performed. Valid values are from 0 to 100 percent. The default is 10 percent. This value plus the passthru-rate-percent value must not exceed 100.
passthru-rate-percent *value*	Percentage of all requests (or sessions) to be sampled for performance without optimization. No optimizations for the class will be performed. Valid values are from 0 to 100 percent. The default is 10 percent. This value plus the optimize-rate-percent value must not exceed 100.

Command Modes

Parameter map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The statistical log contains an entry for each ACE optimization request to the server and is used for statistical analysis by the optional Cisco AVS 3180A Management Station. The ACE collects statistical log and sends it to the Cisco AVS 3180A Management Station for loading into the database. For details about the use of the Cisco AVS 3180A Management Station for database, management, and reporting features for the ACE optimization functionality, including AppScope reporting, see the *Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide*.

To control the AppScope features that measure application acceleration and optimization performance, use the **appscope** commands in action list optimization configuration mode. See the "Action List Optimization Configuration Mode Commands" section for details.

To specify the host (the syslog server on the Management Station) that receives the syslog messages sent by the ACE, use the **logging host** configuration command. See the (config) logging host command. This command allows you to identify the IP address of the Management Station that will be used as the syslog server. You can specify that the host uses either UDP or TCP to send messages to the syslog server.

Examples

To specify a percentage of all requests (or sessions) to be sampled for performance with acceleration and without optimization applied by AppScope, enter:

```
host1/Admin(config-parammap-optmz)# appscope optimize-rate-percent 50
passthru-rate-percent 50
```

To revert to the default rate AppScope performance rate settings of 10 percent, enter:

```
host1/Admin(config-parammap-optmz)# no appscope optimize-rate-percent 50
passthru-rate-percent 50
```

Related Commands

(config-actlist-optm) appscope
(config-parammap-optmz) request-grouping-string

(config-parammap-optmz) basefile anonymous-level

To define the base file anonymity level for the all-user delta optimization method, use the **basefile anonymous-level** command. By default, the base file anonymity level is disabled. Use the **no** form of the command to revert to the default base file anonymity level of 0.

basefile anonymous-level *value*

no basefile anonymous-level *value*

Syntax Description

value	Base file anonymity level for the all-user delta optimization method. Valid values are from 0 to 50. The default is a value of 0 (disables anonymity).

Command Modes

Parameter map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The string can contain a URL regular expression that defines a set of URLs in which URLs that differ only by their query parameters are to be treated as separate URLs in AppScope reports.

Typically, in an AppScope report organized by URL, matching URLs that differ only in their query parameters are treated as the same URL and are not listed on separate lines. Use the **request-grouping-string** command to specify that all URL variations that are based on query parameters are to be treated as separate URLs for reporting purposes. Each variation will appear on a separate line in the report.

For details about the optional Cisco AVS 3180A Management Station database, management, and reporting features for the ACE optimization functionality, including AppScope reporting, see the *Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide*.

Examples

To specify a base file anonymity level of 25, enter:

```
host1/Admin(config-parammap-optmz)# basefile anonymous-level 25
```

To revert to the default base file anonymity level of 0, enter:

```
host1/Admin(config-parammap-optmz)# no basefile anonymous-level
```

Related Commands

(config-parammap-optmz) canonical-url
(config-parammap-optmz) delta

(config-parammap-optmz) cache key-modifier

To modify the canonical form of a URL, which is the portion before the question mark (?), to form the cache key, use the **cache key-modifier** command. This command specifies a regular expression that contains embedded variables that are expanded by the ACE. Use the **no** form of the command to remove a cache key modifier.

cache key-modifier {*string parameter_expander_function*}

no cache key-modifier {*regular_expression parameter_expander_function*}

Syntax Description

string	A regular expression. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters. Alternatively, you can enter a text string with spaces provided that you enclose the entire string in quotation marks (“). The ACE supports the use of regular expressions for matching string expressions. The “Usage Guidelines” section lists the supported characters that you can use for matching string expressions.
parameter_expander_function	A parameter expander function that evaluate to strings. The “Usage Guidelines” section lists the parameter expander functions that you can use.

Command Modes

Parameter map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The key that the ACE uses for any given requesting URL comprises one or more of the following two components:

- Query parameters—The URL portion after a question mark (?). You can modify query parameters by using the **cache parameter** command, which can be used to include selected query parameters, a cookie value, an HTTP header value, or other values.
- Canonical URL—The URL portion up to a question mark (?). You can modify the canonical URL by using the **cache key-modifier** command.

The expanded string that results from the **cache key-modifier** command replaces the default canonical URL portion of the cache key. If you do not specify the **cache key-modifier** command, the canonical URL is used as the default value for the URL portion of the cache key (there may also be a query parameter portion).

For details on modifying the cache key, see the *Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide.*

The following table lists the supported characters that you can use for matching string expressions.

Convention	Description
.	One of any character.
.*	Zero or more of any character.
\.	Period (escaped).
[*charset*]	Match any single character from the range.
[^charset]	Do not match any character in the range. All other characters represent themselves.
()	Expression grouping.
(expr1 | expr2)	OR of expressions.
(expr)*	0 or more of expression.
(expr)+	1 or more of expression.
expr{m,n}	Repeat the expression between *m* and *n* times, where *m* and *n* have a range of 1 to 255.
expr{m}	Match the expression exactly *m* times. The range for *m* is from 1 to 255.
expr{m,}	Match the expression *m* or more times. The range for *m* is from 1 to 255.
\a	Alert (ASCII 7).
\b	Backspace (ASCII 8).
\f	Form-feed (ASCII 12).
\n	New line (ascii 10).
\r	Carriage return (ASCII 13).
\t	Tab (ASCII 9).
\v	Vertical tab (ASCII 11).
\0	Null (ASCII 0).
\\	Backslash.
\x##	Any ASCII character as specified in two-digit hexadecimal notation.

The following table lists the parameter expander functions that you can use.

Variable	Description
`$(number)`	Expands to the corresponding matching subexpression (by *number*) in the URL pattern. Subexpressions are marked in a URL pattern using parentheses (). The numbering of the subexpressions begins with 1 and is the number of the left-parenthesis "(" counting from the left. You can specify any positive integer for the number. $(0) matches the entire URL. For example, if the URL pattern is ((http://server/.*)/(.*)/)a.jsp, and the URL that matched it is the following: http://server/main/sub/a.jsp?category=shoes&session=99999, then the following are correct: $(0) = http://server/main/sub/a.jsp $(1) = http://server/main/sub/ $(2) = http://server/main $(3) = sub If the specified subexpression does not exist in the URL pattern, then the variable expands to the empty string.
`$http_query_string()`	Expands to the value of the whole query string in the URL. For example, if the URL is http://myhost/dothis?param1=value1&param2=value2 then the following is correct: $http_query_string() = param1=value1&param2=value2 This function applies to both GET and POST requests.

`$http_query_param(query-param-name)`
this obsolete syntax is also supported:
`$param(query-param-name)`
	Expands to the value of the named query parameter (case sensitive). For example, if the URL is
	http://server/main/sub/a.jsp?category=shoes&session=99999
	then the following are correct:
	$http_query_param(category) = shoes
	$http_query_param(session) = 99999
	If the specified parameter does not exist in the query, then the variable expands to the empty string. This function applies to both GET and POST requests.

`$http_cookie(cookie-name)`	Evaluates to the value of the named cookie. For example, $http_cookie(cookiexyz). The cookie name is case sensitive.
`$http_header(request-header-name)`	Evaluates to the value of the specified HTTP request header. In the case of multivalued headers, it is the single representation as specified in the HTTP specification. For example, $http_header(user-agent). The HTTP header name is not case sensitive.

Variable	Description
`$http_method()`	Evaluates to the HTTP method used for the request, such as GET or POST.

Boolean Functions:
`$http_query_param_present(query-param-name)`
`$http_query_param_notpresent (query-param-name)`
`$http_cookie_present(cookie-name)`
`$http_cookie_notpresent(cookie-name)`
`$http_header_present(request-header-name)`
`$http_header_notpresent(request-header-name)`
`$http_method_present(method-name)`
`$http_method_notpresent(method-name)`
	Evaluates to a Boolean value: True or False, depending on the presence or absence of the element in the request. The elements are a specific query parameter (query-param-name), a specific cookie (cookie-name), a specific request header (request-header-name), or a specific HTTP method (method-name). All identifiers are case sensitive except for the HTTP request header name.

Examples

For example, enter:

```
host1/Admin(config-parammap-optmz)# cache key-modifier $http://www(1)
```

To remove a cache key modifier, enter:

```
host1/Admin(config-parammap-optmz)# no cache key-modifier
```

Related Commands

(config-parammap-optmz) cache parameter
(config-parammap-optmz) cache ttl

(config-parammap-optmz) cache parameter

To modify the query parameter part of a URL, which is the portion after the question mark (?), to form the cache key, use the **cache parameter** command. Use the **no** form of the command to remove a cache parameter.

cache parameter *parameter_expander_function*

no cache parameter *parameter_expander_function*

Syntax Description

parameter_expander_function	Parameter expander function that evaluates to strings. Use the forwardslash (/) character when combining multiple parameter expander functions (for example, **`cache parameter $http_cookie(ID)/$http_query_param(category)`**). The maximum string value is 255 characters. See the "(config-parammap-optmz) cache key-modifier" section for a listing of the parameter expander functions that you can use.

Command Modes

Parameter map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The key that the ACE uses for any given requesting URL comprises one or more of the following two components:

- Query parameters—The URL portion after a question mark (?). You can modify query parameters by using the **cache parameter** command, which can be used to include selected query parameters, a cookie value, an HTTP header value, or other values.
- Canonical URL—The URL portion up to a question mark (?). You can modify the canonical URL by using the **cache key-modifier** command.

The **cache parameter** command specifies an expression that includes one or more parameter expander functions if you want to modify the parameter portion of the cache key. This command specifies one or more parameter expander functions that evaluate to strings. These strings are appended to the canonical URL to form the last portion of the cache key. The parameter expander functions are listed in the (config-parammap-optmz) cache key-modifier command.

The string specified in the **cache parameter** command replaces the default query parameter that is used in the cache key. If you do not specify the **cache parameter** command, the query parameter portion of the URL is used as the default value for this portion of the cache key. The canonical URL, possibly modified by the **cache key-modifier** command, is the first part of the cache key.

For details on modifying the cache key, see the *Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide.*

Examples

To set the value of the query parameter portion of the cache key, enter:

```
host1/Admin(config-parammap-optmz)# cache parameter $http_query_param (version)
```

To remove a cache parameter, enter:

```
host1/Admin(config-parammap-optmz)# no cache parameter
```

Related Commands

(config-parammap-optmz) cache key-modifier
(config-parammap-optmz) cache ttl

(config-parammap-optmz) cache ttl

To define the ACE cache freshness settings, use the **cache ttl** command. Use the **no** form of the command to revert to a default cache time-to-live value.

cache ttl {**min** *time* | **max** *time* | **percent** *value*}

no cache ttl {**min** *time* | **max** *time* | **percent** *value*}

Syntax Description

min *time*	Minimum time in seconds that an object without an explicit expiration time should be considered fresh. The **min** keyword specifies the minimum time that the content can be cached for, which corresponds to the time-to-live value of the content. In the case of a new item that is valid for three hours, this value would be 3 x 60 x 60 = 10800 seconds. If you perform static caching (the **flashforward-object** action), this value should normally be 0. If you perform dynamic caching (the **cache dynamic** action) this value should be set to indicate how long the ACE should cache the page. Valid values are from 0 to 2147483647 seconds. The default is 0.
max *time*	Maximum time in seconds than an object without an explicit expiration time should be considered fresh. The **max** keyword determines how the ACE handles the case when the object has passed its cache minimum time-to-live value.Valid values are from 0 to 2147483647 seconds. The default is 300 seconds.
percent *value*	Percent of an object's age at which an embedded object without an explicit expiration time is considered fresh. Valid values are from 0 to 100 percent. The default is 0 percent.

Command Modes

Parameter map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command sets the maximum time (**max** keyword) or the minimum time (**min** keyword) in seconds that an object without an explicit expiration time should be considered fresh. The **percent** keyword sets the percent of an object's age at which an embedded object without an explicit expiration time is considered fresh.

Examples

To specify a minimum time-to-live value of 1000 seconds in which the content can be cached, enter:

```
host1/Admin(config-parammap-optmz)# cache ttl min 1000
```

To revert to a default cache time-to-live value, enter:

```
host1/Admin(config-parammap-optmz)# no cache ttl min
```

Related Commands

(config-parammap-optmz) cache key-modifier
(config-parammap-optmz) cache parameter
(config-parammap-optmz) cache ttl

(config-parammap-optmz) cache-policy request

To override client request headers (primarily for embedded objects), use the **cache-policy request** command. Use the **no** form of the command to remove a cache policy request selection.

cache-policy request {**override-all** | **override-cache-ctl-no-cache**}

no cache-policy request {**override-all** | **override-cache-ctl-no-cache**}

Syntax Description

override-all	Specifies that all cache request headers are ignored.
override-cache-ctl-no-cache	Overrides the Cache-Control: no cache HTTP header from a request. This keyword is used for a **flashforward-object** command action (see the **"(config-actlist-optm) flashforward-object"** section). Typically, if there is a cache control request header stating no cache, the ACE will not cache this object. The **override-cache-ctl-no-cache** keyword instructs the ACE to ignore the Cache-Control: no cache header from the request side.

Command Modes

Parameter map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE that all cache request headers are ignored, enter:

```
host1/Admin(config-parammap-optmz)# cache-policy request override-all
```

To remove a cache policy request selection, enter:

```
host1/Admin(config-parammap-optmz)# no cache-policy request override-all
```

Related Commands (config-actlist-optm) flashforward-object

(config-parammap-optmz) cache-policy response

To override origin server response headers (primarily for embedded objects), use the **cache-policy response** command. Use the **no** form of the command to remove a cache policy response selection.

cache-policy response {**override-all** | **override-cache-ctl-private**}

no cache-policy response {**override-all** | **override-cache-ctl-private**}

Syntax Description

override-all	Specifies that all cache response headers are ignored.
override-cache-ctl-private	Overrides the Cache-Control: private HTTP header from a response. This keyword is used for a **flashforward-object** command action (see the **"(config-actlist-optm) flashforward-object"** section) and is equivalent to static object caching. Typically, if there is a cache control response header stating private, these response headers will make the object not cacheable. The **override-cache-ctl-private** keyword instructs the ACE to ignore the Cache-Control: private HTTP header from a response.

Command Modes

Parameter map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE that all cache response headers are ignored, enter:

```
host1/Admin(config-parammap-optmz)# cache-policy response override-all
```

To remove a cache policy response selection, enter:

```
host1/Admin(config-parammap-optmz)# no cache-policy response override-all
```

Related Commands (config-actlist-optm) flashforward-object

(config-parammap-optmz) canonical-url

To specify a string containing a canonical URL regular expression that defines a set of URLs to which the parameter map applies, use the **canonical-url** command. Use the **no** form of the command to delete the string that contains a canonical URL regular expression.

canonical-url {*parameter-expander-function*}

no canonical-url {*parameter-expander-function*}

Syntax Description

parameter-expander-function	Parameter expander function that evaluates to strings. See the "(config-parammap-optmz) cache key-modifier" section for a listing of the parameter expander functions that you can use.

Command Modes

Parameter map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

At least one URL must be specified using the **canonical-url** command.

Use the canonical URL function in a parameter map to specify a base file selection policy. The canonical URL function specifies a regular expression that is used to match a variety of actual URLs. All matched URLs share a single base file.

The ACE uses the canonical URL feature to modify a parameterized request to eliminate the question mark (?) and the characters that follow to identify the general part of the URL. This general URL is then used to create the base file. The ACE uses this feature to map multiple parameterized URLs to a single canonical URL.

Examples

To specify a string that contains a canonical URL regular expression, enter:

```
host1/Admin(config-parammap-optmz)# canonical-url (1)/http_query_param(category)
```

To delete the string that contains a canonical URL regular expression, enter:

```
host1/Admin(config-parammap-optmz)# no canonical-url
```

Related Commands

(config-parammap-optmz) basefile anonymous-level
(config-parammap-optmz) cache key-modifier
(config-parammap-optmz) cache parameter
((config-parammap-optmz) expires-setting

(config-parammap-optmz) clientscript-default

To configure the ACE to recognize the scripting language used on delta optimized content pages, either JavaScript or Visual Basic, use the **clientscript-default** command. Use the **no** form of the command to revert to the default JavaScript scripting language.

clientscript-default {**javascript** | **vbscript**}

no clientscript-default {**javascript** | **vbscript**}

Syntax Description

javascript	Sets the default scripting language to JavaScript (default).
vbscript	Sets the default scripting language to Visual Basic.

Command Modes

Parameter map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To set the default scripting language to Visual Basic, enter:

```
host1/Admin(config-parammap-optmz)# clientscript-default vbscript
```

To revert to the default JavaScript scripting language, enter:

```
host1/Admin(config-parammap-optmz)# no clientscript-default vbscript
```

Related Commands

This command has no related commands.

(config-parammap-optmz) description

To add a description for the parameter map, use the **description** command. Use the **no** form of this command to remove the description from the parameter map.

description *text_string*

no description

Syntax Description

text_string	Description for the action list. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Parameter map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A3(2.3)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description for the parameter map, enter:

```
host1/Admin(config)# parameter-map type optimization http OPTIMIZE_PARAM_MAP
host1/Admin(config-parammap-optmz)# description OPTIMIZATION HTTP-TYPE PARAMETER MAP
```

To remove the description from the parameter map, enter:

```
host1/Admin(config-parammap-optz)# no description
```

Related Commands

show parameter-map

(config-parammap-optmz) delta

To control the delta optimization mode used by the ACE and to configure the delta optimization operating parameters on the ACE, use the **delta** command. Use the **no** form of the command to revert to the default all-user delta optimization mode.

delta {**all-user** | **cacheable-content** | **exclude** {**iframes** | **mime-type** *mime-type* | **non-ascii** | **scripts**} | **first-visit** | **page-size** {**min** *value* | **max** *value*} | **per-user**}

no delta {**all-user** | **cacheable-content** | **exclude** {**iframes** | **mime-type** *mime-type* | **non-ascii** | **scripts**} | **first-visit** | **page-size** {**min** *value* | **max** *value*} | **per-user**}

Syntax Description

all-user	Specifies the corresponding URLs are to be delta optimized using the all-user delta optimization mode. This is the default.
cacheable-content	Enables delta optimization of cacheable content. Typically, the ACE detects cacheable content and prevents its delta optimization.
exclude	Defines the cacheable objects that should not be delta optimized.
iframes	Specifies that IFrames should not be delta optimized.
mime-type *mime-type*	Specifies the Multipurpose Internet Mail Extension (MIME)-type messages that should not be delta optimized (such as image/Jpeg, text/html, application/msword, audio/mpeg).
non-ascii	Specifies that non-ASCII data should not to be delta optimized. Specify this keyword if the content has UTF8 characters. Using this keyword excludes such UTF8 characters from delta optimization but the remainder of that page can still have delta optimization.
scripts	Specifies that JavaScript should not to be delta optimized.
first-visit	Enables delta optimization on the first visit to a web page.
page-size	Sets the minimum and maximum page size, in bytes, that can be delta optimized.
min *value*	Specifies the minimum page size, in bytes, that can be delta optimized. Valid values are from 1 to 250000 bytes. The default is 1024 bytes.
max *value*	Specifies the maximum page size, in bytes, that can be delta optimized. Valid values are 1024 to 250000 bytes. The default is 250000 bytes.
per-user	Specifies the corresponding URLs are to be delta optimized using the per-user delta optimization mode.

Command Modes

Parameter map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Delta optimization mode specifies whether the web pages to be delta optimized are common to all users or personalized for individual users, which determines what kind of page deltas are generated by the ACE.

The ACE supports two delta optimization modes:

- All-user mode
- Per-user mode

In the all-user delta optimization mode, the delta is generated against a single base file that is shared by all users of the URL. The all-user delta optimization mode is usable in most cases, even in the case of dynamic personalized content if the structure of a page is common across users. The disk space overhead is minimal (the disk space requirements are determined by the number of delta optimized pages, not the number of users).

In the per-user delta optimization mode, when a specific user requests a URL, the delta for the response is generated against a base file that is created specifically for that user. The per-user delta optimization mode is useful in situations where the contents of a page (including layout elements) are different for each user. This mode delivers the highest level of delta optimization. However, a copy of the base page that is delivered to each user has to be kept in the ACE cache which increases the requirements on disk space for the ACE cache. The per-user delta optimization mode is useful for content privacy because base pages are not shared among users.

Examples

To specify that the corresponding URLs are to be delta optimized using the per-user delta optimization mode, enter:

```
host1/Admin(config-parammap-optmz)# delta per-user
```

To revert to the default all-user delta optimization mode, enter:

```
host1/Admin(config-parammap-optmz)# no delta per-user
```

To specify the MIME-type messages that should not be delta optimized, enter:

```
host1/Admin(config-parammap-optmz)# delta exclude mime-type audio/mpeg
```

To disable a delta optimization operating parameter on the ACE, enter:

```
host1/Admin(config-parammap-optmz)# no delta exclude mime-type audio/mpeg
```

Related Commands

(config-actlist-optm) delta
(config-parammap-optmz) basefile anonymous-level

((config-parammap-optmz) expires-setting

To control the period of time that objects in the client's browser remain fresh, use the **expires-setting** command. Use the **no** form of the command to remove an expiration setting.

expires-setting {**cachettl** | **time-to-live** *seconds* | **unmodified**)

no expires-setting {**cachettl** | **time-to-live** *seconds* | **unmodified**)

Syntax Description

cachettl	Sets the freshness similar to FlashForwarded objects and uses the minimum and maximum settings configured by the **cache ttl** command (if set). See the "(config-parammap-optmz) cache ttl" section.
time-to-live *seconds*	The duration that objects in the client's browser remain fresh. Valid entries are from 0 to 2147483647 seconds.
unmodified	Disables browser object freshness control (default).

Command Modes

Parameter map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The **expires-setting** command instructs the ACE to insert an Expires response header with a time value for an object. It is not necessary to configure this command when specifying the **flashforward** command in an action list because, in this case, the ACE always inserts a long time value in the Expires header for the transformed object. The **expires-setting** command is typically used when you are not using FlashForward but want to achieve the FlashForward affect by making all of the embedded objects perceived as being fresh by the browser.

Examples

To specify that the ACE use the settings configured by the **cache ttl** command, enter:

```
host1/Admin(config-parammap-optmz)# expires-setting cachettl
```

To remove an expiration setting, enter:

```
host1/Admin(config-parammap-optmz)# no expires-setting cachettl
```

Related Commands

(config-parammap-optmz) cache ttl

(config-parammap-optmz) extract meta

To configure the ACE to remove HTML Meta elements from documents to prevent them from being condensed, use the **extract meta** command. By default, the ACE includes HTML Meta elements in documents. Use the **no** form of the command to include HTML Meta elements in documents.

extract meta

no extract meta

Syntax Description

This command has no keywords or arguments.

Command Modes

Parameter map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To remove HTML Meta elements from documents, enter:

```
host1/Admin(config-parammap-optmz)# extract meta
```

To include HTML Meta elements in documents, enter:

```
host1/Admin(config-parammap-optmz)# no extract meta
```

Related Commands

This command has no related commands.

(config-parammap-optmz) flashforward refresh-policy

To configure the ACE to bypass FlashForward for stale embedded objects, use the **flashforward refresh-policy** command. Use the **no** form of the command to revert to the default of allowing FlashForward to indirectly refresh embedded objects.

flashforward refresh-policy {**all** | **direct**}

no flashforward refresh-policy {**all** | **direct**}

Syntax Description

all	Allows FlashForward to indirectly refresh embedded objects (default).
direct	Bypasses FlashForward for stale embedded objects so that they are directly refreshed.

Command Modes

Parameter map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Request headers that the ACE sends to the origin server for stale embedded objects (indirect GET) may not be accepted by the origin server and cause errors. In this case, specify **direct** to prevent this behavior.

FlashForward is disabled by default; you must enable it by specifying the following commands in action list optimization mode: **flashforward** and **flashforward-object** (for embedded objects).

Examples

To bypass FlashForward for stale embedded objects, enter:

```
host1/Admin(config-parammap-optmz)# flashforward refresh-policy direct
```

To revert to the default of allowing FlashForward to indirectly refresh embedded objects, enter:

```
host1/Admin(config-parammap-optmz)# no flashforward refresh-policy
```

Related Commands

(config-actlist-optm) flashforward
(config-actlist-optm) flashforward-object

(config-parammap-optmz) ignore-server-content

To specify a comma-separated list of HTTP response codes for which the response body must not be read (ignored), use the **ignore-server-content** command. Use the **no** form of the command to remove one or more response codes to ignore.

ignore-server-content *value*

no ignore-server-content *value*

Syntax Description

value	The response code as an unquoted text string with a maximum of 64 alphanumeric characters. For example, a response code value of 302 directs the ACE to ignore the response body in the case of a 302 (redirect) response from the origin server.

Command Modes

Parameter map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To specify a response code value of 302 to ignore, enter:

```
host1/Admin(config-parammap-optmz)# ignore-server-content 302
```

To remove one or more response codes to ignore, enter:

```
host1/Admin(config-parammap-optmz)# no ignore-server-content
```

Related Commands

This command has no related commands.

(config-parammap-optmz) parameter-summary parameter-value-limit

To set the maximum number of bytes that are logged for each parameter value in the parameter summary of a transaction log entry in the statistics log, use the **parameter-summary parameter-value-limit** command. Use the **no** form of the command to revert to the default of 100 bytes as the parameter summary value.

parameter-summary parameter-value-limit *bytes*

no parameter-summary parameter-value-limit *bytes*

Syntax Description

bytes	Maximum number of bytes that are logged for each parameter value in the parameter summary of a transaction log entry in the statistical log. If a parameter value is longer than this limit, it is truncated at the specified parameter limit. Valid values are from 0 to 10,000 bytes. The default is 100 bytes.

Command Modes

Parameter map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To specify 5000 bytes as the value of the parameter summary, enter:

```
host1/Admin(config-parammap-optmz)# parameter-summary parameter-value-limit 5000
```

To revert to the default of 100 bytes as the value of the parameter summary, enter:

```
host1/Admin(config-parammap-optmz)# no parameter-summary parameter-value-limit
```

Related Commands

(config) logging host
(config-actlist-optm) appscope
(config-parammap-optmz) appscope optimize-rate-percent
(config-parammap-optmz) request-grouping-string

(config-parammap-optmz) post-content-buffer-limit

To set the buffer size of an HTTP POST to a maximum number of kilobytes, use the **post-content-buffer-limit** command. Use the **no** form of the command to revert to the default buffer size of 40K.

post-content-buffer-limit *value*

no post-content-buffer-limit *value*

Syntax Description

value	The buffer size for POST data for the purpose of logging transaction parameters in the statistics log. Valid values are 0 to 1000 KB. The default is 40 KB. Parameters beyond this limit will not be logged by the ACE.

Command Modes

Parameter map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

An HTTP POST can send a very large (effectively unlimited) amount of data; in an extreme case, the client can keep sending a stream of data for the server to handle. In order to parse and inspect the POST data, the ACE needs to load the data into a buffer in memory.

Two types of standard HTTP form POST operations are as follows (they are distinguished by the value in the Content-Type header):

- application/x-www-form-urlencoded—This type represents the majority of all HTTP POSTs. This type is just a standard POST of a webpage form.
- multipart/form-data—This type is much less common. It allows browser users to upload files to a website or application. For example, if you use a web-based email program, and you want to attach a file to an e-mail that you are sending, the upload of the file is done using this type. Another usage (even less common) of this type of HTTP POST is to send binary data (for example, from a custom browser plug-in, or from a non-browser HTTP client).

Examples To specify a buffer size of 1000 KB, enter:

```
host1/Admin(config-parammap-optmz)# post-content-buffer-limit 1000
```

To revert to the default buffer size of 40 KB, enter:

```
host1/Admin(config-parammap-optmz)# no post-content-buffer-limit
```

Related Commands This command has no related commands.

(config-parammap-optmz) rebase

To control the rebasing of base files by the ACE, use the **rebase** command. Use the **no** form of the command to revert to a default rebase setting.

rebase {**delta-percent** *value* | **flashforward-percent** *value* | **history-size** *value* | **modification-cooloff-period** *value* | **reset-period** *value*}

no rebase {**delta-percent** *value* | **flashforward-percent** *value* | **history-size** *value* | **modification-cooloff-period** *value* | **reset-period** *value*}

Syntax Description

delta-percent *value*	Specifies the delta threshold at which rebasing is triggered. This number represents the size of a page delta relative to the page total size, expressed as a percentage. Valid values are from 0 to 10000 percent. The default threshold is 50 percent.
flashforward-percent *value*	Specifies a rebase, based on the percent of FlashForwarded URLs in the response. Rebasing is triggered when the difference between the percentages of FlashForwarded URLs in the delta response and the base file exceed the threshold. Valid values are from 0 to 10000 percent. The default is 50 percent. The **flashforward-percent** keyword provides a threshold control for rebasing based on the percent of FlashForwarded URLs in the response. Where the **delta-percent** keyword triggers rebasing when the delta response size exceeds the threshold as a percentage of base file size; the **flashforward-percent** keyword triggers rebasing when the difference between the percentages of FlashForwarded URLs in the delta response and the base file exceed the threshold.
history-size *value*	Controls how much history is stored before resetting. Once the sample collection reaches the specified history size, the ACE resets all rebase control parameters to zero and starts over. Using the **history-size** keyword prevents the base file from becoming too rigid. That is, if a base file has served approximately one million pages, then it would take another half million unfavorable responses before the base file can be rebased. Valid values are from 10 to 2147483647 pages. The default value for this parameter is 1000 pages.

modification-cooloff-period *value*	Specifies the time, in seconds, after the last modification before performing a rebase. Valid values are from 1 to 14400 seconds (4 hours).The default is 14400 seconds.
reset-period *value*	Specifies the period for performing a meta data refresh Valid values are from 1 to 900 seconds (15 minutes). The default is 900 seconds.

Command Modes

Parameter map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Rebasing refers to the process of updating the base file that is used for generating deltas between subsequent content retrievals. Because the base content of a site often changes over a period of time, the size of the generated deltas can grow relatively large. To maintain the effectiveness of the delta optimization process, the base files are automatically updated as required.

Examples

To specify a rebase, based on a percentage of 1000 FlashForwarded URLs in the response, enter:

```
host1/Admin(config-parammap-optmz)# rebase flashforward-percent 1000
```

To revert to a default rebase setting, enter:

```
host1/Admin(config-parammap-optmz)# no rebase flashforward-percent
```

Related Commands

This command has no related commands.

(config-parammap-optmz) request-grouping-string

To define a string to sort requests for AppScope reporting by the optional Cisco AVS 3180A Management Station, use the **request-grouping-string** command. Use the **no** form of the command to re move a request grouping string.

request-grouping-string *string*

no request-grouping-string *string*

Syntax Description

string	URL regular expression that defines a set of URLs. The string can contain the parameter expander functions listed in the **(config-parammap-optmz) cache key-modifier** section.

Command Modes

Parameter map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The string can contain a URL regular expression that defines a set of URLs in which URLs that differ only by their query parameters are to be treated as separate URLs in AppScope reports.

Typically, in an AppScope report organized by URL, matching URLs that differ only in their query parameters are treated as the same URL and are not listed on separate lines. Use the **request-grouping-string** command to specify that all URL variations that are based on query parameters are to be treated as separate URLs for reporting purposes. Each variation will appear on a separate line in the report.

For details about the Cisco AVS 3180A Management Station database, management, and reporting features for the ACE optimization functionality, including AppScope reporting, see the *Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide*.

Examples

To define a string that is used to make the URLs http://server/catalog.asp?region=asia and http://server/catalog.asp?region=america into two separate reporting categories, enter:

```
host1/Admin(config-parammap-optmz)# request-grouping-string http_query_param(region)
```

To remove a request grouping string, enter:

```
host1/Admin(config-parammap-optmz)# no request-grouping-string
```

Related Commands

(config-parammap-optmz) appscope optimize-rate-percent
(config-actlist-optm) appscope

(config-parammap-optmz) server-header

To define a user-specified string to be sent in the server header for an HTTP response, use the **server-header** command in parameter map optimization configuration mode. Use the **no** form of the command to delete the server header string.

server-header *string*

no server-header *srting*

Syntax Description

string	A particular string to be included in the server header. Enter a quoted text string. A maximum of 64 alphanumeric characters are allowed.

Command Modes

Parameter map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command provide you with a method to uniquely tag the context or URL match statement by setting server header value to a particular string. The server header string can be used in cases where a particular URL is not being transmitted to the correct target context or the match statement.

Examples

To specify a string to be sent in the server header, enter:

```
host1/Admin(config-parammap-optmz)# server-header "Header from Admin Context"
```

To delete the server header string, enter:

```
host1/Admin(config-parammap-optmz)# no server-header
```

Related Commands

This command has no related commands.

(config-parammap-optmz) server-load

To control load-based expiration for the cache, use the **server-load** command. Use the **no** form of the command to revert to a default setting of 20 percent.

server-load {**trigger-percent** *value* | **ttl-change-percent** *value*}

no server-load {**trigger-percent** *value* | **ttl-change-percent** *value*}

Syntax Description

trigger-percent *value*	Defines the threshold that triggers a change in the cache TTL. This keyword enables the ACE to monitor server load in real time and make intelligent "closed loop" content expiration decisions so that site performance is maximized and existing hardware resources are used most efficiently, even during periods of peak traffic load. Valid values are from 0 to 100 percent. The default is 20 percent.
ttl-change-percent *value*	Defines the percentage by which the cache TTL is increased or decreased in response to a change in the server load. For example, if you set this value to 20 and the current TTL for a particular response is 300 seconds, and if the current server response time exceeds the trigger threshold, then the cache TTL for the response is raised to 360 seconds (20 percent increase). Valid values are from 0 to 100 percent. The default is 20 percent.

Command Modes

Parameter map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Performance assurance with load-based expiration allows an object in the cache to expire (excluding the natural process of cache pruning). The origin server's load determines when the object expires.

This type of expiration allows you to dynamically increase the time to live (TTL) of cached responses if the current response time (average computed over a short time window) from the origin servers is larger than the average response time (average computed over a longer time window) by a threshold amount. Similarly, the TTL is dynamically decreased if the reverse holds true. The starting value for the cache TTL is the **cache ttl min** value (see the "(config-parammap-optmz) cache ttl" section) or 0 if you do not specify a value. Moving average-based calculation allows the cache to respond to trends in usage patterns, smoothing out uncharacteristic spikes.

Examples

To specify a threshold trigger of 50 percent, enter:

```
host1/Admin(config-parammap-optmz)# server-load trigger-percent 50
```

To revert to a default setting of 20 percent, enter:

```
host1/Admin(config-parammap-optmz)# no server-load trigger-percent
```

Related Commands

(config-parammap-optmz) cache ttl

(config-parammap-optmz) utf8 threshold

To determine how many UTF-8 characters on a page constitute a UTF-8 character set page for purposes of UTF-8 detection, use the **utf8 threshold** command. Use the **no** form of the command to disable the UTF-8 threshold.

utf8 threshold *value*

no utf8 threshold *value*

Syntax Description

value	Number of UTF-8 characters on a page that constitute a UTF-8 character set page. Valid values are from 1 to 1,000,000 characters. The default is 5 characters.

Command Modes

Parameter map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This threshold adjusts the detection of multibyte UTF-8 character set pages.

Examples

To specify a value of 1000 UTF-8 characters on a page, enter:

```
host1/Admin(config-parammap-optmz)# utf8 threshold 1000
```

To disable the UTF-8 threshold, enter:

```
host1/Admin(config-parammap-optmz)# no utf8 threshold
```

Related Commands

This command has no usage guidelines.

Parameter Map RTSP Configuration Mode Commands

Parameter map RTSP configuration mode commands allow you to specify a Real-Time Streaming Protocol (RTSP-type) parameter map and define its settings. To create an RTSP-type parameter map and access parameter map RTSP configuration mode, use the **parameter-map type rtsp** command. The prompt changes to (config-parammap-rtsp). Use the **no** form of this command to remove an RTSP-type parameter map from the configuration.

parameter-map type rtsp *name*

no parameter-map type rtsp *name*

Syntax Description

name	Name assigned to the parameter map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The commands in this mode require the connection feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

After you create and configure a parameter map, you must associate the parameter map with a policy map to activate it. For details, see the **(config-pmap-c) appl-parameter rtsp advanced-options** command in the "Policy Map Configuration Mode Commands" section.

Examples

To create an RTSP-type parameter map called RTSP_MAP, enter:

```
host1/Admin(config)# parameter-map type rtsp RTSP_MAP
host1/Admin(config-parammap-rtsp)#
```

Related Commands

(config) parameter-map type
(config-pmap-c) appl-parameter rtsp advanced-options
show parameter-map

(config-parammap-rtsp) case-insensitive

ACETo disable case-sensitivity matching for RTSP, use the **case-insensitive** command. Use the **no** form of this command to reset the ACE to its default of case-sensitive RTSP matching.

case-insensitive

no case-insensitive

Syntax Description

This command has no keywords or arguments.

Command Modes

Parameter map RTSP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

By default, the ACE CLI is case sensitive. With case-insensitive matching enabled, uppercase and lowercase letters are considered the same.

When case sensitivity is disabled, it applies to the following:

- RTSP header names and values
- RTSP URL strings
- RTSP inspection (for details, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*)

Examples

To enable case-insensitive matching, enter:

```
host1/Admin(config-parammap-rtsp)# case-insensitive
```

To reenable case-sensitive matching, enter:

```
host1/Admin(config-parammap-rtsp)# no case-insensitive
```

Related Commands

show parameter-map

(config-parammap-rtsp) description

To add a description for the parameter map, use the **description** command. Use the **no** form of this command to remove the description from the parameter map.

description *text_string*

no description

Syntax Description

text_string	Description for the action list. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Parameter map RTSP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(2.3)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description for the parameter map, enter:

```
host1/Admin(config)# parameter-map type rtsp RTSP_MAP
host1/Admin(config-parammap-rtsp)# description RTSP-TYPE PARAMETER MAP
```

To remove the description from the parameter map, enter:

```
host1/Admin(config-parammap-rtsp)# no description
```

Related Commands

show parameter-map

(config-parammap-rtsp) set header-maxparse-length

To set the maximum number of bytes to parse for RTSP headers, use the **set header-maxparse-length** command. Use the **no** form of this command to reset the RTSP header maximum parse length to the default of 2048 bytes.

set header-maxparse-length *bytes*

no set-header maxparse-length

Syntax Description

bytes	Maximum number of bytes to parse for the total length of all RTSP headers. Enter an integer from 1 to 65535. The default is 2048 bytes.

Command Modes

Parameter map RTSP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To set the RTSP header maximum parse length to 16,384 bytes, enter:

```
host1/Admin(config-parammap-rtsp)# set header-maxparse-length 16384
```

To reset the RTSP header maximum parse length to the default of 2048 bytes, enter:

```
host1/Admin(config-parammap-rtsp)# no set header-maxparse-length 8192
```

Related Commands

show parameter-map

Parameter Map SCCP Configuration Mode Commands

Parameter map Skinny Client Control Protocol (SCCP) configuration mode commands allow you to specify an SCCP-type parameter map and configure SCCP packet inspection on the ACE. To configure SCCP packet inspection, use the **parameter-map type skinny** command in configuration mode. The prompt changes to (config-parammap-skinny). Use the **no** form of this command to remove the parameter map from the configuration.

parameter-map type skinny *name*

no parameter-map type skinny *name*

Syntax Description

name	Name assigned to the parameter map. Enter an unquoted text string with no spaces and a maximum of 32 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

Note the following considerations when you configure SCCP inspection on the ACE:

- If the IP address of an internal Cisco CallManager (CCM) is configured for Network Address Translation (NAT) or Port Address Translation (PAT) to a different IP address or port, registrations for external IP phones fail because the ACE does not support NAT or PAT of the file content transferred over TFTP. Although the ACE supports NAT of TFTP messages and opens a secure port for the TFTP file, the ACE cannot translate the CCM IP address and port that are embedded in the IP phone configuration files. The configuration files are transferred using TFTP during phone registration.
- If a Skinny phone is in a low security zone and the TFTP server is in a high security zone, the ACE cannot translate the TFTP server IP address. In this case, the ACE opens the TFTP port (69) for Skinny phones.

Examples

To create an SCCP-type parameter map called SCCP_PARAMMAP, enter:

```
host1/Admin(config)# parameter-map type skinny SCCP_PARAMMAP
host1/Admin(config-parammap-skinny)#
```

To remove the parameter map from the configuration, enter:

```
host1/Admin(config)# no parameter-map type skinny SCCP_PARAMMAP
```

Related Commands

(config) parameter-map type
(config-pmap-c) appl-parameter skinny advanced-options
show parameter-map

(config-parammap-skinny) description

To add a description for the parameter map, use the **description** command. Use the **no** form of this command to remove the description from the parameter map.

description *text_string*

no description

Syntax Description

text_string	Description for the action list. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Parameter map SCCP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(2.3)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description for the parameter map, enter:

```
host1/Admin(config)# parameter-map type skinny SCCP_PARAMMAP
host1/Admin(config-parammap-skinny)# description SCCP-TYPE PARAMETER MAP
```

To remove the description from the parameter map, enter:

```
host1/Admin(config-parammap-skinny)# no description
```

Related Commands

show parameter-map

(config-parammap-skinny) enforce-registration

To enable registration enforcement, use the **enforce-registration** command. Use the **no** form of this command to disable registration enforcement.

enforce-registration

no enforce-registration

Syntax Description

This command has no keywords or arguments.

Command Modes

Parameter map SCCP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

You can configure the ACE to allow only registered Skinny clients to make calls. To accomplish this task, the ACE maintains the state of each Skinny client. After a client registers with CCM, the ACE opens a secure port (pinhole) to allow that client to make a call. By default, this feature is disabled.

Examples

To enable registration enforcement for Skinny clients, enter:

```
host1/Admin(config-parammap-skinny)# enforce-registration
```

To disable registration enforcement, enter:

```
host1/Admin(config-parammap-skinny)# no enforce-registration
```

Related Commands

(config-pmap-c) appl-parameter skinny advanced-options
(config-parammap-skinny) message-id max
(config-parammap-skinny) sccp-prefix-len

(config-parammap-skinny) message-id max

To set the maximum SCCP StationMessageID that the ACE allows, use the **message-id max** command. Use the **no** form of this command to reset the maximum message ID to the default of 0x181.

message-id max *number*

no message-id max *number*

Syntax Description

number	Largest value for the station message ID in hexadecimal that the ACE accepts. Enter a hexadecimal value from 0 to 4000. If a packet arrives with a station message ID greater than the maximum configured value or greater than the default value, the ACE drops the packet and generates a syslog message.

Command Modes

Parameter map SCCP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To set the maximum SCCP message ID to 0x3000, enter:

```
host1/Admin(config-parammap-skinny)# message-id max 3000
```

To reset the maximum message ID to the default of 0x181, enter

```
host1/Admin(config-parammap-skinny)# no message-id max 3000
```

Related Commands

(config-pmap-c) appl-parameter skinny advanced-options
(config-parammap-skinny) enforce-registration
(config-parammap-skinny) sccp-prefix-len

(config-parammap-skinny) sccp-prefix-len

To set the minimum and maximum SCCP prefix length, use the **sccp-prefix-len** command. Use the **no** form of this command to reset the minimum prefix length to the default behavior.

sccp-prefix len {**max** *number* | **min** *number*}

no sccp-prefix len {**max** *number* | **min** *number*}

Syntax Description

max *number*	Enables the check of the maximum SCCP prefix length. Enter an integer from 4 to 4000 bytes. The default is 4 bytes.
min *number*	Specifies the minimum SCCP prefix length. Enter an integer from 4 to 4000 bytes.

Command Modes

Parameter map SCCP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

By default, the ACE drops SCCP messages that have an SCCP Prefix length that is less than the message ID. You can configure the ACE to check for a specific minimum prefix length. You can also configure the ACE to check for a maximum prefix length, but this check is disabled by default. The ACE drops any Skinny message packets that fails these checks and generates a syslog message.

Examples

To set the minimum SCCP prefix length, enter:

```
host1/Admin(config-parammap-skinny)# sccp-prefix-len min 4
```

To reset the minimum SCCP prefix length to the default behavior, enter:

```
host1/Admin(config-parammap-skinny)# no sccp-prefix-len min 4
```

Related Commands

(config-pmap-c) appl-parameter skinny advanced-options
(config-parammap-skinny) enforce-registration
(config-parammap-skinny) message-id max

Parameter Map SIP Configuration Mode Commands

Parameter map Session Initiation Protocol (SIP) configuration mode commands allow you to specify an SIP-type parameter map and configure a SIP deep packet inspection policy map. To configure SIP deep packet inspection, use the **parameter-map type sip** command in configuration mode. The prompt changes to (config-parammap-sip). Use the **no** form of this command to remove the parameter map from the configuration.

parameter-map type sip *name*

no parameter-map type sip *name*

Syntax Description

name	Name assigned to the parameter map. Enter an unquoted text string with no spaces and a maximum of 32 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

Note the following considerations when you configure SIP inspection on the ACE:

- If the IP address in the owner field (o=) is different from the IP address in the connection field (c=) of the Session Description Protocol (SDP) portion of a SIP packet, the ACE may not translate the IP address properly. This improper IP address translation is caused by a limitation of the SIP protocol, which does not provide a port value in the owner field (o=).
- If a remote endpoint attempts to register with a SIP proxy server on a network protected by the ACE, the registration fails under the following conditions:
  - PAT is configured on the remote endpoint
  - The SIP registration server is on the outside network

The port value is missing in the contact field of the REGISTER message that the endpoint sends to the proxy server.

Examples

To create an SIP-type parameter map called SIP_PARAMMAP, enter:

```
host1/Admin(config)# parameter-map type sip SIP_PARAMMAP
host1/Admin(config-parammap-sip)#
```

To remove the parameter map from the configuration, enter:

```
host1/Admin(config)# no parameter-map type sip SIP_PARAMMAP
```

Related Commands

(config) parameter-map type
(config-pmap-c) appl-parameter sip advanced-options
show parameter-map

(config-parammap-sip) description

To add a description for the parameter map, use the **description** command. Use the **no** form of this command to remove the description from the parameter map.

description *text_string*

no description

Syntax Description

text_string	Description for the action list. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Parameter map SIP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(2.3)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description for the parameter map, enter:

```
host1/Admin(config)# parameter-map type sip SIP_PARAMMAP
host1/Admin(config-parammap-sip)# description SIP-TYPE PARAMETER MAP
```

To remove the description from the parameter map, enter:

```
host1/Admin(config-parammap-sip)# no description
```

Related Commands

show parameter-map

(config-parammap-sip) im

To enable instant messaging (IM) over SIP, use the **im** command. Use the **no** form of this command to disable instant messaging.

im

no im

Syntax Description

This command has no keywords or arguments.

Command Modes

Parameter map SIP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

Disabling IM results in the ACE dropping all messages belonging to the IM.

Examples

To enable instant messaging over SIP, enter:

```
host1/Admin(config-parammap-sip)# im
```

To disable instant messaging, enter:

```
host1/Admin(config-parammap-sip)# no im
```

Related Commands

(config-parammap-sip) max-forward-validation
(config-parammap-sip) software-version
(config-parammap-sip) strict-header-validation
(config-parammap-sip) uri-non-sip

(config-parammap-sip) max-forward-validation

To instruct the ACE to validate the value of the Max-Forwards header field, use the ACE **max-forward-validation** command. Use the **no** form of this command to disable maximum forward field validation.

max-forward-validation {**log**} | {{**drop**| **reset**} [**log**]}

no max-forward-validation {**log**} | {{**drop**| **reset**} [**log**]}

Syntax Description

log	Specifies that the ACE log a max forward validation event.
drop	Specifies that the ACE drop the SIP message.
reset	Specifies that the ACE reset the SIP connection.

Command Modes

Parameter map SIP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The Max-Forwards header field limits the number of hops that a SIP request can take on the way to its destination. This header field contains an integer that is decremented by one at each hop. If the Max-Forwards value reaches zero before the request reaches its destination, the request is rejected with a 483 Too Many Hops error response. You can instruct the ACE to validate the Max-Forwards header field value and to take appropriate action if the validation fails.

Examples

To enable Max-Forwards header field validation, enter:

```
host1/Admin(config-parammap-sip)# max-forward-validation drop log
```

To disable maximum forward field validation, enter:

```
host1/Admin(config-parammap-sip)# no max-forward-validation
```

Related Commands

(config-parammap-sip) im
(config-parammap-sip) software-version
(config-parammap-sip) strict-header-validation
(config-parammap-sip) uri-non-sip

(config-parammap-sip) software-version

To enable user agent (UA) software version options, use the **software-version** command. Use the **no** form of this command to reset the software version to the default behavior.

software-version {log} | {mask [log]}

no software-version {log} | {mask [log]}

Syntax Description

log	Specifies that the ACE log the UA software version.
mask	Specifies that the ACE mask the UA software version.

Command Modes

Parameter map SIP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

If the software version of a user agent (UA) were exposed, the UA may be more vulnerable to attacks from hackers who exploit the security holes present in that particular version of software. To protect the UA from such attacks, the ACE allows you to log or mask the UA software version.

Examples

To configure the ACE to mask the UA software version, enter:

```
host1/Admin(config-parammap-sip)# software-version mask
```

To return the ACE behavior to the default of not masking the UA software version, enter:

```
host1/Admin(config-parammap-sip)# no software-version mask
```

Related Commands

(config-parammap-sip) im
(config-parammap-sip) max-forward-validation
(config-parammap-sip) strict-header-validation
(config-parammap-sip) uri-non-sip

(config-parammap-sip) strict-header-validation

To enable strict header validation and the action that you want the ACE to perform if a SIP header does not meet the validation requirements, use the **strict-header-validation** command. Use the **no** form of this command to disable strict header validation.

strict-header-validation {**log**} | {{**drop** | **reset**} [**log**]}

no strict-header-validation {**log**} | {{**drop**| **reset**} [**log**]}

Syntax Description

drop	Specifies that the ACE drop the SIP message.
reset	Specifies that the ACE reset the connection.
log	Specifies that the ACE log the header validation event.

Command Modes

Parameter map SIP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

You can ensure the validity of SIP packet headers by configuring the ACE to check for the presence of the following mandatory SIP header fields:

- From
- To
- Call-ID
- CSeq
- Via
- Max-Forwards

If one of these header fields is missing in a SIP packet, the ACE considers that packet invalid. The ACE also checks for forbidden header fields, according to RFC 3261.

Use care if you plan to enable the **drop** option to ensure the validity of SIP packet headers. The **drop** option results in dropping requests which do not include the mandatory headers of that request. In some cases, the use of the **drop** option can lead to problems with some phones which do not utilize the mandatory headers in the request. For example, when a call is made and then cancelled, the phone receives a 487 Request Terminated cancel status request and transmits an ACK. However, for the Cisco IP Phone 7960, the transmitted ACK does not contain the MAX-FORWARDS header, which is a mandatory header for ACK. The ACE will then drop this packet, which can result in operational issues with the phone.

Examples

To enable strict header validation, instruct the ACE to drop the connection if the packet header does not meet the header validation requirements, and log the event, enter:

```
host1/Admin(config-parammap-sip)# strict-header-validation drop log
```

To disable strict header validation, enter:

```
host1/Admin(config-parammap-sip)# no strict-header-validation drop log
```

Related Commands

(config-parammap-sip) im
(config-parammap-sip) max-forward-validation
(config-parammap-sip) software-version
(config-parammap-sip) uri-non-sip

(config-parammap-sip) timeout

To prevent a hacker from exploiting this port, set a timeout for SIP media by using the **timeout** command in parameter map SIP configuration mode. Use the **no** form of this command to return the streaming media port timeout value to the default of 5 seconds.

timeout sip-media *number*

no timeout sip-media *number*

Syntax Description

number	The timeout in seconds for the media port. Enter an integer from 1 to 65535 seconds. The default is 5 seconds. Be sure to provide a timeout value that is large enough for streaming media applications to complete.

Command Modes

Parameter map SIP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To specify a secure streaming media port timeout value of 1 hour, enter:

```
host1/Admin(config)# parameter-map type sip SIP_PARAMMAP
host1/Admin(config-parammap-sip)# timeout sip-media 3600
```

To return the streaming media port timeout value to the default of 5 seconds, enter:

```
host1/Admin(config-parammap-sip)# no timeout sip-media 3600
```

Related Commands

(config-parammap-sip) im
(config-parammap-sip) max-forward-validation
(config-parammap-sip) software-version
(config-parammap-sip) uri-non-sip

(config-parammap-sip) uri-non-sip

To enable the detection of non-SIP URIs in SIP messages, use the **uri-non-sip** command. Use the **no** form of this command to disable the detection of non-SIP URIs.

uri-non-sip {**log**} | {**mask** [**log**]}

no uri-non-sip {**log**} | {**mask** [**log**]}

Syntax Description

log	Specifies the ACE log the non-SIP URI.
mask	Specifies that the ACE mask the non-SIP URI.

Command Modes

Parameter map SIP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To enable the detection of non-SIP URIs in SIP messages and log the event, enter:

```
host1/Admin(config-parammap-sip)# uri-non-sip log
```

To disable the detection of non-SIP URIs in SIP messages, enter:

```
host1/Admin(config-parammap-sip)# no uri-non-sip log
```

Related Commands

(config-parammap-sip) im
(config-parammap-sip) max-forward-validation
(config-parammap-sip) software-version
(config-parammap-sip) strict-header-validation

Parameter Map SSL Configuration Mode Commands

Parameter map Secure Sockets Layer (SSL) configuration mode commands allow you to specify an SSL-type parameter map and configure SSL settings for the map. To create an SSL-type parameter map and access parameter map SSL configuration mode, use the **parameter-map type ssl** command in configuration mode. The prompt changes to (config-parammap-ssl). Use the **no** form of this command to remove the parameter map from the configuration.

parameter-map type ssl *name*

no parameter-map type ssl *name*

Syntax Description

name	Name assigned to the parameter map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the connection or SSL feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

After you create and configure an SSL parameter map, you must associate the parameter map with a policy map to activate it. For details, see the **(config-ssl-proxy) ssl advanced-options** command in the "SSL Proxy Configuration Mode Commands" section.

Examples

To create an SSL-type parameter map called SSL_MAP, enter:

```
host1/Admin(config)# parameter-map type ssl SSL_MAP
host1/Admin(config-parammap-ssl)#
```

Related Commands

(config) parameter-map type
(config-ssl-proxy) ssl advanced-options
show parameter-map

(config-parammap-ssl) authentication-failure ignore

To enable the ACE to ignore expired or invalid server certificates and to continue setting up the back-end connection in an SSL initiation configuration, use the **authentication-failure ignore** command. Use the **no** form of this command to return to the default setting of disabled.

authentication-failure ignore

no authentication-failure ignore

Syntax Description

This command has no keywords or arguments.

Command Modes

SSL parameter map configuration mode

Command HistoryA

Release	Modification
A1(8)	This command was introduced.

Usage Guidelines

This command allows the ACE to ignore the following nonfatal errors that are related to server certificates:

- Certificate not yet valid
- Certificate has expired
- Unable to get issuer certificate
- Certificate revoked

Examples

For example, to ignore expired or invalid server certificates, enter:

```
host1/Admin(config)# parameter-map type ssl SSL_PARAMMAP_SSL
host1/Admin(config-parammap-ssl)# authentication-failure ignore
```

To return to the default setting of disabled, use the no form of the command:

```
host1/Admin(config-parammap-ssl)# no authentication-failure ignore
```

Related Commands

This command has no related commands.

(config-parammap-ssl) cipher

To define each of the cipher suites that you want the ACE to support during a secure session, use the **cipher** command. Use the **no** form of this command to delete a cipher suite from the SSL parameter map.

cipher *cipher_name* [**priority** *cipher_priority*]

no cipher *cipher_name*

Syntax Description

cipher_name	Name of the cipher suite. See the "Usage Guidelines" section for the TCP options available for the available cipher suites that the ACE supports. Enter one of the supported cipher suites from Table 2-14. The default setting is **all**.
priority	(Optional) Assigns a priority level to the cipher suite. The priority level represents the preference-for-use ranking of the cipher suite, with 10 being the most preferred and 1 being the least preferred. By default, all configured cipher suites have a priority level of 1.
cipher_priority	Priority level of the cipher suite. Enter a value from 1 to 10. The default priority value is 1.

Command Modes

SSL parameter map configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Table 2-14 lists the available cipher suites that the ACE supports and indicates which of the supported cipher suites are exportable from the ACE. Table 2-14 also lists the authentication certificate and encryption key required by each cipher suite.

Table 2-14 Supported Cipher Suites

Cipher Suite	Exportable	Authentication Certificate Used	Key Exchange Algorithm Used
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
RSA_EXPORT_WITH_RC4_40_MD5	Yes	RSA certificate	RSA key exchange
RSA_EXPORT_WITH_DES40_CBC_SHA	Yes	RSA certificate	RSA key exchange
RSA_EXPORT1024_WITH_RC4_56_MD5	Yes	RSA certificate	RSA key exchange
RSA_EXPORT1024_WITH_DES_CBC_SHA	Yes	RSA certificate	RSA key exchange

Table 2-14 Supported Cipher Suites (continued)

Cipher Suite	Exportable	Authentication Certificate Used	Key Exchange Algorithm Used
RSA_EXPORT1024_WITH_RC4_56_SHA	Yes	RSA certificate	RSA key exchange
RSA_WITH_AES_128_CBC_SHA	No	RSA certificate	RSA key exchange
RSA_WITH_AES_256_CBC_SHA	No	RSA certificate	RSA key exchange

Repeat the **cipher** command for each cipher suite that you want to include in the SSL parameter map.

The ACE chooses a cipher suite with the highest priority level from the client list. For SSL termination applications, the ACE uses the priority level to match cipher suites in the client's ClientHello handshake message. For SSL initiation applications, the priority level represents the order in which the ACE places the cipher suites in its ClientHello handshake message to the server.

The default "all cipher suites" setting works only when you do not configure the SSL parameter map with any specific ciphers. To return to using the "all cipher suites" setting, you must delete each of the specifically defined ciphers from the parameter map using the **no** form of the command.

Examples

To add the cipher suite RSA_WITH _AES_128_CBC_SHA and assign it a priority 2 level, enter:

```
host1/Admin(config-parammap-ssl)# cipher RSA_WITH_AES_128_CBC_SHA priority 2
```

To delete the cipher suite RSA_WITH _AES_128_CBC_SHA from the SSL parameter map, enter:

```
host1/Admin(config-parammap-ssl)# no cipher RSA_WITH_AES_128_CBC_SHA
```

Related Commands

(config-parammap-ssl) queue-delay timeout
(config-parammap-ssl) session-cache timeout
(config-parammap-ssl) version
show parameter-map

(config-parammap-ssl) close-protocol

To configure how the ACE handles the sending of close-notify messages, use the **close-protocol** command. By default, the ACE sends a close-notify alert message to its peer when closing a session but has no expectation of receiving one back from the peer. Use the **no** form of this command to reset the the default behavior.

close-protocol {**disabled** | **none**}

no close-protocol

Syntax Description

disabled	Configures the ACE not to send a close-notify alert message to its peer when closing a session with no expectation of receiving one back from the peer.
none	Configures the ACE to send a close-notify alert message to its peer when closing a session, but the ACE has no expectation of receiving one back from the peer.

Command Modes

SSL parameter map configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To set **close-protocol** to disabled, enter:

```
host1/Admin(config)# parameter-map type ssl SSL_PARAMMAP_SSL
host1/Admin(config-parammap-ssl)# close-protocol disabled
```

To configure the **close-protocol** command with the default setting of none, enter:

```
host1/Admin(config-parammap-ssl)# no close-protocol
```

Related Commands

show parameter-map

(config-parammap-ssl) description

To add a description for the parameter map, use the **description** command. Use the **no** form of this command to remove the description from the parameter map.

description *text_string*

no description

Syntax Description

text_string	Description for the action list. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Parameter map SSL configuration mode

Admin and user contexts

Command History

Release	Modification
A3(2.3)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description for the parameter map, enter:

```
host1/Admin(config)# parameter-map type ssl SSL_PARAMMAP
host1/Admin(config-parammap-ssl)# description SSL-TYPE PARAMETER MAP
```

To remove the description from the parameter map, enter:

```
host1/Admin(config-parammap-ssl)# no description
```

Related Commands

show parameter-map

(config-parammap-ssl) expired-crl reject

To configure the ACE to reject a client certificate when the CRL in use has expired, use the **expired-crl reject** command. Use the **no** form of this command to reset the default behavior of the ACE accepting a client certificate after the CRL in use has expired.

expired-crl reject

no expired-crl reject

Syntax Description

This command has no keywords or arguments.

Command Modes

SSL parameter map configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

When you configure certificate revocation lists (CRLs) on the ACE for client authentication by using the **crl** command in SSL proxy configuration mode, the CRLs contain an update field that specifies the date when a new version would be available. By default, the ACE does not continue to use CRLs that contain an update field with an expired date and, thus, does not reject incoming certificates using the CRL.

Examples

To configure the ACE to reject a client certificate when the CRL in use has expired, enter:

```
host1/Admin(config-parammap-ssl)# expired-crl reject
```

To reset the default behavior of the ACE accepting a client certificate after the CRL in use has expired, enter:

```
host1/Admin(config-parammap-ssl)# no expired-crl reject
```

Related Commands

show parameter-map
(config-ssl-proxy) crl

(config-parammap-ssl) queue-delay timeout

To set the delay time, use the **queue-delay timeout** command. The queue delay time is the amount of time that the ACE waits before emptying the queued data for encryption. Use the **no** form of this command to disable the queue delay time to its default value of 0. By default, the queue delay timer is disabled.

queue-delay timeout *milliseconds*

no queue-delay

Syntax Description

milliseconds	Delay time in milliseconds before the data is emptied from the queue. Enter an integer from 0 to 10000. A value of 0 disables the delay timer, causing the ACE to encrypt data from the server as it arrives and then sends the encrypted data to the client.

Command Modes

SSL parameter map configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The queue delay applies only to data that the ACE sends to the client.

Examples

To set the queue delay time to 500 milliseconds, enter:

```
host1/Admin(config-parammap-ssl)# queue-delay timeout 500
```

To disable the queue delay time to its default value of 0, enter:

```
host1/Admin(config-parammap-ssl)# no queue-delay
```

Related Commands

show parameter-map

(config-parammap-ssl) session-cache timeout

To set the session cache timeout, use the **session-cache timeout** command. Use the **no** form of this command to disable the timer and ensure that the full SSL handshake occurs for each new connection with the ACE.

session-cache timeout *seconds*

no session-cache timeout

Syntax Description

seconds	Time in seconds that the ACE reuses the key stored in the cache before removing the session IDs. Enter an integer from 0 to 72000 (20 hours). By default, session ID reuse is disabled. A value of 0 causes the ACE to remove the session IDs from the cache when the cache is full and to implement the least-recently-used (LRU) timeout policy.

Command Modes

SSL parameter map configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

A SSL session ID is created every time the client and the ACE perform a full SSL key exchange and establish a new master secret key. To quicken the SSL negotiation process between the client and the ACE, the SSL session ID reuse feature allows the ACE to reuse the secret key information in the session cache. On subsequent connections with the client, the ACE reuses the key stored in the cache from the last negotiated session.

You can enable session ID reuse by setting a session cache timeout value for the total amount of time that the SSL session ID remains valid before the ACE requires a full SSL handshake to establish a new session.

Examples

To set the session cache timeout to 600 milliseconds, enter:

```
host1/Admin(config-parammap-ssl)# session-cache timeout 600
```

To disable the timer and ensure that the full SSL handshake occurs for each new connection with the ACE, enter:

```
host1/Admin(config-parammap-ssl)# no session-cache timeout
```

Related Commands

show parameter-map

(config-parammap-ssl) version

To specify the versions of Secure Sockets Layer (SSL) and Transport Layer Security (TLS) that the ACE supports when it uses the SSL proxy parameter map during the handshake process, use the **version** command. Use the **no** form of the command to remove a version from the SSL proxy parameter map.

version {**all** | **ssl3** | **tls1**}

no version

Syntax Description

all	Specifies that the ACE supports both SSL (version SSL3) and TLS (version TLS1). This is the default setting.
ssl3	Specifies that the ACE supports only SSL version SSL3.
tls1	Specifies that the ACE supports only TLS version TLS1.

Command Modes

SSL parameter map configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To specify the version SSL3, enter:

```
host1/Admin(config-parammap-ssl)# version SSL3
```

To remove the version TLS1 from the SSL proxy parameter map, enter:

```
host1/Admin(config-parammap-ssl)# no version
```

Related Commands

(config-parammap-ssl) cipher
(config-parammap-ssl) queue-delay timeout
(config-parammap-ssl) session-cache timeout
show parameter-map

Policy Map Configuration Mode Commands

Policy map configuration mode commands allow you to configure a Layer 3 and Layer 4 policy map that defines the different actions applied to traffic that passes through the ACE. The ACE attempts to match multiple classes within the Layer 3 and Layer 4 policy map to allow a multifeature Layer 3 and Layer 4 policy map. The ACE executes the action for only one matching class within each of the class sets. The definition of which classes are in the same class set depends on the actions applied to the classes; the ACE associates each policy map action with a specific set of classes.

To create a Layer 3 and Layer 4 policy map and access policy map configuration mode, use the **policy-map multi-match** command in configuration mode. When you access the policy map configuration mode, the prompt changes to (config-pmap). Use the **no** form of this command to remove a Layer 3 and Layer 4 policy map from the ACE.

For a Layer 3 and Layer 4 traffic classification, you create Layer 3 and Layer 4 policy maps with actions that configure the following:

- Server load balancing based on Layer 3 and Layer 4 connection information (virtual IP address)
- Application acceleration and optimization
- Secure Sockets Layer (SSL) security services between a web browser (the client) and the HTTP connection (the server)
- Static or dynamic Network Address Translation (NAT)
- Application protocol inspection (also known as protocol fixup)
- TCP termination, normalization, and reuse
- IP normalization and fragment reassembly

Use the **no** form of the **policy-map multimatch** command to remove a policy map from the ACE.

policy-map multi-match *map_name*

no policy-map multi-match *map_name*

Syntax Description

map_name	Name assigned to the Layer 3 and Layer 4 policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the loadbalance, inspect, connection, NAT, or SSL feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To perform HTTP load balancing, HTTP deep packet inspection, or FTP command inspection functions, you associate a previously created Layer 7 policy map within a Layer 3 and Layer 4 policy map to provide an entry point for the traffic classification. Layer 7 policy maps are considered to be child policies and can be associated only within a Layer 3 and Layer 4 policy map. Only a Layer 3 and Layer 4 policy map can be activated on a VLAN interface. A Layer 7 policy map cannot be directly applied on a VLAN (or any) interface. For example, to associate a Layer 7 HTTP load-balancing policy map, you nest the Layer 7 load-balancing policy map by using the Layer 3 and Layer 4 **(config-pmap-c) loadbalance policy** command.

The ACE supports a system-wide maximum of 4096 policy maps.

Examples

To create a Layer 3 and Layer 4 server load balancing (SLB) policy map named L4_SLB_POLICY, enter:

```
host1/Admin(config)# policy-map multi-match L4_SLB_POLICY
host1/Admin(config-pmap)#
```

To create a Layer 3 and Layer 4 application protocol inspection policy map named L4_HTTP_APP_INSPECTION_POLICY, enter:

```
host1/Admin(config)# policy-map multi-match L4_HTTP_APP_INSPECTION_POLICY
host1/Admin(config-pmap)#
```

Related Commands

show startup-config
(config) class-map

(config-pmap) class

To associate a Layer 3 and Layer 4 class map with a Layer 3 and Layer 4 policy map, use the **class** command. The prompt changes from (config-pmap) to (config-pmap-c). For information about commands in this mode, see the "Policy Map Class Configuration Mode Commands" section. Use the **no** form of this command to remove an associated class map from a policy map.

class {*name1* [**insert-before** *name2*] | **class-default**}

no class {*name1* [**insert-before** *name2*]}

Syntax Description

name1	Name of a previously defined Layer 3 and Layer 4 traffic class configured with the **class-map** command. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
insert-before *name2*	(Optional) Places the current named class map ahead of an existing class map or inline match condition specified by the *name2* argument in the policy-map configuration. The ACE does not save the sequence reordering as part of the configuration. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
class-default	Associates the reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified under the **class class-default** command. The **class-default** class map has an implicit **match any** statement in it that enables it to match all traffic.

Command Modes

Policy map configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To associate a Layer 3 and Layer 4 class map with a Layer 3 and Layer 4 policy map, enter:

```
host1/Admin(config)# policy-map multi-match L4_SLB_POLICY
host1/Admin(config-pmap)# class L4_SLB_CLASS
host1/Admin(config-pmap-c)#
```

Related Commands

(config-pmap) description

(config-pmap) description

To provide a brief summary about the Layer 3 and Layer 4 policy map, use the **description** command. Use the **no** form of this command to remove the description from the class map.

description *text*

no description

Syntax Description

text	Description for the policy map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Policy map configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description that the class map is to perform Layer 3 and Layer 4 server load balancing, enter:

```
host1/Admin(config)# policy-map multi-match L4_SLB_POLICY
host1/Admin(config-pmap)# description Policy map for L3/L4 SLB
```

Related Commands

(config-pmap) class

Policy Map Class Configuration Mode Commands

Policy map class configuration mode commands allow you to specify the actions that the ACE should take when network traffic matches one or more match statements in the associated Layer 3 and Layer 4 class map. To access policy map class configuration mode, use the **class** command in policy map configuration mode (see the **(config-pmap) class** command for details). The prompt changes from (config-pmap) to (config-pmap-c).

The features required in your user role to execute a specific command in policy map class configuration mode are described in the "Usage Guidelines" section of the command. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

(config-pmap-c) appl-parameter dns advanced-options

To associate a DNS parameter map with a Layer 3 and Layer 4 policy map, use the **appl-parameter dns advanced-options** command. Use the **no** form of this command to disassociate the DNS parameter map as an action from the Layer 3 and Layer 4 generic application inspection policy map.

appl-parameter dns advanced-options *name*

no appl-parameter dns advanced-options *name*

Syntax Description

name	Name of an existing DNS parameter map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Policy map class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To associate a DNS parameter map with a Layer 3 and Layer 4 policy map, enter:

```
host1/Admin(config)# policy-map multi-match DNS_INSPECT_L4POLICY
host1/Admin(config-pmap)# class DNS_INSPECT_L4CLASS
host1/Admin(config-pmap-c)# appl-parameter dns advanced-options DNS_PARAM_MAP1
```

To disassociate the DNS parameter map from the Layer 3 and Layer 4 policy map, enter:

```
host1/Admin(config-pmap-c)# no appl-parameter dns advanced-options DNS_PARAM_MAP1
```

Related Commands

show parameter-map
(config) parameter-map type

(config-pmap-c) appl-parameter generic advanced-options

To associate a generic Layer 7 parameter map with a Layer 3 and Layer 4 policy map, use the **appl-parameter generic advanced-options** command. Use the **no** form of this command to disassociate the generic Layer 7 parameter map as an action from the Layer 3 and Layer 4 generic application inspection policy map.

appl-parameter generic advanced-options *name*

no appl-parameter generic advanced-options *name*

Syntax Description

name	Name of an existing generic Layer 7 parameter map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Policy map class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To associate a generic Layer 7 parameter map with the Layer 3 and Layer 4 policy map, enter:

```
host1/Admin(config)# policy-map multi-match GEN_L7_INSPECT_L4POLICY
host1/Admin(config-pmap)# class GEN_L7_INSPECT_L4CLASS
host1/Admin(config-pmap-c)# appl-parameter generic advanced-options GEN_L7_PARAM_MAP1
```

To disassociate the generic Layer 7 parameter map from the Layer 3 and Layer 4 policy map, enter:

```
host1/Admin(config-pmap-c)# no appl-parameter generic advanced-options GEN_L7_PARAM_MAP1
```

Related Commands

show parameter-map
(config) parameter-map type

(config-pmap-c) appl-parameter http advanced-options

To associate an HTTP parameter map with a Layer 3 and Layer 4 policy map, use the **appl-parameter http advanced-options** command. A parameter map is a means to combine related actions for use in a Layer 3 and Layer 4 HTTP policy map. Use the **no** form of this command to disassociate the HTTP parameter map as an action from the policy map.

appl-parameter http advanced-options *name*

no appl-parameter http advanced-options *name*

Syntax Description

name	Name of an existing HTTP parameter map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Policy map class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the loadbalance and inspect features in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To associate an HTTP parameter map with a Layer 3 and Layer 4 policy map, enter:

```
host1/Admin(config)# policy-map multi-match L4SLBPOLICY
host1/Admin(config-pmap)# class FILTERHTTP
host1/Admin(config-pmap-c)# appl-parameter http advanced-options http_param_map1
```

Related Commands

show parameter-map
(config) parameter-map type

(config-pmap-c) appl-parameter rtsp advanced-options

To associate a Real-Time Streaming Protocol (RTSP) parameter map with a Layer 3 and Layer 4 policy map, use the **appl-parameter rtsp advanced-options** command. A parameter map is a means to combine related actions for use in a Layer 3 and Layer 4 RTSP policy map. Use the **no** form of this command to disassociate the RTSP parameter map from the policy map.

appl-parameter rtsp advanced-options *name*

no appl-parameter rtsp advanced-options *name*

Syntax Description

name	Name of an existing RTSP parameter map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Policy map class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command requires the loadbalance and inspect features in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To associate an RTSP parameter map with a Layer 3 and Layer 4 policy map, enter:

```
host1/Admin(config)# policy-map multi-match L4SLBPOLICY
host1/Admin(config-pmap)# class FILTERHTTP
host1/Admin(config-pmap-c)# appl-parameter rtsp advanced-options rtsp_param_map1
```

Related Commands

show parameter-map
(config) parameter-map type

(config-pmap-c) appl-parameter sip advanced-options

To associate a Session Initiation Protocol (SIP) application protocol inspection parameter map with a Layer 3 and Layer 4 policy map, use the **appl-parameter sip advanced-options** command. Use the **no** form of this command to disassociate the SIP parameter map as an action from the Layer 3 and Layer 4 SIP application inspection policy map.

appl-parameter sip advanced-options *name*

no appl-parameter sip advanced-options *name*

Syntax Description

name	Name of an existing SIP parameter map. Parameter maps aggregate SIP traffic-related actions together. Enter the name of an existing SIP parameter map as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Policy map class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To associate a SIP parameter map with a SIP packet inspection policy map, enter:

```
host1/Admin(config)# policy-map multi-match SIP_INSPECT_L4POLICY
host1/Admin(config-pmap)# class SIP_INSPECT_L4CLASS
host1/Admin(config-pmap-c)# appl-parameter sip advanced-options SIP_PARAM_MAP1
```

To disassociate the SIP parameter map from the SIP packet inspection policy map, enter:

```
host1/Admin(config-pmap-c)# no appl-parameter sip advanced-options SIP_PARAM_MAP1
```

Related Commands

show parameter-map
(config) parameter-map type

(config-pmap-c) appl-parameter skinny advanced-options

To associate a Skinny Client Control Protocol (SCCP) parameter map with a Layer 3 and Layer 4 policy map, use the **appl-parameter skinny advanced-options** command. Use the **no** form of this command to disassociate the SCCP parameter map as an action from the Layer 3 and Layer 4 SCCP application inspection policy map.

appl-parameter skinny advanced-options *name*

no appl-parameter skinny advanced-options *name*

Syntax Description

name	Name of an existing SCCP parameter map. Parameter maps aggregate SCCP traffic-related actions together. Enter the name of an existing SCCP parameter map as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Policy map class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To associate an SCCP parameter map with the SCCP deep packet inspection policy map, enter:

```
host1/Admin(config)# policy-map multi-match SCCP_INSPECT_L4POLICY
host1/Admin(config-pmap)# class SCCP_INSPECT_L4CLASS
host1/Admin(config-pmap-c)# appl-parameter skinny advanced-options SCCP_PARAM_MAP1
```

To disassociate the SCCP parameter map from the SCCP packet inspection policy map, enter:

```
host1/Admin(config-pmap-c)# no appl-parameter skinny advanced-options SCCP_PARAM_MAP1
```

Related Commands

show parameter-map
(config) parameter-map type

(config-pmap-c) connection advanced-options

To associate a connection parameter map with a Layer 3 and Layer 4 policy map, use the **connection advanced-options** command. Use the **no** form of this command to disassociate the parameter map from a policy map.

connection advanced-options *name*

no connection advanced-options *name*

Syntax Description

name	Name of an existing connection parameter map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Policy map class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the connection feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

For details about configuring a connection parameter map, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

Examples

To associate the connection parameter map IP_MAP with a Layer 3 and Layer 4 TCP/IP policy map:

```
host1/Admin(config)# policy-map multi-match TCPIP_POLICY
host1/Admin(config-pmap)# class TCP_CLASS
host1/Admin(config-pmap-c)# connection advanced-options IP_MAP
```

Related Commands

This command has no related commands.

(config-pmap-c) inspect

To define the Layer 3 and Layer 4 HTTP deep packet inspection, File Transfer Protocol (FTP) command inspection, or application protocol inspection policy actions, use the **inspect** command. Application inspection involves the examination of protocols such as Domain Name System (DNS), FTP, HTTP, Internet Control Message Protocol (ICMP), and Real Time Streaming Protocol (RTSP) to verify the protocol behavior and identify unwanted or malicious traffic that passes through the ACE. Use the **no** form of this command to remove an associated class map from a policy map.

inspect {**dns** [**maximum-length** *bytes*]} | {**ftp** [**strict policy** *name1* | **sec-param** *conn_parammap_name1*]} | {**http** [**policy** *name4* | **url-logging**]} | {**icmp** [**error**]} | **ils** | {**rtsp** [**sec-param** *conn_parammap_name3*]} | {**sip** [**sec-param** *conn_parammap_name4*] [**policy** *name5*]} | {**skinny** [**sec-param** *conn_parammap_name5*] [**policy** *name6*]}

no inspect {**dns** [**maximum-length** *bytes*]} | {**ftp** [**strict policy** *name1* | **sec-param** *conn_parammap_name1*]} | {**http** [**policy** *name4* | **url-logging**]} | {**icmp** [**error**]} | **ils** | {**rtsp** [**sec-param** *conn_parammap_name3*]} | {**sip** [**sec-param** *conn_parammap_name4*] [**policy** *name5*]} | {**skinny** [**sec-param** *conn_parammap_name5*] [**policy** *name6*]}

Syntax Description

dns	Enables DNS query inspection. DNS requires application inspection so that DNS queries will not be subject to the generic UDP handling based on activity timeouts. Instead, the UDP connections associated with DNS queries and responses are torn down as soon as a reply to a DNS query has been received. The ACE performs the reassembly of DNS packets to verify that the packet length is less than the configured maximum length.
maximum-length *bytes*	(Optional) Sets the maximum length of a DNS reply. Valid entries are from 512 to 65535 bytes. The default is 512 bytes.
ftp	Enables FTP inspection. The ACE inspects FTP packets, translates the address and the port that are embedded in the payload, and opens up a secondary channel for data.
strict	(Optional) Checks for protocol RFC compliance and prevents web browsers from sending embedded commands in FTP requests. The **strict** keyword prevents an FTP client from determining valid usernames that are supported on an FTP server. When an FTP server replies to the USER command, the ACE intercepts the 530 reply code from the FTP server and replaces it with the 331 reply code. Specifying an FTP inspection policy allows selective command filtering and also prevents the display of the FTP server system type to the FTP client. The ACE intercepts the FTP server 215 reply code and message to the SYST command, and then replaces the text following the reply code with asterisks.
policy *name1*	Specifies the name assigned to a previously created Layer 7 FTP command inspection policy map to implement the inspection of Layer 7 FTP commands by the ACE. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. Use the **inspect ftp** command in policy map class configuration mode to define the FTP command request inspection policy. **Note** If you do not specify a Layer 7 policy map, the ACE performs a general set of Layer 3 and Layer 4 FTP fixup actions.

sec-param *conn_parammap_name1*	(Optional) Specifies the name of a previously created connection parameter map used to define parameters for FTP inspection.
http	Enables enhanced Hypertext Transfer Protocol (HTTP) inspection on the HTTP traffic. The inspection checks are based on configured parameters in an existing Layer 7 policy map and internal RFC compliance checks performed by the ACE. By default, the ACE allows all request methods.
policy *name4*	(Optional) Specifies the name assigned to a previously created Layer 7 HTTP application inspection policy map to implement the deep packet inspection of Layer 7 HTTP application traffic by the ACE. The inspection checks are based on configured parameters in an existing Layer 7 policy map and internal RFC compliance checks performed by the ACE. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. **Note** If you do not specify a Layer 7 policy map, the ACE performs a general set of Layer 3 and Layer 4 HTTP fixup actions and internal RFC compliance checks.
url-logging	(Optional) Enables the monitoring of Layer 3 and Layer 4 traffic. This function logs every URL request that is sent in the specified class of traffic, including the source or destination IP address and the URL that is accessed.
icmp	Enables ICMP payload inspection. ICMP inspection allows ICMP traffic to have a “session” so it can be inspected similarly to TCP and UDP traffic.
error	(Optional) Performs a Network Address Translation (NAT) of ICMP error messages. The ACE creates translation sessions for intermediate or endpoint nodes that send ICMP error messages based on the NAT configuration. The ACE overwrites the packet with the translated IP addresses.
ils	Enables Internet Locator Service (ILS) protocol inspection.
rtsp	Enables RTSP packet inspection. RTSP is used by RealAudio, RealNetworks, Apple QuickTime 4, RealPlayer, and Cisco IP/TV connections. The ACE monitors Setup and Response (200 OK) messages in the control channel established using TCP port 554 (no UDP support).
sec-param *conn_parammap_name3*	(Optional) Specifies the name of a previously created connection parameter map used to define parameters for RTSP inspection.
sip	Enables Session Initiation Protocol (SIP) inspection. SIP is used for call handling sessions and instant messaging. The ACE inspects signaling messages for media connection addresses, media ports, and embryonic connections. The ACE also uses NAT to translate IP addresses that are embedded in the user-data portion of the packet.
sec-param *conn_parammap_name4*	(Optional) Specifies the name of a previously created connection parameter map used to define parameters for SIP inspection.

policy *name5*	(Optional) Specifies the name of a previously created Layer 7 SIP application inspection policy map to implement packet inspection of Layer 7 SIP application traffic by the ACE. The inspection checks are based on configured parameters in an existing Layer 7 policy map and internal RFC compliance checks performed by the ACE. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. **Note** If you do not specify a Layer 7 policy map, the ACE performs a general set of Layer 3 and Layer 4 HTTP fixup actions and internal RFC compliance checks.
skinny	Enables Cisco Skinny Client Control Protocol (SCCP) inspection. The SCCP is a Cisco proprietary protocol that is used between Cisco CallManager and CIsco VOiP phones. The ACE uses NAT to translate embedded IP addresses and port numbers in SCCP packet data.
sec-param *conn_parammap_name5*	(Optional) Specifies the name of a previously created connection parameter map used to define parameters for SCCP inspection.
policy *name6*	(Optional) Specifies the name of a previously created deep packet inspection of Layer 7 SCCP application traffic by the ACE. The inspection checks are based on configured parameters in an existing Layer 7 policy map and internal RFC compliance checks performed by the ACE. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. **Note** If you do not specify a Layer 7 policy map, the ACE performs a general set of Layer 3 and Layer 4 HTTP fixup actions and internal RFC compliance checks.

Command Modes

Policy map class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised.

Usage Guidelines

This command requires the inspect feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To perform the deep packet inspection of Layer 7 HTTP application traffic by the ACE, you should create a Layer 7 HTTP deep packet inspection policy using the **policy-map type inspect http** command (see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*). Nest the Layer 7 deep packet inspection policy using the Layer 3 and Layer 4 **inspect http** command. If you do not specify a Layer 7 HTTP policy map, the ACE performs a general set of Layer 3 and Layer 4 HTTP fixup actions and internal RFC compliance checks.

To perform checks for protocol RFC compliance and to prevent web browsers from sending embedded commands in FTP requests, you should create a Layer 7 FTP policy using the **policy-map type inspect ftp** command (see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*). Nest the Layer 7 FTP inspection traffic policy using the Layer 3 and Layer 4 **inspect ftp** command. If you do not specify a Layer 7 FTP policy map, the ACE performs a general set of Layer 3 and Layer 4 FTP fixup actions.

Examples

To specify the **inspect http** command as an action for an HTTP application protocol inspection policy map, enter:

```
host1/Admin(config)# policy-map multi-match HTTP_INSPECT_L4POLICY
host1/Admin(config-pmap)# class HTTP_INSPECT_L4CLASS
host1/Admin(config-pmap-c)# inspect http policy HTTP_DEEPINSPECT_L7POLICY
```

Related Commands

This command has no related commands.

(config-pmap-c) loadbalance policy

To associate a Layer 7 server load balancing (SLB) policy map with a Layer 3 and Layer 4 SLB policy map, use the **loadbalance policy** command. Use the **no** form of this command to disassociate the Layer 7 SLB policy from the Layer 3 and Layer 4 SLB policy map.

loadbalance policy *name*

no loadbalance policy *name*

Syntax Description

name	Name of an existing Layer 7 SLB policy map. Enter the name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Policy map class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The ACE treats all Layer 7 policy maps as child policies, so you must always associate a Layer 7 SLB policy map with a Layer 3 and Layer 4 SLB policy map.

Examples

To reference the Layer 7 L7SLBPOLICY policy map within the Layer 3 and Layer 4 L4SLBPOLICY policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance first-match L7SLBPOLICY
host1/Admin(config-pmap)# class L7SLBCLASS
host1/Admin(config-pmap-c)# serverfarm FARM2

host1/Admin(config)# policy-map multi-match L4SLBPOLICY
host1/Admin(config-pmap)# class L4SLBCLASS
host1/Admin(config-pmap-c)# loadbalance policy L7SLBPOLICY
```

Related Commands

This command has no related commands.

(config-pmap-c) loadbalance vip icmp-reply

To enable a VIP to reply to ICMP requests, use the **loadbalance vip icmp-reply** command. For example, if a user sends an ICMP ECHO request to a VIP, this command instructs the VIP to send an ICMP ECHO-REPLY. Use the **no** form of this command to disable a VIP reply to ICMP requests as an action from the policy map.

loadbalance vip icmp-reply [**active** [**primary-inservice**]]

no loadbalance vip icmp-reply [**active** [**primary-inservice**]]

Syntax Description

active	(Optional) Instructs the ACE to reply to an ICMP request only if the configured VIP is active. If the VIP is not active and the **active** option is specified, the ACE discards the ICMP request and the request times out.
primary-inservice	(Optional) Instructs the ACE to reply to an ICMP ping only if the primary server farm state is UP, regardless of the state of the backup server farm. If this option is enabled and the primary server farm state is DOWN, the ACE discards the ICMP request and the request times out.

Command Modes

Policy map class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To complete the configuration when you configure the **active** option of this command, be sure to configure a Telnet probe and associate it with the server farm. The probe monitors the health of all the real servers in the server farm and ensures that the VIP responds with an ICMP ECHO REPLY only if the server port is active. If the server port is down or unreachable, the probe fails and the VIP stops responding to the ECHO request. For details about configuring probes, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

The **loadbalance vip icmp-reply active** command alone controls a ping to a VIP on the ACE. This command implicitly downloads an ICMP access control list entry for the VIP. When you configure this command on the ACE, any configured ACLs that deny ICMP traffic have no effect on a client's ability to ping the VIP.

Examples

To enable a VIP to reply to ICMP requests, enter:

```
host1/Admin(config)# policy-map multi-match L4SLBPOLICY
host1/Admin(config-pmap)# class FILTERHTTP
host1/Admin(config-pmap-c)# loadbalance vip icmp-reply active
```

Related Commands This command has no related commands.

(config-pmap-c) loadbalance vip inservice

To enable a VIP for server load-balancing operations, use the **loadbalance vip inservice** command. Use the **no** form of this command to disable a VIP.

loadbalance vip inservice

no loadbalance vip inservice

Syntax Description This command has no keywords or arguments.

Command Modes Policy map class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines This command requires the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples To specify the **loadbalance vip inservice** command as an action for a server load-balancing policy map, enter:

```
host1/Admin(config)# policy-map multi-match L4SLBPOLICY
host1/Admin(config-pmap)# class FILTERHTTP
host1/Admin(config-pmap-c)# loadbalance vip oos-arpreply enable
host1/Admin(config-pmap-c)# loadbalance vip inservice
```

Related Commands This command has no related commands.

(config-pmap-c) loadbalance vip udp-fast-age

To close the connection immediately after a response is sent back to the client, enabling per-packet load balancing for User Datagram Protocol (UDP) traffic, use the **loadbalance vip udp-fast-age** command. Use the **no** form of this command to reset the ACE default behavior.

loadbalance vip udp-fast-age

no loadbalance vip udp-fast-age

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command requires the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

When you use this command, the ACE load balances all new requests to a new real server in the server farm according to the predictor algorithm. All retransmitted UDP packets from the client go to the same real server.

By default, the ACE load balances UDP packets using the same tuple to the same real server on an existing connection.

Examples

To configure the ACE to perform per-packet load balancing for UDP traffic, enter:

```
host1/Admin(config)# policy-map multi-match L4SLBPOLICY
host1/Admin(config-pmap)# class FILTERHTTP
host1/Admin(config-pmap-c)# loadbalance vip udp-fast-age
```

To reset the default ACE handling of UDP traffic, enter:

```
host1/Admin(config-pmap-c)# no loadbalance vip udp-fast-age
```

Related Commands

This command has no related commands.

(config-pmap-c) nat dynamic

To configure dynamic Network Address Translation (NAT) and Port Address Translation (PAT) as an action in a policy map, use the **nat dynamic** command. The ACE applies the dynamic NAT from the interface attached to the traffic policy (through the **service-policy** interface configuration command) to the interface specified in the **nat dynamic** command. Use the **no** form of this command to remove a dynamic NAT action from a policy map.

nat dynamic *nat_id* **vlan** *number*

no nat dynamic *nat_id* **vlan** *number*

Syntax Description

nat dynamic *nat_id*	Refers to a global pool of IP addresses that exists under the VLAN number. Dynamic NAT translates a group of local source IP addresses to a pool of global IP addresses that are routable on the destination network. All packets going from the interface attached to the traffic policy have their source address translated to one of the available addresses in the global pool. Enter an integer from 1 to 2147483647.
vlan *number*	Specifies the VLAN number of an existing interface for which you are configuring NAT. Enter an integer from 2 to 4094.

Command Modes

Policy map class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the NAT feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

If a packet egresses an interface that you have not configured for NAT, the ACE transmits the packet untranslated.

Examples

To specify the **nat dynamic** command as an action for a dynamic NAT policy map, enter:

```
host1/Admin(config)# policy-map multi-action NAT_POLICY
host1/Admin(config-pmap)# class NAT_CLASS
host1/Admin(config-pmap-c)# nat dynamic 1 vlan 200
```

Related Commands

This command has no related commands.

(config-pmap-c) nat static

To configure static Network Address Translation (NAT) and static port redirection in a policy map, use the **nat static** command. Static NAT allows you to identify local traffic for address translation by specifying the source and destination addresses in an extended access control list (ACL) that is referenced as part of the class map traffic classification. The ACE applies static NAT from the interface attached to the traffic policy (through the **service-policy** interface configuration command) to the interface specified in the **nat static** command. Use the **no** form of this command to remove a NAT action from a policy map.

nat static *ip_address* **netmask** *mask* {*port1* | **tcp eq** *port2* | **udp eq** *port3*} **vlan** *number*

no nat static *ip_address* **netmask** *mask* {*port1* | **tcp eq** *port2* | **udp eq** *port3*} **vlan** *number*

Syntax Description

ip_address	IP address for a single static translation. This argument establishes the globally unique IP address of a host as it appears to the outside world. The policy map performs the global IP address translation for the source IP address specified in the ACL (as part of the class map traffic classification).
netmask *mask*	Specifies the subnet mask for the IP address. Enter a subnet mask in dotted-decimal notation (for example, 255.255.255.0).
port1	Global TCP or UDP port for static port redirection. Enter an integer from 0 to 65535.
tcp eq *port2*	Specifies a TCP port name or number. Enter an integer from 0 to 65535. A value of 0 instructs the ACE to match any port. Alternatively, you can enter a protocol keyword that corresponds to a TCP port number. See the "Usage Guidelines" section for a list of supported well-known TCP port names and numbers.
udp eq *port3*	Specifies a UDP port name or number. Enter an integer from 0 to 65535. A value of 0 instructs the ACE to match any port. Alternatively, you can enter a protocol keyword that corresponds to a UDP port number. See the "Usage Guidelines" section for a list of supported well-known UDP port names and numbers.
vlan *number*	Specifies the interface for the global IP address. This interface must be different from the interface that the ACE uses to filter and receive traffic that requires NAT.

Command Modes

Policy map class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the NAT feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Table 2-15 provides a list of supported well-known TCP and UDP port names and numbers.

Table 2-15 Supported TCP and UDP Ports

Well-Known TCP Port Numbers and Keywords		
Keyword	**Port Number**	**Description**
ftp	21	File Transfer Protocol
http	80	Hyper Text Transfer Protocol
https	443	HTTP over TLS/SSL
irc	194	Internet Relay Chat
matip-a	350	Mapping of Airline Traffic over Internet Protocol (MATIP) Type A
nntp	119	Network News Transport Protocol
pop2	109	Post Office Protocol v2
pop3	110	Post Office Protocol v3
rtsp	554	Real Time Streaming Protocol
smtp	25	Simple Mail Transfer Protocol
telnet	23	Telnet
Well-Known UDP Port Numbers and Keywords		
dns	53	Domain Name System
wsp	9200	Connectionless Wireless Session Protocol (WSP)
wsp-wtls	9202	Secure Connectionless WSP
wsp-wtp	9201	Connection-based WSP
wsp-wtp-wtls	9203	Secure Connection-based WSP

Examples

To specify the **nat** command as an action for a static NAT and port redirection policy map, enter:

```
host1/Admin(config)# policy-map multi-action NAT_POLICY
host1/Admin(config-pmap)# class NAT_CLASS
host1/Admin(config-pmap-c)# nat static 192.168.12.15 255.255.255.0 8080 vlan 200
```

Related Commands

This command has no related commands.

(config-pmap-c) ssl-proxy

To associate the Secure Sockets Layer (SSL) client or server proxy service with the policy map, use the **ssl-proxy** command. Use the **no** form of this command to remove the SSL proxy service from the policy map.

ssl-proxy {**client** | **server**} *ssl_service_name*

no ssl-proxy {**client** | **server**} *ssl_service_name*

Syntax Description

client	Associates an SSL client proxy service with the policy map. This keyword is available only when building a Layer 7 policy map, where the ACE acts as an SSL client device.
server	Associates an SSL server proxy service with the policy map. This keyword is available only when building a Layer 2 or Layer 3 policy map, where the ACE acts as an SSL server device.
ssl_service_name	Name of an existing SSL proxy service. Enter the name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Policy map configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the SSL feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To associate the SSL proxy service with the policy map, enter:

```
host1/C1(config-pmap-c)# ssl-proxy server SSL_SERVER_PROXY_SERVICE
host1/C1(config-pmap-c)#
```

Related Commands

This command has no related commands.

Policy Map FTP Inspection Configuration Mode Commands

Policy map FTP inspection configuration mode commands allow you to configure a Layer 7 policy map that defines the inspection of the File Transfer Protocol (FTP) commands by the ACE. The ACE executes the action for the first matching classification.

To create an FTP command request inspection policy map and access policy map FTP inspection configuration mode, use the **policy-map type inspect ftp first-match** command in configuration mode. When you access the policy map FTP inspection configuration mode, the prompt changes to (config-pmap-ftp-ins). Use the **no** form of this command to remove an FTP command request inspection policy map from the ACE.

policy-map type inspect ftp first-match *map_name*

no policy-map type inspect ftp first-match *map_name*

Syntax Description

map_name	Name assigned to the Layer 7 FTP command request class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the inspect feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You associate the Layer 7 FTP command request inspection policy map within a Layer 3 and Layer 4 policy map to provide an entry point for the traffic classification. Layer 7 policy maps are considered to be child policies and can be associated only within a Layer 3 and Layer 4 policy map. Only a Layer 3 and Layer 4 policy map can be activated on a VLAN interface. A Layer 7 policy map cannot be directly applied on a VLAN (or any) interface.

To associate the Layer 7 FTP inspection policy map, you nest it by using the Layer 3 and Layer 4 **inspect ftp strict** command (see the **(config-pmap-c) inspect** command).

Examples

To create a Layer 7 FTP command inspection policy map, enter:

```
host/Admin(config)# policy-map type inspect ftp first-match FTP_INSPECT_L7POLICY
host/Admin(config-pmap-ftp-ins) #
```

Related Commands

show startup-config
(config) class-map

(config-pmap-ftp-ins) class

To associate a Layer 7 File Transfer Protocol (FTP) inspection class map with a Layer 7 FTP inspection policy map, use the **class** command. The prompt changes from (config-pmap-ftp-ins) to (config-pmap-ftp-ins-c). For information about commands in this mode, see the "Policy Map FTP Inspection Class Configuration Mode Commands" section. Use the **no** form of this command to remove an associated class map from a policy map.

class *name*

no class *name*

Syntax Description

name	Name of a previously defined Layer 7 FTP command inspection class map configured with the **class-map** command. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Policy map FTP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To associate a Layer 7 FTP inspection class map with a Layer 7 FTP inspection policy map, enter:

```
host/Admin(config)# policy-map type inspect ftp first-match FTP_INSPECT_L7POLICY
host/Admin(config-pmap-ftp-ins)# class FTP_INSPECT_L7CLASS
host1/Admin(config-pmap-ftp-ins-c)#
```

Related Commands

(config-pmap-ftp-ins) description

(config-pmap-ftp-ins) description

To provide a brief summary about the Layer 7 File Transfer Protocol (FTP) command inspection policy map, use the **description** command. Use the **no** form of this command to remove the description from the class map.

description *text*

no description *text*

Syntax Description

text	Description for the policy map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Policy map configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description that the policy map is to perform FTP command inspection, enter:

```
host1/Admin(config-pmap-ftp-ins)# description FTP command inspection of incoming traffic
```

To remove d a description from the FTP policy map, enter:

```
host1/Admin(config-pmap-ftp-ins)# no description FTP command inspection of incoming
traffic
```

Related Commands

(config-pmap-ftp-ins) class

(config-pmap-ftp-ins) match request-method

To configure the Layer 7 FTP inspection policy map to define FTP command inspection decisions performed by the ACE, use the **match request-method** command. The prompt changes from (config-pmap-ftp-ins) to (config-pmap-ftp-ins-m). For information about commands in this mode, see the "Policy Map FTP Inspection Match Configuration Mode Commands" section. Use the **no** form of this command to clear the FTP inspection request method from the policy map.

match *name* **request-method** *ftp_command*

no match *name*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
ftp_command	FTP command in the class map to be subjected to FTP inspection by the ACE. The FTP commands are as follows: • **appe**—Appends to a file. • **cd**—Change to the specified directory. • **cdup**—Changes to the parent of the current directory. • **dele**—Deletes a file at the server side. • **get**—Retrieves a file. • **help**—Retrieves Help information from the server. • **mkd**—Creates a directory. • **put**—Stores a file. • **rmd**—Removes a directory. • **rnfr**—Renames from. • **rnto**—Renames to. • **site**—Specifies the server-specific command. • **stou**—Stores a file with a unique name. • **syst**—Gets system information.

Command Modes

Policy map FTP inspection configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The **match** command identifies the FTP command that you want filtered by the ACE.

You can specify multiple **match request-method** commands within a class map.

Examples

To add an inline **match** command to a Layer 7 FTP command policy map, enter:

```
host/Admin(config-pmap-ftp-ins)# match FTP_REQUEST_MATCH request-method mkdir
host/Admin(config-pmap-ftp-ins-m)#
```

Related Commands

This command has no related commands.

Policy Map FTP Inspection Class Configuration Mode Commands

Use the policy map File Transfer Protocol (FTP) inspection class configuration mode to specify the actions that the ACE should take when network traffic matches one or more match statements in the associated Layer 7 FTP inspection class map. To access policy map FTP inspection class configuration mode, use the **class** command in the policy map FTP inspection configuration mode (see the **(config-pmap-ftp-ins) class** command for details). The prompt changes from (config-pmap-ftp-ins) to (config-pmap-ftp-ins-c).

The commands in this mode require the inspect feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

(config-pmap-ftp-ins-c) deny

To deny the FTP request commands specified in the class map by resetting the FTP session, use the **deny** command. Use the **no** form of this command to return to the default state and permit all FTP request commands to pass.

deny

no deny

Command Modes

Policy map FTP inspection class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to deny the FTP request commands specified in the Layer 7 FTP inspection class map by resetting the FTP session, enter:

```
host1/Admin(config)# policy-map type inspect ftp first-match FTP_INSPECT_L7POLICY
host1/Admin(config-pmap-ftp-ins)# class FTP_INSPECT_L7CLASS
host1/Admin(config-pmap-ftp-ins-c)# deny
```

Related Commands

This command has no related commands.

(config-pmap-ftp-ins-c) mask-reply

To instruct the ACE to mask the reply to the FTP SYST command by filtering sensitive information from the command output, use the **mask-reply** command. Use the **no** form of this command to disable the masking of the system reply to the FTP SYST command.

mask-reply

no mask-reply

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map FTP inspection class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The **mask-reply** command is applicable only to the FTP SYST command and its associated reply. The SYST command is used to find out the FTP server's operating system type.

Examples

To instruct the ACE to mask the reply to the FTP SYST command, enter:

```
host1/Admin(config)# policy-map type inspect ftp first-match FTP_INSPECT_L7POLICY
host1/Admin(config-pmap-ftp-ins)# class FTP_INSPECT_L7CLASS
host1/Admin(config-pmap-ftp-ins-c)# mask-reply
```

Related Commands

This command has no related commands.

Policy Map FTP Inspection Match Configuration Mode Commands

Policy map FTP inspection match configuration mode commands allow you to specify the actions that the ACE should take when network traffic matches the specified inline match command. To access policy map FTP inspection match configuration mode, use the **match request-method** command in policy map FTP inspection configuration mode (see the **(config-pmap-ftp-ins) match request-method** command for details). The prompt changes from (config-pmap-ftp-ins) to (config-pmap-ftp-ins-m).

The inline Layer 7 policy map **match** commands allow you to include a single inline match criteria in the policy map without specifying a traffic class. The **match** commands function the same as with the Layer 7 class map **match** commands. However, when you use an inline **match** command, you can specify an action for only a single **match** command in the Layer 7 policy map.

The commands in this mode require the inspect feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

(config-pmap-ftp-ins-m) deny

To deny the FTP request commands specified in the inline **match** command by resetting the FTP session, use the **deny** command. By default, the ACE allows all FTP commands to pass. Use the **no** form of this command to return to the default state and permit all FTP request commands to pass.

deny

no deny

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map FTP inspection match configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to deny the FTP request commands specified in the Layer 7 FTP inspection class map by resetting the FTP session, enter:

```
host1/Admin(config)# policy-map type inspect ftp first-match FTP_INSPECT_L7POLICY
host/Admin(config-pmap-ftp-ins)# match FTP_REQUEST_MATCH request-method mkdir
host/Admin(config-pmap-ftp-ins-m)# deny
```

Related Commands

This command has no related commands.

(config-pmap-ftp-ins-m) mask-reply

To instruct the ACE to mask the system's reply to the FTP SYST command by filtering sensitive information from the command output, use the **mask-reply** command. Use the **no** form of this command to disable the masking of the system reply to the FTP SYST command.

mask-reply

no mask-reply

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map FTP inspection match configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The **mask-reply** command is applicable only to the FTP SYST command and its associated reply. The SYST command is used to find out the FTP server's operating system type.

Examples

To instruct the ACE to mask the system's reply to the FTP SYST command, enter:

```
host1/Admin(config)# policy-map type inspect ftp first-match FTP_INSPECT_L7POLICY
host/Admin(config-pmap-ftp-ins)# match FTP_REQUEST_MATCH request-method syst
host/Admin(config-pmap-ftp-ins-m)# mask-reply
```

Related Commands

This command has no related commands.

Policy Map Inspection HTTP Configuration Mode Commands

Policy map inspection HTTP configuration mode commands allow you to define a policy map that initiates the deep packet inspection of the HTTP protocol by the ACE. The ACE attempts to match all specified conditions against the matching classification and executes the actions of all matching classes until it encounters a deny for a match request.

To create an HTTP deep packet inspection policy map and access policy map inspection HTTP configuration mode, use the **policy-map type inspect http all-match** command in configuration mode. When you access the policy map inspection HTTP configuration mode, the prompt changes to (config-pmap-ins-http). Use the **no** form of this command to remove an HTTP deep packet inspection policy map from the ACE.

policy-map type inspect http all-match *map_name*

no policy-map type inspect http all-match *map_name*

Syntax Description

map_name	Name assigned to the Layer 7 HTTP deep packet inspection policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the inspect feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You associate the Layer 7 HTTP deep packet inspection policy map within a Layer 3 and Layer 4 policy map to provide an entry point for the traffic classification. Layer 7 policy maps are considered to be child policies and can only be associated within a Layer 3 and Layer 4 policy map. Only a Layer 3 and Layer 4 policy map can be activated on a VLAN interface. A Layer 7 policy map cannot be directly applied on a VLAN (or any) interface.

To associate the Layer 7 HTTP inspection policy map, you nest it by using the Layer 3 and Layer 4 **inspect http** command (see the **(config-pmap-c) inspect** command).

Examples

To create a Layer 7 HTTP deep packet inspection policy map, enter:

```
host/Admin(config)# policy-map type inspect http all-match HTTP_INSPECT_L7POLICY
host/Admin(config-pmap-ins-http)#
```

Related Commands

show startup-config
(config) class-map

(config-pmap-ins-http) class

To associate a Layer 7 HTTP inspection class map with a Layer 7 HTTP inspection policy map, use the **class** command. The prompt changes from (config-pmap-ins-http) to (config-pmap-ins-http-c). Use the **no** form of this command to remove an associated class map from a policy map.

class {*name1* [**insert-before** *name2*] | **class-default**}

no class {*name1* [**insert-before** *name2*] | **class-default**}

Syntax Description

name1	Name of a previously defined Layer 7 HTTP inspection class map configured with the **class-map** command. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
insert-before *name2*	(Optional) Places the current class map ahead of an existing class map or inline match condition specified by the *name2* argument in the policy map configuration. The ACE does not save the sequence reordering as part of the configuration.
class-default	Associates a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified under the **class class-default** command. The **class-default** class map has an implicit **match any** statement in it that enables it to match all traffic. **Note** By default, all matches are applied to both HTTP request and response messages, but the **class class-default** command is applied only to HTTP requests.

Command Modes

Policy map inspection HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To associate a Layer 7 HTTP inspection class map with a Layer 7 HTTP inspection policy map, enter:

```
host/Admin(config)# policy-map type inspect http all-match HTTP_INSPECT_L7POLICY
host1/Admin(config-pmap-ins-http)# class HTTP_INSPECT_L7CLASS
host1/Admin(config-pmap-ins-http-c)#
```

Related Commands

(config-pmap-ins-http) description

(config-pmap-ins-http) description

To provide a brief summary about the Layer 7 HTTP inspection policy map, use the **description** command. Use the **no** form of this command to remove the description from the class map.

description *text*

no description

Syntax Description

text	Description for the policy map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Policy map configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description that the policy map is to perform HTTP deep packet inspection, enter:

```
host1/Admin(config-pmap-ins-http)# description HTTP protocol deep inspection of incoming traffic
```

Related Commands

(config-pmap-ins-http) class

(config-pmap-ins-http) match content

To configure the Layer 7 HTTP inspection policy map to define HTTP application inspection decisions based on content expressions contained within the HTTP entity body, use the **match content** command. Use the **no** form of this command to clear content expression-checking match criteria from the policy map.

match *name* **content** *expression* [**offset** *number*] [**insert-before** *map_name*]

no match *name*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
expression	Content expression contained within the HTTP entity body. The range is from 1 to 255 alphanumeric characters. See the "Usage Guidelines" section for a list of the supported characters that you can use in regular expressions.
offset *number*	(Optional) Provides an absolute offset where the content expression search string starts. The offset starts at the first byte of the message body, after the empty line (CR, LF, CR, LF) between the headers and the body of the message. The offset value is from 1 to 4000 bytes.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map inspection HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When you use the **match content** command, you access the policy map inspection HTTP match configuration mode and the prompt changes from (config-pmap-ins-http) to (config-pmap-ins-http-m). You can then specify the actions that the ACE should take when network traffic matches the specified inline **match** command. For information about commands in this mode, see the "Policy Map Inspection HTTP Match Configuration Mode Commands" section.

The ACE supports regular expressions for matching. Expressions are stored in a header map in the form *header-name: expression*. Header expressions allow spaces, if the spaces are escaped or quoted. Table 2-16 lists the supported characters that you can use in regular expressions.

Table 2-16 Characters Supported in Regular Expressions

Convention	Description
.*	Zero or more characters.
.	Exactly one character.
\ .	Escaped character.
\xhh	Any ASCII character as specified in two-digit hex notation.
()	Expression grouping.
Bracketed range [for example, 0-9]	Matches any single character from the range.
A leading ^ in a range [^charset]	Does not match any character in the range; all other characters represent themselves.
(expr1 | expr2)	OR of expressions.
(expr)*	0 or more of expressions.
(expr)+	1 or more of expressions.
(expr{m,n}	Matches the previous item between *m* and *n* times; valid entries are from 0 to 255.
(expr{m}	Matches the previous item exactly *m* times; valid entries are from 1 to 255.
(expr{m,}	Matches the previous item *m* or more times; valid entries are from 1 to 255.
\a	Alert (ASCII 7).
\b	Backspace (ASCII 8).
\f	Form-feed (ASCII 12).
\n	New line (ASCII 10).
\r	Carriage return (ASCII 13).
\t	Tab (ASCII 9).
\v	Vertical tab (ASCII 11).
\0	Null (ASCII 0).
.\\	Backslash.

Examples

To specify a content expression contained within the entity body sent with an HTTP request, enter:

```
(config)# policy-map type inspect http all-match HTTP_INSPECT_L7POLICY
host1/Admin(config-pmap-ins-http)# match MATCH1 content .*newp2psig
host1/Admin(config-pmap-ins-http-m)
```

Related Commands

This command has no related commands.

(config-pmap-ins-http) match content length

To configure the Layer 7 HTTP inspection policy map to define application inspection decisions in the HTTP content up to the configured maximum content parse length, use the **match content length** command. Use the **no** form of this command to clear the HTTP content length match criteria from the policy map.

match *name* **content length** {**eq** *bytes* | **gt** *bytes* | **lt** *bytes* | **range** *bytes1 bytes 2*} [**insert-before** *map_name*]

no match *name*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
eq *bytes*	Specifies a value for the content parse length in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with a content length equal to the specified value. Valid entries are from 1 to 65535 bytes.
gt *bytes*	Specifies a minimum value for the content parse length in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with a content length greater than the specified value. Valid entries are from 1 to 65535 bytes.
lt *bytes*	Specifies a maximum value for the content parse length in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with a content length less than the specified value. Valid entries are from 1 to 65535 bytes.
range *bytes1 bytes*	Specifies a size range for the content parse length in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with a content length within this range. The range is from 1 to 65535 bytes.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map inspection HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Messages that meet the specified criteria will be either allowed or denied based on the Layer 7 HTTP deep packet inspection policy map action.

When you use the **match content length** command, you access the policy map inspection HTTP match configuration mode and the prompt changes from (config-pmap-ins-http) to (config-pmap-ins-http-m). You can then specify the actions that the ACE should take when network traffic matches the specified inline **match** command. For information about commands in this mode, see the "Policy Map Inspection HTTP Match Configuration Mode Commands" section.

Examples

To define application inspection decisions in the HTTP content up to the configured maximum content parse length, enter:

```
(config)# policy-map type inspect http all-match HTTP_INSPECT_L7POLICY
host1/Admin(config-pmap-ins-http)# match MATCH2 content length eq 3495
host1/Admin(config-pmap-ins-http-m)
```

Related Commands

This command has no related commands.

(config-pmap-ins-http) match content-type-verification

To verify the content MIME-type messages with the header MIME type, use the **match content-type-verification** command. Use the **no** form of this command to clear the MIME-type match criteria from the policy map.

match *name* **content-type-verification** [**insert-before** *map_name*]

no match *name*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map inspection HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When you use the **match content-type-verification** command, you access the policy map inspection HTTP match configuration mode and the prompt changes from (config-pmap-ins-http) to (config-pmap-ins-http-m). You can then specify the actions that the ACE should take when network traffic matches the specified inline **match** command. For information about commands in this mode, see the "Policy Map Inspection HTTP Match Configuration Mode Commands" section.

This inline match condition limits the MIME types in HTTP messages allowed through the ACE. It verifies that the header MIME-type value is in the internal list of supported MIME types and that the header MIME type matches the actual content in the data or entity body portion of the message. If they do not match, the ACE performs either the **permit** or **reset** policy map action.

The MIME-type HTTP inspection process searches the entity body of the HTTP message, which may degrade performance of the ACE.

Examples

To verify the content MIME-type messages with the header MIME type, enter:

```
(config)# policy-map type inspect http all-match HTTP_INSPECT_L7POLICY
host1/Admin(config-pmap-ins-http)# match MATCH3 content-type-verification
host1/Admin(config-pmap-ins-http-m)
```

Related Commands

This command has no related commands.

(config-pmap-ins-http) match cookie secondary

To configure a policy map to define HTTP inspection decisions based on the name or prefix and value of a secondary cookie (URL query string), use the **match cookie secondary** command. Use the **no** form of this command to clear secondary cookie match criteria from the class map.

match *name* **cookie secondary** [**name** *cookie_name* | **prefix** *prefix_name*] **value** *expression* [**insert-before** *map_name*]

no match *name* **cookie secondary** [**name** *cookie_name* | **prefix** *prefix_name*] **value** *expression*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
name *cookie_name*	Identifier of the secondary cookie to match. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
prefix *prefix_name*	Prefix of the secondary cookie to match. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

value *expression*	Regular expression of the secondary cookie to match. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map inspection HTTP configuration mode

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The following configuration guidelines apply when you configure a secondary cookie inline match statement for HTTP inspection:

- Ensure that secondary cookie names do not overlap with other secondary cookie names in the same match-all class map. For example, the following configuration is not allowed because the two match statements have overlapping cookie names:

```
(config)#  policy-map type inspect http all-match HTTP_INSPECT_L7POLICY
host1/Admin(config-pmap-insp-http)# match cookie secondary prefix id value .*
host1/Admin(config-pmap-insp-http-m)# exit
host1/Admin(config-pmap-insp-http)# match cookie secondary name identity value bob
```

- When you configure a secondary cookie value match across all secondary cookie names in a match-all class map, you cannot configure any other secondary cookie match in the same class map. That is because a secondary cookie match on value alone is equivalent to a wildcard match on name. In the following example, the second match statement is not allowed:

```
(config)#  policy-map type inspect http all-match HTTP_INSPECT_L7POLICY
host1/Admin(config-pmap-insp-http)# match cookie secondary value bob
host1/Admin(config-pmap-insp-http-m)# exit
host1/Admin(config-pmap-insp-http)# match cookie secondary name identity value jane
```

Examples

To match a secondary cookie called “matchme” with a regular expression value of .*abc123, enter the following commands:

```
(config)#  policy-map type inspect http all-match HTTP_INSPECT_L7POLICY
host1/Admin(config-pmap-insp-http)# match cookie secondary name matchme value .*abc123
```

Related Commands

(config-cmap-http-insp) match cookie secondary

(config-pmap-ins-http) match header

To define HTTP deep packet inspection decisions based on the name and value in an HTTP header, use the **match header** command. The ACE performs regular expression matching against the received packet data from a particular connection based on the HTTP header expression.Use the **no** form of this command to clear an HTTP header match criteria from the policy map.

match *name* **header** {*header_name* | *header_field*} **header-value** *expression* [**insert-before** *map_name*]

no match *name* **header**

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
header_name	Name of the HTTP header to match (for example, www.example1.com). The range is from 1 to 64 alphanumeric characters. **Note** The *header_name* argument cannot include the colon in the name of the HTTP header; the ACE rejects the colon as an invalid token.

header_field	Standard HTTP/1.1 header field. Valid selections include request-header fields, general-header fields, and entity-header fields. Selections also include two lower-level header-matching commands: "length" and "mime-type." The supported selections are as follows: • **Accept**—Semicolon-separated list of representation schemes (content type metainformation values) that will be accepted in the response to the request. • **Accept-Charset**—Character sets that are acceptable for the response. This field allows clients capable of understanding more comprehensive or special-purpose character sets to signal that capability to a server that can represent documents in those character sets. • **Accept-Encoding**—Restricts the content encoding that a user will accept from the server. • **Accept-Language**—ISO code for the language in which the document is written. The language code is an ISO 3316 language code with an optional ISO639 country code to specify a national variant. • **Authorization**—Specifies that the user agent wants to authenticate itself with a server, usually after receiving a 401 response. • **Cache-Control**—Directives that must be obeyed by all caching mechanisms along the request/response chain. The directives specify behavior intended to prevent caches from adversely interfering with the request or response. • **Connection**—Allows the sender to specify connection options. • **Content-MD5**—MD5 digest of the entity body that provides an end-to-end integrity check. Only a client or an origin server can generate this header field. • **Expect**—Used by a client to inform the server about the behaviors that the client requires. • **From**—Contains the e-mail address of the person that controls the requesting user agent. • **Host**—Internet host and port number of the resource being requested, as obtained from the original URI given by the user or referring resource. The Host field value must represent the naming authority of the origin server or gateway given by the original URL. • **If-Match**—Used with a method to make it conditional. A client that has one or more entities previously obtained from the resource can verify that one of those entities is current by including a list of their associated entity tags in the If-Match header field. This feature allows efficient updates of cached information with a minimum amount of transaction overhead. It is also used on updating requests to prevent inadvertent modification of the wrong version of a resource. As a special case, the value "*" matches any current entity of the resource.

	• **length** —See the **(config-pmap-ins-http) match header length** command for details. • **mime-type**—See the **(config-pmap-ins-http) match header mime-type** command for details. • **Pragma**—Pragma directives that are understood by servers to whom the directives are relevant. The syntax is the same as for other multiple-value fields in HTTP. For example, the accept field is a comma-separated list of entries for which the optional parameters are separated by semicolons. • **Referer**—Address (URI) of the resource from which the URI in the request was obtained. • **Transfer-Encoding**—Indicates what (if any) type of transformation has been applied to the message body in order to safely transfer it between the sender and the recipient. • **User-Agent**—Information about the user agent (for example, a software program that originates the request). This information is for statistical purposes, the tracing of protocol violations, and automated recognition of user agents. • **Via**—Used by gateways and proxies to indicate the intermediate protocols and recipients between the user agent and the server on requests and between the origin server and the client on responses.
header-value *expression*	Specifies the header value expression string to compare against the value in the specified field in the HTTP header. The range is from 1 to 255 alphanumeric characters. For a list of supported characters that you can use in regular expressions, see the "Usage Guidelines" section for the **(config-pmap-ins-http) match content** command.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map inspection HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When you use the **match header** command, you access the policy map inspection HTTP match configuration mode and the prompt changes from (config-pmap-ins-http) to (config-pmap-ins-http-m). You can then specify the actions that the ACE should take when network traffic matches the specified inline **match** command. For information about commands in this mode, see the "Policy Map Inspection HTTP Match Configuration Mode Commands" section.

The ACE supports the use of regular expressions for matching. Expressions are stored in a header map in the form *header-name: expression*. Header expressions allow spaces, if the spaces are escaped or quoted. For a list of supported characters that you can use in regular expressions, see the "Usage Guidelines" section for the **(config-pmap-ins-http) match content** command.

Examples

To filter on the content and allow HTTL headers that contain the expression *html*, enter:

```
host1/Admin(config)# policy-map type inspect http all-match HTTP_INSPECT_L7POLICY
host1/Admin(config-pmap-ins-http)# match MATCH4 header accept header-value html
host1/Admin(config-pmap-ins-http-m)
```

Related Commands

This command has no related commands.

(config-pmap-ins-http) match header length

To limit the HTTP traffic allowed through the ACE based on the length of the entity body in the HTTP message, use the **match header length** command. Messages will be either allowed or denied based on the Layer 7 HTTP deep packet inspection policy map action. Use the **no** form of this command to clear an HTTP header length match criteria from the policy map.

match *name* **header length** {**request** | **response**} {**eq** *bytes* | **gt** *bytes* | **lt** *bytes* | **range** *bytes1 bytes 2*} [**insert-before** *map_name*]

no match *name*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
request	Specifies the size of the HTTP header request message that can be received by the ACE.
response	Specifies the size of the HTTP header response message sent by the ACE.
eq *bytes*	Specifies a value for the entity body in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with an entity body size equal to the specified value. Valid entries are from 1 to 65535 bytes.
gt *bytes*	Specifies a minimum value for the entity body in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with an entity body size greater than the specified value. Valid entries are from 1 to 65535 bytes.

lt *bytes*	Specifies a maximum value for the entity body in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with an entity body size less than the specified value. Valid entries are from 1 to 65535 bytes.
range *bytes1 bytes 2*	Specifies a size range for the entity body in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with a entity body size within this range. The range is from 1 to 65535 bytes.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map inspection HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When you use the **match header length** command, you access the policy map inspection HTTP match configuration mode and the prompt changes from (config-pmap-ins-http) to (config-pmap-ins-http-m). You can then specify the actions that the ACE should take when network traffic matches the specified inline **match** command.

By default, the maximum header length for HTTP deep packet inspection is 2048 bytes. For information about commands in this mode, see the "Policy Map Inspection HTTP Match Configuration Mode Commands" section.

Examples

To specify that the policy map match on HTTP traffic received with a length less than or equal to 3600 bytes in the entity body of the HTTP message, enter:

```
host1/Admin(config)# policy-map type inspect http all-match HTTP_INSPECT_L7POLICY
host1/Admin(config-pmap-http-insp)# match MATCH4 header length request eq 3600
host1/Admin(config-pmap-ins-http-m)
```

Related Commands

This command has no related commands.

(config-pmap-ins-http) match header mime-type

To specify a subset of the MIME-type messages that the ACE permits or denies based on the actions in the policy map, use the **match header mime-type** command. Use the **no** form of this command to deselect the specified Multipurpose Internet Mail Extension (MIME) message match criteria from the policy map.

match *name* **header mime-type** *mime_type* [**insert-before** *map_name*]

no match *name*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
mime_type	MIME type. The ACE includes a predefined list of MIME types, such as image\Jpeg, text\html, application\msword, or audio\mpeg. Choose whether only the MIME types included in this list are permitted through the ACE firewall or whether all MIME types are acceptable. The default behavior is to allow all MIME types. The supported MIME types are as follows: • **application\msexcel** • **application\mspowerpoint** • **application\msword** • **application\octet-stream** • **application\pdf** • **application\postscript** • **application\x-gzip** • **application\x-java-archive** • **application\x-java-vm** • **application\x-messenger** • **application\zip** • **audio*** • **audio\basic** • **audio\midi** • **audio\mpeg** • **audio\x-adpcm** • **audio\x-aiff** • **audio\x-ogg** • **audio\x-wav image *** • **image\gifimage\jpeg** • **image\png**

	• **image\tiff** • **image\x-3ds** • **image\x-bitmap** • **image\x-niff** • **image\x-portable-bitmap** • **image\x-portable-greymap** • **image\x-xpm** • **text*** • **text\css** • **text\html** • **text\plain** • **text\richtext** • **text\sgml** • **text\xmcd** • **text\xml** • **video*** • **video\flc** • **video\mpeg** • **video\quicktime** • **video\sgi** • **video\x-fli**
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map inspection HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When you use the **match header mime-type** command, you access the policy map inspection HTTP match configuration mode and the prompt changes from (config-pmap-ins-http) to (config-pmap-ins-http-m). You can then specify the actions that the ACE should take when network traffic matches the specified inline **match** command. For information about commands in this mode, see the "Policy Map Inspection HTTP Match Configuration Mode Commands" section.

MIME-type validation extends the format of Internet mail to allow non-US-ASCII textual messages, nontextual messages, multipart message bodies, and non-US-ASCII information in message headers.

Examples To specify that the policy map permits MIME-type audio/midi messages through the ACE, enter:

```
(config)# policy-map type inspect http all-match HTTP_INSPECT_L7POLICY
host1/Admin(config-pmap-ins-http)# match MATCH5 header mime-type audio\midi
host1/Admin(config-pmap-ins-http-m)#
```

Related Commands This command has no related commands.

(config-pmap-ins-http) match port-misuse

To define HTTP deep packet inspection compliance decisions that restrict certain HTTP traffic from passing through the ACE, use the **match port-misuse** command. Use the **no** form of this command to clear the HTTP restricted application category match criteria from the policy map.

match *name* **port-misuse** {**im** | **p2p** | **tunneling**} [**insert-before** *map_name*]

no match *name*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
im	Defines the instant messaging application category. The ACE checks for the Yahoo Messenger instant messaging application.
p2p	Defines the peer-to-peer application category. The applications checked include Kazaa, GoToMyPC, and Gnutella.
tunneling	Defines the tunneling application category. The applications checked include HTTPort/HTTHost, GNU httptunnel, and FireThru.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes Policy map inspection HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines The policy map detects the misuse of port 80 (or any other port running HTTP) for tunneling protocols such as peer-to-peer (p2p) applications, tunneling applications, and instant messaging.

When you use the **match port-misuse** command, you access the policy map inspection HTTP match configuration mode and the prompt changes from (config-pmap-ins-http) to (config-pmap-ins-http-m). You can then specify the actions that the ACE should take when network traffic matches the specified inline **match** command. For information about commands in this mode, see the "Policy Map Inspection HTTP Match Configuration Mode Commands" section.

The port misuse application inspection process searches the entity body of the HTTP message, which may degrade performance of the ACE.

The ACE disables the **match port-misuse** command by default. If you do not configure a restricted HTTP application category, the default action by the ACE is to allow the applications without generating a log.

Examples

To specify that the policy map identifies peer-to-peer applications as restricted HTTP traffic, enter:

```
(config)# policy-map type inspect http all-match HTTP_INSPECT_L7POLICY
host1/Admin(config-pmap-ins-http)# match MATCH6 port-misuse p2p
host1/Admin(config-pmap-ins-http-m)#
```

Related Commands

This command has no related commands.

(config-pmap-ins-http) match request-method

To define HTTP deep packet inspection compliance decisions based on the request methods defined in RFC 2616 and by HTTP extension methods, use the **match request-method** command. If the HTTP request method or extension method compliance checks fails, the ACE denies or resets the specified HTTP traffic based on the policy map action. Use the **no** form of this command to clear the HTTP request method match criteria from the policy map.

match *name* **request-method** {**ext** *method* | **rfc** *method*} [**insert-before** *map_name*]

no match *name*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
ext *method*	Specifies an HTTP extension method. If the RFC request messages does not contain one of the RFC 2616 HTTP request methods, the ACE verifies if it is an extension method. The ACE supports the inspection of the following HTTP request extension methods: **bcopy**, **bdelete**, **bmove**, **bpropfind**, **bproppatch**, **copy**, **edit**, **getattr**, **getattrname**, **getprops**, **index**, **lock**, **mkcol**, **mkdir**, **move**, **propfind**, **proppatch**, **revadd**, **revlabel**, **revlog**, **revnum**, **save**, **search**, **setattr**, **startrev**, **stoprev**, **unedit**, and **unlock**.

rfc *method*	Specifies an RFC 2616 HTTP request method that you want to perform an RFC compliance check. The ACE supports the inspection of the following RFC 2616 HTTP request methods: **connect**, **delete**, **get**, **head**, **options**, **post**, **put**, and **trace**.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map inspection HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When you use the **match request-method** command, you access the policy map inspection HTTP match configuration mode and the prompt changes from (config-pmap-ins-http) to (config-pmap-ins-http-m). You can then specify the actions that the ACE should take when network traffic matches the specified inline **match** command. For information about commands in this mode, see the "Policy Map Inspection HTTP Match Configuration Mode Commands" section.

For unsupported HTTP request methods, include the **inspect http strict** command as an action in the Layer 3 and Layer 4 policy map (see **(config-pmap-c) inspect** command).

The ACE disables the **match request-method** command by default. If you do not configure a request method, the default action by the ACE is to allow the RFC 2616 HTTP request method without generating a log. By default, the ACE allows all request and extension methods.

Examples

To specify that the policy map identifies the **index** HTTP RFC 2616 protocol for application inspection, enter:

```
(config)# policy-map type inspect http all-match HTTP_INSPECT_L7POLICY
host1/Admin(config-pmap-ins-http)# match MATCH7 request-method ext index
host1/Admin(config-pmap-ins-http-m)#
```

Related Commands

This command has no related commands.

(config-pmap-ins-http) match strict-http

To ensure that the internal compliance checks verify message compliance with the HTTP RFC standard, RFC 2616, use the **match strict-http** command. If the HTTP message is not compliant, the ACE denies or resets the specified HTTP traffic based on the policy map action. Use the **no** form of this command to clear the HTTP RFC standard, RFC 2616, match criteria from the policy map.

match *name* **strict-http** [**insert-before** *map_name*]

no match *name*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map inspection HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

When you use the **match strict-http** command, you access the policy map inspection HTTP match configuration mode and the prompt changes from (config-pmap-ins-http) to (config-pmap-ins-http-m). You can then specify the actions that the ACE should take when network traffic matches the specified inline **match** command. For information about commands in this mode, see the "Policy Map Inspection HTTP Match Configuration Mode Commands" section.

To configure the policy map to ensure that the internal compliance checks verify message compliance with the HTTP RFC standard, RFC 2616, enter:

```
(config)# policy-map type inspect http all-match HTTP_INSPECT_L7POLICY
host1/Admin(config-pmap-ins-http)# match MATCH8 strict-http
host1/Admin(config-pmap-ins-http-m)#
```

Related Commands

This command has no related commands.

(config-pmap-ins-http) match transfer-encoding

To define HTTP deep packet inspection decisions that limit the HTTP transfer-encoding types that can pass through the ACE, use the **match transfer-encoding** command. Use the **no** form of this command to clear the HTTP transfer-encoding type match criteria from the policy map.

match *name* **transfer-encoding** *coding_types* [**insert-before** *map_name*]

no match *name*

Syntax Descriptionh

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
transfer-encoding *coding_types*	Specifies the HTTP transfer-encoding type for the class map. The possible values for *coding_types* are as follows: • **chunked**—Message body transferred as a series of chunks. • **compress**—Encoding format produced by the common UNIX file compression program "compress." This format is an adaptive Lempel-Ziv-Welch coding (LZW). • **deflate**—.zlib format defined in RFC 1950 with the deflate compression mechanism described in RFC 1951. • **gzip**—Encoding format produced by the file compression program gzip (GNU zip) as described in RFC 1952. This format is a Lempel-Ziv coding (LZ77) with a 32-bit CRC. • **identity**—Default (identity) encoding, which does not require the use of transformation.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Policy map inspection HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When you use the **match transfer-encoding** command, you access the policy map inspection HTTP match configuration mode and the prompt changes from (config-pmap-ins-http) to (config-pmap-ins-http-m). You can then specify the actions that the ACE should take when network traffic matches the specified inline **match** command. For information about commands in this mode, see the "Policy Map Inspection HTTP Match Configuration Mode Commands" section.

The transfer-encoding general-header field indicates the type of transformation, if any, that has been applied to the HTTP message body to safely transfer it between the sender and the recipient. When an HTTP request message contains the configured transfer-encoding type, the ACE performs the configured action in the policy map.

Each **match transfer-encoding** command configures a single application type.

The ACE disables the **match transfer-encoding** command by default.

Examples

To configure the policy map to specify a chunked HTTP transfer encoding type to limit the HTTP traffic that flows through the ACE, enter:

```
(config)# policy-map type inspect http all-match HTTP_INSPECT_L7POLICY
host1/Admin(config-pmap-ins-http)# match MATCH9 transfer-encoding chunked
host1/Admin(config-pmap-ins-http-m)#
```

Related Commands

This command has no related commands.

(config-pmap-ins-http) match url

To define HTTP deep packet inspection decisions based on the URL name and, optionally, the HTTP method, use the **match url** command. HTTP performs regular expression matching against the received packet data from a particular connection based on the URL expression. Use the **no** form of this command to remove the URL name match criteria from the policy map.

match *name* **url** *expression* [**insert-before** *map_name*]

no match *name*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
expression	URL, or portion of a URL, to match. The URL string range is from 1 to 256 characters. Include only the portion of the URL that follows www.hostname.domain in the match statement.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map inspection HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When you use the **match url** command, you access the policy map inspection HTTP match configuration mode and the prompt changes from (config-pmap-ins-http) to (config-pmap-ins-http-m). You can then specify the actions that the ACE should take when network traffic matches the specified inline **match** command. For information about commands in this mode, see the "Policy Map Inspection HTTP Match Configuration Mode Commands" section.

Include only the portion of the URL that follows www.hostname.domain in the match statement. For example, in the URL www.anydomain.com/latest/whatsnew.html, include only /latest/whatsnew.html. To match the www.anydomain.com portion, the URL string can take the form of a URL regular expression. The ACE supports the use of regular expressions for matching. For a list of the supported characters that you can use in regular expressions, see the "Usage Guidelines" section for the **(config-pmap-ins-http) match content** command.

The period (.) does not have a literal meaning in regular expressions. Use either brackets ([]) or the backslash (\) character to match this symbol. For example, specify www[.]xyz[.]com instead of www.xyz.com.

Examples

To configure the policy map to define application inspection decisions based on a URL, enter

```
(config)# policy-map type inspect http all-match HTTP_INSPECT_L7POLICY
host1/Admin(config-pmap-ins-http)# match MATCH_URL url whatsnew/latest.*
host1/Admin(config-pmap-ins-http-m)#
```

Related Commands

This command has no related commands.

(config-pmap-ins-http) match url length

To limit the HTTP traffic allowed through the ACE by specifying the maximum length of a URL in a request message that can be received by the ACE, use the **match url length** command. Messages will be either allowed or denied based on the Layer 7 HTTP deep packet inspection policy map action. Use the **no** form of this command to clear a URL length match criteria from the policy map.

match *name* **url length** {**eq** *bytes* | **gt** *bytes* | **lt** *bytes* | **range** *bytes1 bytes 2*} [**insert-before** *map_name*]

no match *name*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
eq *bytes*	Specifies a value for the HTTP URL length received by the ACE. Based on the policy map action, the ACE allows or denies messages with an HTTP URL length equal to the specified value. Valid entries are from 1 to 65535 bytes.
gt *bytes*	Specifies a minimum value for the HTTP URL length received by the ACE. Based on the policy map action, the ACE allows or denies messages with an HTTP URL length greater than the specified value. Valid entries are from 1 to 65535 bytes.
lt *bytes*	Specifies a maximum value for the HTTP URL length received by the ACE. Based on the policy map action, the ACE allows or denies messages with an HTTP URL length less than the specified value. Valid entries are from 1 to 65535 bytes.
range *bytes1 bytes*	Specifies a size range for the HTTP URL length received by the ACE. Based on the policy map action, the ACE allows or denies messages with an HTTP URL length within this range. The range is from 1 to 65535 bytes.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map inspection HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When you use the **match url length** command, you access the policy map inspection HTTP match configuration mode and the prompt changes from (config-pmap-ins-http) to (config-pmap-ins-http-m). You can then specify the actions that the ACE should take when network traffic matches the specified inline **match** command. For information about commands in this mode, see the "Policy Map Inspection HTTP Match Configuration Mode Commands" section.

Examples

To specify that the policy map is to match on a URL with a length less than or equal to 10,000 bytes in the request message, enter:

```
(config)# policy-map type inspect http all-match HTTP_INSPECT_L7POLICY
host1/Admin(config-pmap-ins-http)# match MATCH10 url length eq 10000
host1/Admin(config-pmap-ins-http-m)#
```

Related Commands

This command has no related commands.

Policy Map Inspection HTTP Class Configuration Mode Commands

Policy map inspection HTTP class configuration mode commands allow you to specify the actions that the ACE should take when network traffic matches one or more match statements in the associated Layer 7 HTTP deep packet inspection class map. To access policy map inspection HTTP class configuration mode, use the **class** command in policy map inspection HTTP configuration mode (see the **(config-pmap-ins-http) class** command for details). The prompt changes from (config-pmap-ins-http) to (config-pmap-ins-http-c).

The default of the ACE is to permit HTTP traffic. For example, if a policy map explicitly permits the HTTP GET method, other methods such as PUT will also be permitted. Only an explicit deny through the **reset** command is capable of dropping traffic.

The commands in this mode require the inspect feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

(config-pmap-ins-http-c) permit

To allow the specified HTTP traffic to be received by the ACE if it passes the HTTP deep packet inspection match criteria specified in the class map, use the **permit** command. Use the **no** form of this command to disallow the specified HTTP traffic to be received by the ACE.

permit [**log**]

no permit

Syntax Description

log	(Optional) Generates a log message for traffic that matches the class map.

Command Modes

Policy map inspection HTTP class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

By default, HTTP inspection allows traffic that does not match any of the configured Layer 7 HTTP deep packet inspection matches. You can modify this behavior by including the **class class-default** command with the **reset** action to deny the specified Layer 7 HTTP traffic. In this case, if none of the class matches configured in the Layer 7 HTTP deep packet inspection policy map are hit, the **class-default** action will be taken by the ACE. For example, you can include a class map to allow the HTTP GET method and use the **class class-default** command to block all of the other requests.

Note By default, all matches are applied to both HTTP request and response messages, but the **class class-default** command is applied only to HTTP requests.

Examples

To allow the specified HTTP traffic to be received by the ACE if the class map match criteria in class map L7HTTP_CHECK are met, enter:

```
host1/Admin(config)# policy-map type inspect http all-match HTTP_DEEPINSPECT_L7POLICY
host1/Admin(config-pmap-ins-http)# class L7HTTP_CHECK
host1/Admin(config-pmap-ins-http-c)# permit
```

Related Commands

This command has no related commands.

(config-pmap-ins-http-c) reset

To deny the specified HTTP traffic by sending a TCP reset message to the client or server to close the connection, use the **reset** command. Use the **no** form of this command to allow the specified HTTP traffic to be received by the ACE.

reset [**log**]

no reset

Syntax Description

log	(Optional) Generates a log message for traffic that matches the class map.

Command Modes

Policy map inspection HTTP class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To deny the specified HTTP traffic to be received by the ACE if the class map match criteria in class map L7HTTP_CHECK are met, enter:

```
host1/Admin(config)# policy-map type inspect http all-match HTTP_DEEPINSPECT_L7POLICY
host1/Admin(config-pmap-ins-http)# class http_check
host1/Admin(config-pmap-ins-http-c)# reset
```

Related Commands

This command has no related commands.

Policy Map Inspection HTTP Match Configuration Mode Commands

Policy map inspection HTTP match configuration mode commands allow you to specify the actions that the ACE should take when network traffic matches the specified inline **match** command. To access policy map inspection HTTP match configuration mode, use one of the **match** commands in policy map inspection HTTP configuration mode (see the "Policy Map Inspection HTTP Configuration Mode Commands" section for command details). The prompt changes from (config-pmap-ins-http) to (config-pmap-ins-http-m).

The inline Layer 7 policy map **match** commands allow you to include a single inline match criteria in the policy map without specifying a traffic class. The **match** commands function the same as with the Layer 7 class map **match** commands. However, when you use an inline **match** command, you can specify an action for only a single **match** command in the Layer 7 policy map.

The default of the ACE is to permit HTTP traffic. For example, if a policy map explicitly permits the HTTP GET method, other methods such as PUT will also be permitted. Only an explicit deny through the **reset** command is capable of dropping traffic.

The commands in this mode requires the inspect feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

(config-pmap-ins-http-m) permit

To allow the specified HTTP traffic to be received by the ACE if it passes inspection of the match criteria in an inline match condition, use the **permit** command. Use the **no** form of this command to disallow the specified HTTP traffic to be received by the ACE.

permit [**log**]

no permit

Syntax Description

log	(Optional) Generates a log message for traffic that matches the inline **match** command.

Command Modes

Policy map inspection HTTP match configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The default of the ACE is to permit HTTP traffic. For example, if a policy map explicitly permits the HTTP GET method, other methods such as PUT will also be permitted. Only an explicit deny through the **reset** command is capable of dropping traffic.

Examples

To allow the specified HTTP traffic to be received by the ACE if the match criteria are met, enter:

```
host1/Admin(config)# policy-map type inspect http all-match HTTP_DEEPINSPECT_L7POLICY
host1/Admin(config-pmap-ins-http)# match MATCH5 transfer-encoding chunked
host1/Admin(config-pmap-ins-http-m)# permit
```

Related Commands

This command has no related commands.

(config-pmap-ins-http-m) reset

To deny the specified HTTP traffic by sending a TCP reset message to the client or server to close the connection, use the **reset** command. Use the **no** form of this command to allow the specified HTTP traffic to be received by the ACE.

reset [**log**]

no reset

Syntax Description

log	(Optional) Generates a log message for traffic that matches the inline **match** command.

Command Modes

Policy map inspection HTTP match configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To deny the specified HTTP traffic to be received by the ACE if the match criteria are met, enter:

```
host1/Admin(config)# policy-map type inspect http all-match HTTP_DEEPINSPECT_L7POLICY
host1/Admin(config-pmap-ins-http)# match MATCH5 transfer-encoding chunked
host1/Admin(config-pmap-ins-http-m)# reset
```

Related Commands

This command has no related commands.

Policy Map Inspection SIP Configuration Mode Commands

Policy map inspection SIP configuration mode commands allow you to define a policy map that initiates the inspection of the SIP protocol packets by the ACE. The ACE attempts to match all specified conditions against the matching classification and executes the actions of all matching classes until it encounters a deny for a match request.

To create a SIP policy map and access policy map inspection SIP configuration mode, use the **policy-map type inspect sip all-match** command in configuration mode. When you access the policy map inspection SIP configuration mode, the prompt changes to (config-pmap-ins-sip). Use the **no** form of this command to remove a SIP inspection policy map from the ACE.

policy-map type inspect sip all-match *map_name*

no policy-map type inspect sip all-match *map_name*

Syntax Description

sip all-match	Specifies the policy map that initiates the inspection of the SIP protocol packets by the ACE. The ACE attempts to match all specified conditions against the matching classification and executes the actions of all matching classes until it encounters a deny for a match request.
map_name	Name assigned to the Layer 7 SIP inspection policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The commands in this mode require the inspect feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The Layer 7 policy map configures the applicable SIP inspection actions executed on the network traffic that match the classifications defined in a class map. You then associate the completed Layer 7 SIP inspection policy with a Layer 3 and Layer 4 policy map to activate the operation on a VLAN interface.

Examples

To create a Layer 7 SIP inspection policy map, enter:

```
host1/Admin(config)# policy-map type inspect sip all-match SIP_INSPECT_L7POLICY
host1/Admin(config-pmap-ins-sip)#
```

To remove the SIP inspection policy map from the configuration, enter:

```
host1/Admin(config)# no policy-map type inspect sip all-match SIP_INSPECT_L7POLICY
```

Related Commands

show startup-config

(config-pmap-ins-sip) class

To associate a Layer 7 SIP inspection class map with a Layer 7 SIP inspection policy map, use the **class** command. The prompt changes from (config-pmap-sip-ins) to (config-pmap-sip-ins-c). Use the **no** form of this command to remove an associated class map from a policy map.

class *map_name* [**insert-before** *map_name*]

no class *map_name*

Syntax Description

map_name	Name of a previously defined Layer 7 SIP inspection class map configured with the **class-map** command. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
insert-before *map_name*	(Optional) Places the class map ahead of an existing class map in the policy map configuration.

Command Modes

Policy map inspection SIP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To associate a Layer 7 SIP inspection class map with a Layer 7 SIP inspection policy map, enter:

```
host/Admin(config-pmap-ins-sip)# class SIP_INSPECT_L7CLASS
host/Admin(config-pmap-ins-sip-c)#
```

To disassociate the class map from the policy map, enter:

```
host/Admin(config-pmap-ins-sip)# no class SIP_INSPECT_L7CLASS
```

Related Commands

(config-pmap-ins-sip) description
(config-pmap-ins-sip-c) drop
(config-pmap-ins-sip-c) log
(config-pmap-ins-sip-c) permit
(config-pmap-ins-sip-c) reset

(config-pmap-ins-sip) description

To provide a brief summary about the Layer 7 SIP inspection policy map, use the **description** command. Use the **no** form of this command to remove the description from the policy map.

description *text*

no description

Syntax Description

text	Description for the policy map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Policy map inspection SIP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description for a Layer 7 SIP inspection policy map, enter:

```
host1/Admin(config-pmap-ins-sip)# description layer 7 sip inspection policy
```

To remove the description from the policy map, enter:

```
host1/Admin(config-pmap-ins-sip)# no description
```

Related Commands

(config-pmap-ins-sip) class

(config-pmap-ins-sip) match called-party

To filter SIP traffic based on the called party, use the **match called-party** command. Use the **no** form of this command to remove the match statement from the policy map.

match *name* **called-party** *expression* [**insert-before** *map_name*]

no match *name* **called-party** *expression*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
expression	Called party in the URI of the SIP To header. Enter a regular expression from 1 to 255 alphanumeric characters.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map inspection SIP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

You can filter SIP traffic based on the called party (callee or destination) as specified in the URI of the SIP To header. The ACE does not include the display name or tag part of the field.

The ACE supports the use of regular expressions for matching. Expressions are stored in a header map in the form *header-name: expression*. Header expressions allow spaces if the spaces are escaped or quoted. Table 2-16 lists the supported characters that you can use in regular expressions.

Examples

To identify the called party in the SIP To header, enter:

```
host1/Admin(config-pmap-ins-sip)# match MATCH_CALLED called-party
sip:some-user@somenetwork.com
```

To remove the match statement from the policy map, enter:

```
host1/Admin(config-pmap-ins-sip)# no match MATCH_CALLED called-party
sip:some-user@somenetwork.com
```

Related Commands

(config-pmap-ins-sip) match calling-party
(config-pmap-ins-sip) match content
(config-pmap-ins-sip) match im-subscriber
(config-pmap-ins-sip) match message-path
(config-pmap-ins-sip) match request-method
(config-pmap-ins-sip) match third-party registration
(config-pmap-ins-sip) match uri

(config-pmap-ins-sip) match calling-party

To filter SIP traffic based on the calling party, use the **match calling-party** command. Use the **no** form of this command to remove the description from the policy map.

match *name* **calling-party** *expression* [**insert-before** *map_name*]

no match *name* **calling-party** *expression*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
expression	Calling party in the URI of the SIP From header. Enter a regular expression from 1 to 255 alphanumeric characters. The ACE supports the use of regular expressions for matching.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map inspection SIP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

You can filter SIP traffic based on the calling party (caller or source) as specified in the URI of the SIP From header. The ACE does not include the display name or tag part of the field.

The ACE supports the use of regular expressions for matching. Expressions are stored in a header map in the form *header-name: expression*. Header expressions allow spaces if the spaces are escaped or quoted. See Table 2-16 for a list of the supported characters that you can use in regular expressions.

Examples

To identify the calling party in the SIP From header, enter:

```
host1/Admin(config-pmap-ins-sip)# match MATCH_CALLING calling-party
sip:this-user@thisnetwork.com;tag=745g8
```

To remove the match statement from the policy map, enter:

```
host1/Admin(config-pmap-ins-sip)# no match MATCH_CALLING calling-party
sip:this-user@thisnetwork.com;tag=745g8
```

Related Commands

(config-pmap-ins-sip) match called-party
(config-pmap-ins-sip) match content
(config-pmap-ins-sip) match im-subscriber
(config-pmap-ins-sip) match message-path
(config-pmap-ins-sip) match request-method
(config-pmap-ins-sip) match third-party registration
(config-pmap-ins-sip) match uri

(config-pmap-ins-sip) match content

To define SIP content checks, use the **match content** command. Use the **no** form of this command to remove the match statement from the policy map.

match *name* **content** {**length gt** *number*} | {**type sdp** | *expression*} [**insert-before** *map_name*]

no match *name* **content** {**length gt** *number*} | {**type sdp** | *expression*}

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
length	Specifies the SIP message body length.
gt	Specifies the greater than operator.
number	Maximum size of a SIP message body that the ACE allows. Enter an integer from 0 to 65534 bytes. If the message body is greater than the configured value, the ACE performs the action that you configure in the policy map.
type	Specifies a content type check.
sdp	Specifies that the traffic must be of type Session Description Protocol (SDP) to match the policy map.

expression	Regular expression that identifies the content type in the SIP message body that is required to match the policy map. Enter a regular expression from 1 to 255 alphanumeric characters. The ACE supports the use of regular expressions for matching. See Table 2-16 for a list of the supported characters that you can use in regular expressions.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map inspection SIP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

You can configure the ACE to perform SIP content checks based on content length or content type. By default, the ACE allows all content types.

Examples

To configure the ACE to drop SIP packets that have content with a length greater than 4000 bytes in length, enter:

```
host1/Admin(config)# class-map type sip inspect match-all SIP_INSP_CLASS
host1/Admin(config-pmap-ins-sip)# match MATCH_CONTENT content length gt 200

host1/Admin(config)# policy-map type inspect sip all-match SIP_INSP_POLICY
host1/Admin(config-pmap-ins-sip)# class SIP_INSP_CLASS
host1/Admin(config-pmap-ins-sip-c)# deny
```

To remove the match statement from the policy map, enter:

```
host1/Admin(config-cmap-sip-insp)# no match MATCH_CONTENT content length gt 200
```

Related Commands

(config-pmap-ins-sip) match called-party
(config-pmap-ins-sip) match calling-party
(config-pmap-ins-sip) match im-subscriber
(config-pmap-ins-sip) match message-path
(config-pmap-ins-sip) match request-method
(config-pmap-ins-sip) match third-party registration
(config-pmap-ins-sip) match uri

(config-pmap-ins-sip) match im-subscriber

To filter SIP traffic based on the IM subscriber, use the **match im-subscriber** command. Use the **no** form of this command to remove the description from the policy map.

match *name* **im-subscriber** *expression* [**insert-before** *map_name*]

no match *name* **im-subscriber** *expression*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
expression	Calling party. Enter a regular expression from 1 to 255 alphanumeric characters. The ACE supports the use of regular expressions for matching.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map inspection SIP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The ACE supports the use of regular expressions for matching. Expressions are stored in a header map in the form *header-name: expression*. Header expressions allow spaces if the spaces are escaped or quoted. See Table 2-16 for a list of the supported characters that you can use in regular expressions.

Examples

To filter SIP traffic based on the IM subscriber, John Q. Public, enter:

```
host1/Admin(config-pmap-ins-sip)# match MATCH_IM im-subscriber John_Q_Public
```

To remove the match statement from the policy map, enter:

```
host1/Admin(config-pmap-ins-sip)# no match MATCH_IM im-subscriber John_Q_Public
```

Related Commands

(config-pmap-ins-sip) match called-party
(config-pmap-ins-sip) match calling-party
(config-pmap-ins-sip) match content
(config-pmap-ins-sip) match message-path
(config-pmap-ins-sip) match request-method
(config-pmap-ins-sip) match third-party registration
(config-pmap-ins-sip) match uri

(config-pmap-ins-sip) match message-path

To filter SIP traffic based on the message path, use the **match message-path** command. Use the **no** form of this command to remove the match statement from the policy map.

match *name* **message-path** *expression* [**insert-before** *map_name*]

no match *name* **message-path** *expression*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
expression	SIP proxy server. Enter a regular expression from 1 to 255 alphanumeric characters. The ACE supports the use of regular expressions for matching.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map inspection SIP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

SIP inspection allows you to filter messages coming from or transiting through certain SIP proxy servers. The ACE maintains a list of unauthorized SIP proxy IP addresses or URIs in the form of regular expressions and then checks this list against the VIA header field in each SIP packet. The default action is to drop SIP packets with VIA fields that match regex list.

The ACE supports the use of regular expressions for matching. Expressions are stored in a header map in the form *header-name: expression*. Header expressions allow spaces if the spaces are escaped or quoted. See Table 2-16 for a list of the supported characters that you can use in regular expressions.

Examples

To filter SIP traffic based on the message path 192.168.12.3:5060, enter:

```
host1/Admin(config-pmap-ins-sip)# match MATCH_PATH message-path 192.168.12.3:5060
```

To remove the match statement from the policy map, enter:

```
host1/Admin(config-pmap-ins-sip)# no match MATCH_PATH message-path 192.168.12.3:5060
```

Related Commands

(config-pmap-ins-sip) match called-party
(config-pmap-ins-sip) match calling-party
(config-pmap-ins-sip) match content
(config-pmap-ins-sip) match im-subscriber
(config-pmap-ins-sip) match request-method
(config-pmap-ins-sip) match third-party registration
(config-pmap-ins-sip) match uri

(config-pmap-ins-sip) match request-method

To filter SIP traffic based on the request method, use the **match request-method** command. Use the **no** form of this command to remove the description from the policy map.

match *name* **request-method** *method_name* [**insert-before** *map_name*]

no match *name* **request-method** *method_name*

Syntax Description

method_name	Supported SIP method using one of the following keywords: • **ack** • **bye** • **cancel** • **info** • **invite** • **message** • **notify** • **options** • **prack** • **refer** • **register** • **subscribe** • **unknown** • **update** Use the **unknown** keyword to permit or deny unknown or unsupported SIP methods.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map inspection SIP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To filter SIP traffic based on the INVITE request method, enter:

```
host1/Admin(config-pmap-ins-sip)# match MATCH_REQUEST request-method invite
```

To remove the **match** statement from the policy map, enter:

```
host1/Admin(config-pmap-ins-sip)# no match MATCH_REQUEST request-method invite
```

Related Commands

(config-pmap-ins-sip) match called-party
(config-pmap-ins-sip) match calling-party
(config-pmap-ins-sip) match content
(config-pmap-ins-sip) match im-subscriber
(config-pmap-ins-sip) match message-path
(config-pmap-ins-sip) match third-party registration
(config-pmap-ins-sip) match uri

(config-pmap-ins-sip) match third-party registration

To filter SIP traffic based on third-party registrations or deregistrations, use the **match third-party-registration** command. Use the **no** form of this command to remove the match statement from the policy map.

match *name* **third-party registration** *expression* [**insert-before** *map_name*]

no match *name* **third-party registration** *expression*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).

expression	Privileged user that is authorized for third-party registrations. Enter a regular expression from 1 to 255 alphanumeric characters.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map inspection SIP configuration mode

Admin and user context

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

SIP allows users to register other users on their behalf by sending REGISTER messages with different values in the From and To header fields. This process may pose a security threat if the REGISTER message is actually a DEREGISTER message. A malicious user could cause a Denial of Service (DoS) attack by deregistering all users on their behalf. To prevent this security threat, you ACE can specify a list of privileged users who can register or unregister someone else on their behalf. The ACE maintains the list as a regex table. If you configure this policy, the ACE drops REGISTER messages with mismatched From and To headers and a From header value that does not match any of the privileged user IDs.

The ACE supports the use of regular expressions for matching. Expressions are stored in a header map in the form *header-name: expression*. Header expressions allow spaces if the spaces are escaped or quoted. See Table 2-16 for a list of the supported characters that you can use in regular expressions.

Examples

To filter SIP traffic based on SIP registrations or deregistrations, enter:

```
host1/Admin(config-pmap-ins-sip)# match MATCH_REG third-party-registration USER1
```

To remove the **match** statement from the policy map, enter:

```
host1/Admin(config-pmap-ins-sip)# no match MATCH_REG third-party-registration USER1
```

Related Commands

(config-pmap-ins-sip) match called-party
(config-pmap-ins-sip) match calling-party
(config-pmap-ins-sip) match content
(config-pmap-ins-sip) match im-subscriber
(config-pmap-ins-sip) match message-path
(config-pmap-ins-sip) match request-method
(config-pmap-ins-sip) match uri

(config-pmap-ins-sip) match uri

To filter SIP traffic based on URIs, use the **match uri** command. Use the **no** form of this command to remove the match statement from the policy map.

match *name* **uri** {**sip** | **tel**} **length gt** *value* [**insert-before** *map_name*]

no match *name* **uri** {**sip** | **tel**} **length gt** *value*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
sip	Specifies that the ACE validates the length of a SIP URI.
tel	Specifies that the ACE validates the length of a Tel URI.
length	Specifies the length of the SIP or Tel URI.
gt	Specifies the greater than operator.
value	Maximum value for the length of the SIP URI or Tel URI in bytes. Enter an integer from 0 to 254 bytes.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map inspection SIP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

You can configure the ACE to validate the length of SIP URIs or Tel URIs. A SIP URI is a user identifier that a calling party (source) uses to contact the called party (destination). A Tel URI is a telephone number that identifies the endpoint of a SIP connection. For more information about SIP URIs and Tel URIs, see RFC 2534 and RFC 3966, respectively.

Examples

To instruct the ACE to filter traffic based on SIP URIs, enter:

```
host1/Admin(config-pmap-ins-sip)# match MATCH_URI uri sip length gt 100
```

To remove the match statement from the policy map, enter:

```
host1/Admin(config-pmap-ins-sip)# no match MATCH_URI uri sip length gt 100
```

Related Commands

(config-pmap-ins-sip) match called-party
(config-pmap-ins-sip) match calling-party
(config-pmap-ins-sip) match content
(config-pmap-ins-sip) match im-subscriber
(config-pmap-ins-sip) match message-path
(config-pmap-ins-sip) match request-method
(config-pmap-ins-sip) match third-party registration

Policy Map Inspection SIP Class Configuration Mode Commands

Use the policy map SIP inspection class configuration mode to specify the actions that the ACE should take when network traffic matches one or more match statements in the associated Layer 7 SIP inspection class map. To access policy map SIP inspection class configuration mode, use the **class** command in the policy map SIP inspection configuration mode (see the **(config-pmap-ins-sip) class** command for details). The prompt changes from (config-pmap-ins-sip) to (config-pmap-ins-sip-c).

The commands in this mode require the inspect feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

(config-pmap-ins-sip-c) drop

To discard the SIP traffic that matches the traffic specified in the class map, use the **drop** command. Use the **no** form of this command to return the ACE behavior to the default of permitting all SIP traffic to pass.

drop [**log**]

no drop

Syntax Description

log	(Optional) Generates a log message for traffic that matches the class map.

Command Modes

Policy map inspection SIP class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To discard the SIP traffic that matches the class map, enter:

```
host1/Admin(config)# policy-map type inspect sip first-match SIP_INSPECT_L7POLICY
host1/Admin(config-pmap-ins-sip)# class SIP_INSPECT_L7CLASS
host1/Admin(config-pmap-ins-sip-c)# drop
```

Related Commands

This command has no related commands.

(config-pmap-ins-sip-c) log

To log all SIP traffic that matches the class map, use the **log** command. Use the **no** form of this command to return the ACE behavior to the default of not logging SIP traffic.

log

no log

Syntax Description

This command has no keywords or arguments.

Command Modes Policy map inspection SIP class configuration mode

Admin and user contexts

Command History	Release	Modification
	A3(1.0)	This command was introduced.

Usage Guidelines This command has no usage guidelines.

Examples To log the SIP traffic that matches the class map, enter:

```
host1/Admin(config)# policy-map type inspect sip first-match SIP_INSPECT_L7POLICY
host1/Admin(config-pmap-ins-sip)# class SIP_INSPECT_L7CLASS
host1/Admin(config-pmap-ins-sip-c)# log
```

Related Commands This command has no related commands.

(config-pmap-ins-sip-c) permit

To permit the SIP traffic that matches the class map to pass through the ACE, use the **permit** command. Use the **no** form of this command to return the ACE behavior to the default of permitting all SIP traffic to pass.

permit [**log**]

no permit

Syntax Description		
	log	(Optional) Generates a log message for traffic that matches the class map.

Command Modes Policy map inspection SIP class configuration mode

Admin and user contexts

Command History	Release	Modification
	A3(1.0)	This command was introduced.

Usage Guidelines This command has no usage guidelines.

Examples To permit the SIP traffic that matches the class map to pass through the ACE, enter:

```
host1/Admin(config)# policy-map type inspect sip first-match SIP_INSPECT_L7POLICY
host1/Admin(config-pmap-ins-sip)# class SIP_INSPECT_L7CLASS
host1/Admin(config-pmap-ins-sip-c)# permit
```

Related Commands This command has no related commands.

(config-pmap-ins-sip-c) reset

To instruct the ACE to deny the SIP traffic that matches the class map and to reset the connection using the TCP RESET message, use the **reset** command. Use the **no** form of this command to return the ACE behavior to the default of permitting all SIP traffic to pass.

reset [**log**]

no reset

Syntax Description

log	(Optional) Generates a log message for traffic that matches the class map.

Command Modes Policy map inspection SIP class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines This command has no usage guidelines.

Examples To instruct the ACE to deny the traffic that matches the class map and to reset the connection, enter:

```
host1/Admin(config)# policy-map type inspect sip first-match SIP_INSPECT_L7POLICY
host1/Admin(config-pmap-ins-sip)# class SIP_INSPECT_L7CLASS
host1/Admin(config-pmap-ins-sip-c)# reset
```

Related Commands This command has no related commands.

Policy Map Inspection SIP Match Configuration Mode Commands

Policy map inspection SIP match configuration mode commands allow you to specify the actions that the ACE should take when network traffic matches the specified inline match command. To access policy map inspection SIP match configuration mode, use the **match** command in policy map inspection SIP configuration mode. The prompt changes from (config-pmap-ins-sip) to (config-pmap-ins-sip-m).

The inline Layer 7 policy map **match** commands allow you to include a single inline match criteria in the policy map without specifying a traffic class. The **match** commands function the same as with the Layer 7 class map **match** commands. However, when you use an inline **match** command, you can specify an action for only a single **match** command in the Layer 7 policy map.

The commands in this mode require the inspect feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

(config-pmap-ins-sip-m) drop

To discard the SIP traffic that matches the traffic specified in the single inline **match** command, use the **drop** command. Use the **no** form of this command to return the ACE behavior to the default of permitting all SIP traffic to pass.

drop [**log**]

no drop

Syntax Description

log	(Optional) Generates a log message for traffic that matches the single inline **match** command.

Command Modes

Policy map inspection SIP match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To discard the SIP traffic that matches the traffic specified in the single inline **match** command, enter:

```
host1/Admin(config)# policy-map type inspect sip all-match SIP_INSPECT_L7POLICY
host1/Admin(config-pmap-ins-sip)# match MATCH_URI uri sip length gt 100
host1/Admin(config-pmap-ins-sip-m)# drop
```

Related Commands

This command has no related commands.

(config-pmap-ins-sip-m) permit

To permit the SIP traffic that matches the traffic specified in the single inline **match** command to pass through the ACE, use the **permit** command. Use the **no** form of this command to return to the default state and permit all SIP traffic to pass.

permit [**log**]

no permit

Syntax Description

log	(Optional) Generates a log message for traffic that matches the inline **match** command.

Command Modes

Policy map inspection SIP match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To permit the SIP traffic specified in the single inline **match** command to pass through the ACE, enter:

```
host1/Admin(config)# policy-map type inspect sip all-match SIP_INSPECT_L7POLICY
host1/Admin(config-pmap-ins-sip)# match MATCH_URI uri sip length gt 100
host1/Admin(config-pmap-ins-sip-m)# permit
```

Related Commands

This command has no related commands.

(config-pmap-ins-sip-m) reset

To instruct the ACE to deny SIP traffic that matches the single inline **match** command and to reset the connection using the TCP RESET message, use the **reset** command. Use the **no** form of this command to return the ACE behavior to the default of permitting all SIP traffic to pass.

reset [**log**]

no reset

Syntax Description

log	(Optional) Generates a log message for traffic that matches the single inline **match** command.

Command Modes

Policy map inspection SIP match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to deny the traffic that matches the single inline **match** command and to reset the connection, enter:

```
host1/Admin(config)# policy-map type inspect sip all-match SIP_INSPECT_L7POLICY
host1/Admin(config-pmap-ins-sip)# match MATCH_URI uri sip length gt 100
host1/Admin(config-pmap-ins-sip-m)# reset
```

Related Commands

This command has no related commands.

Policy Map Inspection Skinny Configuration Mode Commands

Policy map inspection Skinny configuration mode commands allow you to define a policy map that initiates inspection of the Skinny Client Control Protocol (SCCP) by the ACE. The ACE uses the SCCP inspection policy to filter traffic based on the message ID and to perform user-configurable actions on that traffic.

To create an SCCP inspection policy map and access policy map inspection Skinny configuration mode, use the **policy-map type inspect skinny** command in configuration mode. When you access the policy map inspection skinny configuration mode, the prompt changes to (config-pmap-ins-skinny). Use the **no** form of this command to remove an SCCP inspection policy map from the ACE.

policy-map type inspect skinnny *map_name*

no policy-map type inspect skinny *map_name*

Syntax Description

map_name	Name assigned to the Layer 7 SCCP inspection policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The commands in this mode require the inspect feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To create a Layer 7 SCCP inspection policy map, enter:

```
host1/Admin(config)# policy-map type inspect skinny SCCP_INSPECT_L7POLICY
host1/Admin(config-pmap-ins-skinny)#
```

Related Commands

This command has no related commands.

(config-pmap-ins-skinny) description

To provide a brief summary about the Layer 7 SCCP inspection policy map, use the **description** command. Use the **no** form of this command to remove the description from the class map.

description *text*

no description

Syntax Description

text	Description for the policy map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Policy map inspection Skinny configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description about the SCCP policy map, enter:

```
host1/Admin(config-pmap-ins-skinny)# description this is an SCCP inspection policy map
```

To remove the inline match statement from the policy map, enter:

```
host1/Admin(config-pmap-ins-skinny)# no match SCCP_MATCH message-id range 100 500
```

Related Commands

(config-pmap-ins-skinny-m) reset
(config-pmap-ins-skinny) match message-id

(config-pmap-ins-skinny) match message-id

To include a single inline match criteria in the policy map without specifying a traffic class, use the **match message-id** command. Use the **no** form of this command to remove the inline match statement from the policy map.

match *name* **message-id** {*number1* | **range** {*number2 number3*}} [**insert-before** *name*]

no match *name*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
number1	Numerical identifier of the SCCP message. Enter an integer from 0 to 65535.
range {*number2 number3*}	Specifies a range of SCCP message IDs. Enter an integer from 0 to 65535 for the lower and the upper limits of the range. The upper limit must be greater than or equal to the lower limit.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map inspection skinny configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

When you use an inline **match** command, you can specify an action for only a single match statement in the Layer 7 policy map.

Examples

To specify an inline **match** command for a Layer 7 SCCP inspection policy map, enter:

```
host1/Admin(config-pmap-ins-skinny)# match SCCP_MATCH message-id range 100 500
host1/Admin(config-pmap-ins-skinny-m)#
```

Related Commands

(config-pmap-ins-skinny) description

Policy Map Inspection Skinny Match Configuration Mode Commands

Policy map inspection Skinny match configuration mode commands allow you to specify the actions that the ACE should take when network traffic matches the specified inline **match** command. To access policy map inspection Skinny match configuration mode, use the **match message-id** command in policy map inspection Skinny configuration mode (see the **(config-pmap-ins-skinny) match message-id** command for details). The prompt changes from (config-pmap-ins-skinny) to (config-pmap-ins-skinny-m).

The inline Layer 7 policy map **match** commands allow you to include a single inline match criteria in the policy map without specifying a traffic class. The **match** commands function the same as with the Layer 7 class map **match** commands. However, when you use an inline **match** command, you can specify an action for only a single **match** command in the Layer 7 policy map.

The commands in this mode require the inspect feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

(config-pmap-ins-skinny-m) reset

To instruct the ACE to deny SCCP traffic that matches the single inline **match** command and to reset the connection using the TCP RESET message, use the **reset** command as the policy map action. By default, the ACE allows all SCCP packets to pass through it. Use the **no** form of this command to reset the ACE behavior to the default of allowing all SCCP traffic to pass.

reset [log]

no reset

Syntax Description

log	(Optional) Generates a log message for traffic that matches the single inline **match** command.

Command Modes

Policy map inspection Skinny match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

You apply the specified action against the single inline **match** command. The **reset** command causes the ACE to drop the SCCP traffic that matches the inline **match** command and reset the connection.

Examples

To specify that the ACE drop SCCP traffic that matches the **match message-id** inline command, enter:

```
host1/Admin(config)# policy-map type inspect sccp SCCP_INSPECT_L7POLICY
host1/Admin(config-pmap-ins-skinny)# match SCCP_MATCH message-id range 100 500
host1/Admin(config-pmap-ins-skinny-m)# reset
```

Related Commands

(config-pmap-ins-skinny) description
(config-pmap-ins-skinny) match message-id

Policy Map Load Balancing Generic Configuration Mode Commands

Policy map load balancing generic configuration mode commands allow you to specify a generic Layer 7 policy map for server load-balancing decisions. The ACE executes the specified action only against the first matching load-balancing classification.

To create a generic Layer 7 server load balancing (SLB) policy map and access policy map load balancing generic configuration mode, use the **policy-map type loadbalance generic first-match** command. When you access the policy map load balancing generic configuration mode, the prompt changes to (config-pmap-lb-generic). Use the **no** form of this command to remove a generic Layer 7 SLB policy map from the ACE.

policy-map type loadbalance generic first-match *map_name*

no policy-map type loadbalance generic first-match *map_name*

Syntax Description

map_name	Name assigned to the generic SLB policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You associate the Layer 7 load balancing policy map with a Layer 3 and Layer 4 policy map to provide an entry point for the traffic classification. Layer 7 policy maps are considered to be child policies. Only a Layer 3 and Layer 4 policy map can be activated on a VLAN interface. A Layer 7 policy map cannot be directly applied on a VLAN (or any) interface.

To associate the Layer 7 load-balancing policy map, you nest it by using the Layer 3 and Layer 4 **(config-pmap-c) loadbalance policy** command.

Examples

To create a generic SLB policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance generic first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-generic)#
```

Related Commands

show running-config
(config) policy-map

(config-pmap-lb-generic) class

To associate a Layer 7 server load balancing (SLB) class map with a Layer 7 SLB policy map, use the **class** command. The prompt changes from (config-pmap-lb-generic) to (config-pmap-lb-generic-c). For information about commands in this mode, see the "Policy Map Load Balancing Generic Class Configuration Mode Commands" section. Use the **no** form of this command to remove an associated class map from a policy map.

class {*name1* [**insert-before** *name2*] | **class-default**}

no class {*name1* [**insert-before** *name2*] | **class-default**}

Syntax Description

name1	Name of a previously defined Layer 7 SLB class map configured with the **class-map** command. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
insert-before *name2*	(Optional) Places the current named class map ahead of an existing class map or inline match condition specified by the *name2* argument in the policy map configuration. The ACE does not save the sequence reordering as part of the configuration.
class-default	Reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified under the **class class-default** command. The **class-default** class map has an implicit **match any** statement in it that enables it to match all traffic.

Command Modes

Policy map load balancing generic configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To associate a Layer 7 SLB class map with a Layer 7 SLB policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance generic first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-generic)# class L7LOADBALNCE_CLASS
```

Related Commands

(config-pmap-lb-generic) description

(config-pmap-lb-generic) description

To provide a brief description of the generic server load balancing (SLB) policy map, use the **description** command. Use the **no** form of this command to remove the description from the policy map.

description *text*

no description

Syntax Description

text	Description for the policy map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Policy map load balancing generic configuration mode

Admin role in any user context

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description that the policy map is to perform server load balancing, enter:

```
host/Admin(config-pmap-lb-generic)# description GENERIC_LOAD_BALANCE_PROTOCOL
```

Related Commands

(config-pmap-lb-generic) class

(config-pmap-lb-generic) match layer4-payload

To make server load balancing (SLB) decisions based on the Layer 4 payload, use the **match layer4-payload** command. Use the **no** form of this command to remove the Layer 4 payload match statement from the policy map.

match *name* **layer4-payload** [**offset** *bytes*] **regex** *expression* [**insert-before** *map_name*]

no match *name* **layer4-payload** [**offset** *bytes*] **regex** *expression* [**insert-before** *map_name*]

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
offset *bytes*	(Optional) Specifies an absolute offset in the data where the Layer 4 payload expression search string starts. The offset starts at the first byte of the TCP or UDP body. Enter an integer from 0 to 999. The default is 0.
regex *expression*	Specifies the Layer 4 payload expression that is contained within the TCP or UDP entity body. Enter a string from 1 to 255 alphanumeric characters. For a list of the supported characters that you can use in regular expression strings, see Table 2-16.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map or other match statement specified by the *map_name* argument. The ACE does not save the sequence reordering as part of the configuration.

Command Modes

Policy map load balancing generic configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

To specify actions for multiple match statements, use a class map as described in the "Class Map Generic Configuration Mode Commands" section.

Generic data parsing begins at Layer 4 with the TCP or UDP payload, which allows you the flexibility to match Layer 5 data (in the case of the Lightweight Directory Access Protocol (LDAP) or the Domain Name System (DNS) or any Layer 7 header or payload (for example, HTTP).

When matching data strings, the period (.) and question mark (?) characters do not have a literal meaning in regular expressions. Use brackets ([]) to match these symbols (for example, enter www[.]xyz[.]com instead of www.xyz.com). You can also use a backslash (\) to escape a dot (.) or a question mark (?).

When you use the **match layer4-payload** command, you access the policy map load balancing generic match configuration mode and the prompt changes to (config-pmap-lb-generic-m). For information about commands in this mode, see the "Policy Map Load Balancing Generic Match Configuration Mode Commands" section.

Examples

To define Layer 4 payload match criteria for a generic policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance generic first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-generic)# match L4_MATCH layer4-payload offset 10 regex abc12.*
host1/Admin(config-pmap-lb-generic-m)#
```

Related Commands

(config-cmap-generic) match layer4-payload

(config-pmap-lb-generic) match source-address

To specify a client source host IP address and subnet mask as the network traffic matching criteria, use the **match source-address** command. You configure the associated policy map to permit or restrict management traffic to the ACE from the specified source network or host. Use the **no** form of this command to clear the source IP address and subnet mask match criteria from the policy map.

match *name* **source-address** *ip_address mask* [**insert-before** *map_name*]

no match *name* **source-address** *ip_address mask*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
ip_address	Source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
mask	Subnet mask of the client entry in dotted-decimal notation (for example, 255.255.255.0).
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map load balancing generic configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

When you use the **match source-address** command, you access the policy map load balancing generic match configuration mode and the prompt changes from (config-pmap-lb-generic) to (config-pmap-lb-generic-m). For information about commands in this mode, see the "Policy Map Load Balancing Generic Match Configuration Mode Commands" section.

Examples

To specify that the Layer 7 SLB policy map matches on source IP address 192.168.10.1 255.255.0.0, enter:

```
host1/Admin(config)# policy-map type loadbalance generic first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-generic)# match match3 source-address 192.168.10.1 255.255.0.0
host1/Admin(config-pmap-lb-generic-m)#
```

Related Commands

(config-cmap-generic) match source-address

Policy Map Load Balancing Generic Class Configuration Mode Commands

Policy map load balancing generic class configuration mode commands allow you to specify the actions that the ACE should take when network traffic matches one or more match statements in the associated Layer 7 server load balancing (SLB) class map. To access policy map load balancing generic class configuration mode, use the **class** command in policy map load balancing generic configuration mode (see the **(config-pmap-lb-generic) class** command for details). The prompt changes to (config-pmap-lb-generic-c).

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

(config-pmap-lb-generic-c) drop

To instruct the ACE to discard packets that match a particular load-balancing criterion in the class map, use the **drop** command. Use the **no** form of this command to reset the ACE to its default of accepting packets from the policy map.

drop

no drop

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map load balancing generic class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to discard packets that match the load-balancing criteria in the class map, enter:

```
host1/Admin(config)# policy-map type loadbalance generic first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-generic)# class L7SLBCLASS
host1/Admin(config-pmap-lb-generic-c)# drop
```

Related Commands

This command has no related commands.

(config-pmap-lb-generic-c) forward

To instruct the ACE to forward requests that match a particular policy map without performing load balancing on the request, use the **forward** command. Use the **no** form of this command to reset the ACE to its default of load balancing packets from the policy map.

forward

no forward

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map load balancing generic class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to forward requests that match a particular policy map without performing load balancing on the request, enter:

```
host1/Admin(config)# policy-map type loadbalance generic first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-generic)# class L7SLBCLASS
host1/Admin(config-pmap-lb-generic-c)# forward
```

Related Commands

This command has no related commands.

(config-pmap-lb-generic-c) serverfarm

To load balance a client request for content to a server farm, use the **serverfarm** command. Server farms are groups of networked real servers that contain the same content and reside in the same physical location. Use the **no** form of this command to remove the server-farm action from the Layer 7 load-balancing policy map.

serverfarm *name1* [**backup** *name2*] [**aggregate-state**]

no serverfarm *name1* [**backup** *name2*] [**aggregate-state**]

Syntax Description

name1	Unique identifier of the server farm. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
backup *name2*	(Optional) Specifies the identifier of an existing server farm that you want the ACE to use as a backup server farm. If the primary server farm goes down, the ACE sends all connections to the configured backup server farm. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
aggregate-state	This option has been deprecated and no longer has an effect on the state of the VIP. By default, the ACE takes into account the state of all real servers in the backup server farm before taking the VIP out of service. If all real servers in the primary server farm fail, but there is at least one real server in the backup server farm that is operational, the ACE keeps the VIP in service.

Command Modes

Policy map load balancing generic class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

If all servers in the server farm fail and you do not configure a backup server farm, the ACE sends a reset (RST) to a client in response to a content request.

If all real servers in the primary server farm fail, the ACE sends client requests to the backup server farm.

Examples

To specify the **serverfarm** command as an action in the load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance generic first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-generic)# class L7SLBCLASS
host1/Admin(config-pmap-lb-generic-c)# serverfarm FARM2 backup FARM3
```

Related Commands

This command has no related commands.

(config-pmap-lb-generic-c) set ip tos

To specify the IP differentiated services code point (DSCP) of packets in a server load balancing (SLB) policy map, use the **set ip tos** command. This command marks a packet by setting the IP DSCP bit in the Type of Service (ToS) byte. Once the IP DSCP bit is set, other Quality of Service (QoS) services can then operate on the bit settings. Use the **no** form of this command to reset the IP DSCP value to the default of 0.

set ip tos *value*

no set ip tos *value*

Syntax Description

value	IP DSCP value. Enter an integer from 0 to 255. The default is 0.

Command Modes

Policy map load balancing generic class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

For details about the ToS byte, see RFC 791, RFC 1122, RFC 1349, and RFC 3168.

Examples

The following example specifies the **set ip tos** command as a QoS action in the Layer 7 load-balancing policy map. All packets that satisfy the match criteria of L7SLBCLASS are marked with the IP DSCP value of 8. How packets marked with the IP DSCP value of 8 are treated is determined by the network configuration.

```
host1/Admin(config)# policy-map type loadbalance generic first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-generic)# class L7SLBCLASS
host1/Admin(config-pmap-lb-generic-c)# set ip tos 8
```

Related Commands

This command has no related commands.

(config-pmap-lb-generic-c) sticky-serverfarm

To specify that all requests that match a Layer 7 policy map are load balanced to a sticky server farm, use the **sticky-serverfarm** command. Use the **no** form of this command to remove a sticky group from the policy map.

sticky-serverfarm *name*

no sticky-serverfarm *name*

Syntax Description

name	Name of an existing sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Policy map load balancing generic class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

For information about sticky groups, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To specify that all requests that match a generic Layer 7 policy map are load balanced to a sticky server farm, enter:

```
host1/Admin(config)# policy-map type loadbalance generic first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-generic)# class L7SLBCLASS
host1/Admin(config-pmap-lb-generic-c)# sticky-serverfarm STICKY_GROUP1
```

Related Commands

This command has no related commands.

Policy Map Load Balancing Generic Match Configuration Mode Commands

Policy map load balancing generic match configuration mode commands allow you to specify the actions that the ACE should take when network traffic matches the specified inline **match** command. To access policy map load balancing generic match configuration mode, use one of the **match** commands in policy map load balancing generic configuration mode (see the "Policy Map Load Balancing Generic Configuration Mode Commands" section for details). The prompt changes to (config-pmap-lb-generic-m).

The inline Layer 7 policy map **match** commands allow you to include a single inline match criteria in the policy map without specifying a traffic class. The inline **match** commands function the same way as the Layer 7 server load balancing (SLB) class map **match** commands. However, when you use an inline **match** command, you can specify an action for only a single **match** command in the generic SLB policy map.

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

(config-pmap-lb-generic-m) drop

To instruct the ACE to discard packets that match a particular load-balancing criteria in an inline **match** command, use the **drop** command. Use the **no** form of this command to reset the ACE to its default of accepting packets from the policy map.

drop

no drop

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map load balancing generic match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to discard packets that match the load-balancing criteria in the inline **match** command, enter:

```
host1/Admin(config)# policy-map type loadbalance generic first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-generic)# match MATCH_SLB1 source-address 192.168.10.1
255.255.0.0
host1/Admin(config-pmap-lb-generic-m)# drop
```

Related Commands

This command has no related commands.

(config-pmap-lb-generic-m) forward

To instruct the ACE to forward requests that match a particular policy map without performing load balancing on the request, use the **forward** command. Use the **no** form of this command to reset the ACE to its default of load balancing packets from the policy map.

forward

no forward

Syntax Description

This command has no keywords or arguments.

Command Modes Policy map load balancing generic match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines This command has no usage guidelines.

Examples To instruct the ACE to forward requests that match a particular policy map without performing load balancing on the request, enter:

```
host1/Admin(config)# policy-map type loadbalance generic first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-generic)# match MATCH_SLB1 source-address 192.168.10.1
255.255.0.0
host1/Admin(config-pmap-lb-generic-m)# forward
```

Related Commands This command has no related commands.

(config-pmap-lb-generic-m) serverfarm

To load balance a client request for content to a server farm, use the **serverfarm** command. Server farms are groups of networked real servers that contain the same content and reside in the same physical location. Use the **no** form of this command to remove the server-farm action from the Layer 7 load balancing policy map.

serverfarm *name1* [**backup** *name2*] [**aggregate-state**]

no serverfarm *name1* [**backup** *name2*] [**aggregate-state**]

Syntax Description

name1	Unique identifier of the server farm. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
backup *name2*	(Optional) Specifies the identifier of an existing server farm that you want the ACE to use as a backup server farm. If the primary server farm goes down, the ACE sends all connections to the configured backup server farm. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
aggregate-state	This option has been deprecated and no longer has an effect on the state of the VIP. By default, the ACE takes into account the state of all real servers in the backup server farm before taking the VIP out of service. If all real servers in the primary server farm fail, but there is at least one real server in the backup server farm that is operational, the ACE keeps the VIP in service.

Command Modes

Policy map load balancing generic match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

If all servers in the server farm fail and you do not configure a backup server farm, the ACE sends a reset (RST) to a client in response to a content request.

If all real servers in the primary server farm fail, the ACE sends client requests to the backup server farm.

Examples

To specify the **serverfarm** command as an action in the load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance generic first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-generic)# match MATCH_SLB1 source-address 192.168.11.2
255.255.255.0
host1/Admin(config-pmap-lb-generic-m)# serverfarm FARM2 backup FARM3
```

Related Commands

This command has no related commands.

(config-pmap-lb-generic-m) set ip tos

To specify the IP differentiated services code point (DSCP) of packets in a server load balancing (SLB) policy map, use the **set ip tos** command. This command marks a packet by setting the IP DSCP bit in the Type of Service (ToS) byte. Once the IP DSCP bit is set, other Quality of Service (QoS) services can then operate on the bit settings. Use the **no** form of this command to reset the IP DSCP value to the default of 0.

set ip tos *value*

no set ip tos *value*

Syntax Description

value	IP DSCP value. Enter an integer from 0 to 255. The default is 0.

Command Modes

Policy map load balancing generic match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

For details about the ToS byte, see RFC 791, RFC 1122, RFC 1349, and RFC 3168.

Examples

To specify the **set ip tos** command as a QoS action in the Layer 7 load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance generic first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-generic)# match MATCH_SLB1 source-address 192.168.10.1
255.255.0.0
host1/Admin(config-pmap-lb-generic-m)# set ip tos 8
```

Related Commands

This command has no related commands.

(config-pmap-lb-generic-m) sticky-serverfarm

To specify that all requests that match a Layer 7 policy map are load balanced to a sticky server farm, use the **sticky-serverfarm** command. Use the **no** form of this command to remove a sticky group from the policy map.

sticky-serverfarm *name*

no sticky-serverfarm *name*

Syntax Description

name	Name of an existing sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Policy map load balancing generic match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

For information about sticky groups, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To specify that all requests that match a Layer 7 policy map are load balanced to a sticky server farm, enter:

```
host1/Admin(config)# policy-map type loadbalance generic first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-generic)# match MATCH_SLB1 source-address 192.168.11.2
255.255.255.0
host1/Admin(config-pmap-lb-generic-m)# sticky-serverfarm STICKY_GROUP1
```

Related Commands

This command has no related commands.

Policy Map Load Balancing HTTP Configuration Mode Commands

Policy map load balancing HTTP configuration mode commands allow you to specify an HTTP Layer 7 policy map for server load-balancing decisions. The ACE executes the specified action only against the first matching load-balancing classification.

To create an HTTP Layer 7 server load balancing (SLB) policy map and access policy map load balancing HTTP configuration mode, use the **policy-map type loadbalance http first-match** command. When you access the policy map load balancing HTTP configuration mode, the prompt changes to (config-pmap-lb). Use the **no** form of this command to remove an HTTP SLB policy map from the ACE.

policy-map type loadbalance [**http**] **first-match** *map_name*

no policy-map type loadbalance [**http**] **first-match** *map_name*

Syntax Description

http	(Optional) Specifies an HTTP Layer 7 load-balancing policy map. HTTP is the default type of load-balancing policy map. If you enter **policy-map type loadbalance first-match** *map_name*, the ACE creates an HTTP load-balancing policy map.
map_name	Name assigned to the HTTP SLB policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You associate the Layer 7 load balancing policy map with a Layer 3 and Layer 4 policy map to provide an entry point for the traffic classification. Layer 7 policy maps are considered to be child policies. Only a Layer 3 and Layer 4 policy map can be activated on a VLAN interface. A Layer 7 policy map cannot be directly applied on a VLAN (or any) interface.

To associate the Layer 7 load-balancing policy map, you nest it by using the Layer 3 and Layer 4 **(config-pmap-c) loadbalance policy** command.

Examples

To create an HTTP SLB policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)#
```

Related Commands

show running-config
(config) policy-map

(config-pmap-lb) class

To associate a Layer 7 server load balancing (SLB) class map with a Layer 7 SLB policy map, use the **class** command. The prompt changes from (config-pmap-lb) to (config-pmap-lb-c). For information about commands in this mode, see the "Policy Map Load Balancing HTTP Class Configuration Mode Commands" section. Use the **no** form of this command to remove an associated class map from a policy map.

class {*name1* [**insert-before** *name2*] | **class-default**}

no class {*name1* [**insert-before** *name2*] | **class-default**}

Syntax Description

name1	Name of a previously defined Layer 7 SLB class map configured with the **class-map** command. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
insert-before *name2*	(Optional) Places the current named class map ahead of an existing class map or inline match condition specified by the *name2* argument in the policy map configuration. The ACE does not save the sequence reordering as part of the configuration.
class-default	Reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified under the **class class-default** command. The **class-default** class map has an implicit **match any** statement in it that enables it to match all traffic.

Command Modes

Policy map load balancing HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To associate a Layer 7 SLB class map with a Layer 7 SLB policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# class L7LOADBALNCE_CLASS
```

Related Commands (config-pmap-lb) description

(config-pmap-lb) description

To provide a brief description of the HTTP server load balancing (SLB) policy map, use the **description** command. Use the **no** form of this command to remove the description from the policy map.

description *text*

no description

Syntax Description

text	Description for the policy map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Policy map load balancing HTTP configuration mode

Admin role in any user context

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description that the policy map is to perform server load balancing, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host/Admin(config-pmap-lb)# description HTTP LOAD BALANCE PROTOCOL
```

Related Commands (config-pmap-lb) class

(config-pmap-lb) match cipher

To make server load-balancing (SLB) decisions based on a specific SSL cipher or cipher strength used to initiate a connection, use the **match cipher** command. Use the **no** form of this command to remove an SSL cipher content match statement from the policy map.

match *name* **cipher** {**equal-to** *cipher* | **less-than** *cipher_strength*}

no match *name* **cipher** {**equal-to** *cipher* | **less-than** *cipher_strength*}

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
equal-to *cipher*	Specifies the SSL cipher. The possible values for *cipher* are as follows: • RSA_EXPORT1024_WITH_DES_CBC_SHA • RSA_EXPORT1024_WITH_RC4_56_MD5 • RSA_EXPORT1024_WITH_RC4_56_SHA • RSA_EXPORT_WITH_DES40_CBC_SHA • RSA_EXPORT_WITH_RC4_40_MD5 • RSA_WITH_3DES_EDE_CBC_SHA • RSA_WITH_AES_128_CBC_SHA • RSA_WITH_AES_256_CBC_SHA • RSA_WITH_DES_CBC_SHA • RSA_WITH_RC4_128_MD5 • RSA_WITH_RC4_128_SHA
less-than *cipher_strength*	Specifies a noninclusive minimum SSL cipher bit strength. For example, if you specify a cipher strength value of 128, any SSL cipher that was no greater than 128 would hit the traffic polkcy. If the SSL cipher was 128-bit or greater, the connection would miss the policy. The possible values for *cipher_strength* are as follows: • 128 • 168 • 256 • 56

Command Modes

Policy map load balancing HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

To specify actions for multiple match statements, use a class map as described in the "Class Map HTTP Load Balancing Configuration Mode Commands" section.

When you use the **match cipher** command, you access the policy map load balancing match configuration mode and the prompt changes to (config-pmap-lb-generic-m). For information about commands in this mode, see the "Policy Map Load Balancing Generic Match Configuration Mode Commands" section.

Examples

To specify that the Layer 7 SLB policy map load balances on a specific SSL cipher, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# match match3 cipher equal-to RSA_WITH_RC4_128_CBC_SHA
host1/Admin(config-pmap-lb-m)#
```

Related Commands

This command has no related commands.

(config-pmap-lb) match http content

To make server load-balancing (SLB) decisions based on the HTTP packet content, use the **match http content** command. Use the **no** form of this command to remove an HTTP content match statement from the policy map.

match *name* **http content** *expression* [**offset** *bytes*] [**insert-before** *map_name*]

no match *name* **http content** *expression*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
expression	Regular expression content to match. Enter a string from 1 to 255 alphanumeric characters. The ACE supports the use of regular expressions for matching data strings. For a list of the supported characters that you can use in regular expressions, see Table 2-16.
offset *number*	(Optional) Specifies the byte at which the ACE begins parsing the packet data. Enter an integer from 1 to 255. The default is 0.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map or other match statement specified by the *map_name* argument. The ACE does not save the sequence reordering as part of the configuration.

Command Modes

Policy map load balancing HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

To specify actions for multiple match statements, use a class map as described in the "Class Map HTTP Load Balancing Configuration Mode Commands" section.

When matching data strings, the period (.) and question mark (?) characters do not have a literal meaning in regular expressions. Use brackets ([]) to match these symbols (for example, enter www[.]xyz[.]com instead of www.xyz.com). You can also use a backslash (\) to escape a dot (.) or a question mark (?).

The ACE can perform regular expression matching against the received packet data from a particular connection based on a regular expression string in HTTP packet data (not the header).

When you use the **match http content** command, you access the policy map load balancing match configuration mode and the prompt changes to (config-pmap-lb-generic-m). For information about commands in this mode, see the "Policy Map Load Balancing Generic Match Configuration Mode Commands" section.

Examples

To specify that the Layer 7 SLB policy map load balances on a specific URL, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# match match3 http content abc*123 offset 50
host1/Admin(config-pmap-lb-m)#
```

Related Commands

(config-cmap-http-lb) match http content

(config-pmap-lb) match http cookie

To make server load balancing (SLB) decisions based on the name and string of a cookie, use the **match http cookie** command. Use the **no** form of this command to remove an HTTP cookie match statement from the policy map.

match *name1* **http cookie** {*name2* | **secondary** *name3*} **cookie-value** *expression* [**insert-before** *map_name*]

no match *name1* **http cookie** {*name2* | **secondary** *name3*} **cookie-value** *expression*

Syntax Description

name1	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
name2	Unique cookie name. Enter an unquoted text string with no spaces and a maximum of 63 alphanumeric characters.
secondary *name3*	Specifies a cookie in a URL string. You can specify the delimiters for cookies in a URL string using a command in an HTTP parameter map.
cookie-value *expression*	Specifies a unique cookie value expression. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. For a list of supported characters that you can use for matching string expressions, see Table 2-16.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map load balancing HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When you use the **match http cookie** command, you access the policy map load balancing HTTP match configuration mode and the prompt changes from (config-pmap-lb) to (config-pmap-lb-m). For information about commands in this mode, see the "Policy Map Load Balancing HTTP Match Configuration Mode Commands" section.

The ACE performs regular expression matching against the received packet data from a particular connection based on the cookie expression. You can configure a maximum of five cookie names per VIP.

The ACE supports regular expressions for matching string expressions. For a list of supported characters that you can use for matching string expressions, see Table 2-16.

For details on defining a list of ASCII-character delimiter strings that you can use to separate the cookies in a URL string, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To specify that the Layer 7 SLB policy map load balances on a cookie with the name of testcookie1, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host/Admin(config-pmap-lb)# match MATCH2 http cookie testcookie1 cookie-value 123456
host1/Admin(config-pmap-lb-m)#
```

Related Commands

(config-parammap-http) set content-maxparse-length
(config-parammap-http) set secondary-cookie-delimiters

(config-pmap-lb) match http header

To make server load balancing (SLB) decisions based on the name and value of an HTTP header, use the **match http header** command. The ACE performs regular expression matching against the received packet data from a particular connection based on the HTTP header expression. Use the **no** form of this command to clear an HTTP header match criteria from the policy map.

match *name* **http header** {*header_name* | *header_field*} **header-value** *expression* [**insert-before** *map_name*]

no match *name* **http header** {*header_name* | *header_field*} **header-value** *expression*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
header_name	Name of the HTTP header to match (for example, www.example1.com.) The range is from 1 to 64 alphanumeric characters. **Note** The *header_name* argument cannot include the colon in the name of the HTTP header; the ACE rejects the colon as an invalid token.
header_field	A standard HTTP/1.1 header field. Valid selections include request-header fields, general-header fields, and the entity-header field. The supported selections are the following: • **Accept**—Semicolon-separated list of representation schemes (content type metainformation values) that will be accepted in the response to the request.

- **Accept-Charset**—Character sets that are acceptable for the response. This field allows clients capable of understanding more comprehensive or special-purpose character sets to signal that capability to a server that can represent documents in those character sets.
- **Accept-Encoding**—Restricts the content encoding that a user will accept from the server.
- **Accept-Language**—ISO code for the language in which the document is written. The language code is an ISO 3316 language code with an optional ISO639 country code to specify a national variant.
- **Authorization**—Specifies that the user agent wants to authenticate itself with a server, usually after receiving a 401 response.
- **Cache-Control**—Directives that must be obeyed by all caching mechanisms along the request/response chain. The directives specify behavior intended to prevent caches from adversely interfering with the request or response.
- **Connection**—Allows the sender to specify connection options.
- **Content-MD5**—MD5 digest of the entity body that provides an end-to-end integrity check. Only a client or an origin server can generate this header field.
- **Expect**—Used by a client to inform the server about the behaviors that the client requires.
- **From**—Contains the e-mail address of the person that controls the requesting user agent.
- **Host**—Internet host and port number of the resource being requested, as obtained from the original URI given by the user or referring resource. The Host field value must represent the naming authority of the origin server or gateway given by the original URL.
- **If-Match**—Used with a method to make it conditional. A client that has one or more entities previously obtained from the resource can verify that one of those entities is current by including a list of their associated entity tags in the If-Match header field. This feature allows efficient updates of cached information with a minimum amount of transaction overhead. It is also used on updating requests to prevent inadvertent modification of the wrong version of a resource. As a special case, the value "*" matches any current entity of the resource.
- **Pragma**—Pragma directives that are understood by servers to whom the directives are relevant. The syntax is the same as for other multiple-value fields in HTTP. For example, the Accept field is a comma-separated list of entries for which the optional parameters are separated by semicolons.

	• **Referer**—Address (URI) of the resource from which the URI in the request was obtained. • **Transfer-Encoding**—Indicates what (if any) type of transformation has been applied to the message body in order to safely transfer it between the sender and the recipient. • **User-Agent**—Information about the user agent (for example, a software program that originates the request). This information is for statistical purposes, the tracing of protocol violations, and automated recognition of user agents. • **Via**—Used by gateways and proxies to indicate the intermediate protocols and recipients between the user agent and the server on requests and between the origin server and the client on responses.
header-value *expression*	Specifies the header value expression string to compare against the value in the specified field in the HTTP header. The range is from 1 to 255 alphanumeric characters. For a list of supported characters that you can use in regular expressions, see Table 2-16.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map load balancing HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When you use the **match http header** command, you access the policy map load balancing HTTP match configuration mode and the prompt changes from (config-pmap-lb) to (config-pmap-lb-m). For information about commands in this mode, see the "Policy Map Load Balancing HTTP Match Configuration Mode Commands" section.

The ACE supports regular expressions for matching. Expressions are stored in a header map in the form *header-name: expression*. Header expressions allow spaces if the spaces are escaped or quoted. For a list of supported characters that you can use in regular expressions, see Table 2-16.

Examples

To specify that the Layer 7 SLB policy map load balances on an HTTP header named Host, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# match match3 http header Host header-value .*cisco.com
host1/Admin(config-pmap-lb-m)#
```

Related Commands

(config-parammap-http) set header-maxparse-length

(config-pmap-lb) match http url

To make server load balancing (SLB) decisions based on the URL name and, optionally, the HTTP method, use the **match http url** command. The ACE performs regular expression matching against the received packet data from a particular connection based on the HTTP URL string. Use the **no** form of this command to remove a URL match statement from the policy map.

match *name* **http url** *expression* [**method** *name*] [**insert-before** *map_name*]

no match *name* **http url** *expression* [**method** *name*]

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
expression	URL, or portion of a URL, to match. Enter a URL string from 1 to 255 alphanumeric characters. Include only the portion of the URL that follows www.*hostname*.*domain* in the match statement. For a list of supported characters that you can use in regular expressions, see Table 2-16.
method *name*	(Optional) Specifies the HTTP method to match. Enter a method name as an unquoted text string with no spaces and a maximum of 15 alphanumeric characters. The method can either be one of the standard HTTP 1.1 method names (OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, or CONNECT) or a text string that must be matched exactly (for example, PROTOPLASM).
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map load balancing HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When you use the **match http url** command, you access the policy map load balancing HTTP match configuration mode and the prompt changes from (config-pmap-lb) to (config-pmap-lb-m). For information about commands in this mode, see the "Policy Map Load Balancing HTTP Match Configuration Mode Commands" section.

Include only the portion of the URL that follows www.*hostname.domain* in the match statement. For example, in the URL www.anydomain.com/latest/whatsnew.html, include only /latest/whatsnew.html. To match the www.anydomain.com portion, the URL string can take the form of a URL regular expression. For a list of supported characters that you can use in regular expressions, see Table 2-16.

When matching data strings, the period (.) and question mark (?) characters do not have a literal meaning in regular expressions. Use brackets ([]) to match these symbols (for example, enter www[.]xyz[.]com instead of www.xyz.com). You can also use a backslash (\) to escape a dot (.) or a question mark (?).

Examples

To specify that the Layer 7 SLB policy map load balances on a specific URL, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# match match3 http url whatsnew/latest.*
```

To use regular expressions to emulate a wildcard search to match on any .gif file, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# match match3 http url .*.gif
host1/Admin(config-pmap-lb-m)#
```

Related Commands

(config-parammap-http) set content-maxparse-length

(config-pmap-lb) match source-address

To specify a client source host IP address and subnet mask from which the ACE accepts traffic as the network traffic matching criteria, use the **match source-address** command. You configure the associated policy map to permit or restrict management traffic to the ACE from the specified source network or host. Use the **no** form of this command to clear the source IP address and subnet mask match criteria from the policy map.

match *name* **source-address** *ip_address mask* [**insert-before** *map_name*]

no match *name* **source-address** *ip_address mask*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
ip_address	Source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
mask	Subnet mask of the client entry in dotted-decimal notation (for example, 255.255.255.0).
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map load balancing HTTP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When you use the **match source-address** command, you access the policy map load balancing HTTP match configuration mode and the prompt changes from (config-pmap-lb) to (config-pmap-lb-m). For information about commands in this mode, see the "Policy Map Load Balancing HTTP Match Configuration Mode Commands" section.

Examples

To specify that the Layer 7 SLB policy map matches on source IP address 192.168.10.1 255.255.0.0, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# match match3 source-address 192.168.10.1 255.255.0.0
host1/Admin(config-pmap-lb-m)#
```

Related Commands

(config-cmap-http-lb) match source-address

Policy Map Load Balancing HTTP Class Configuration Mode Commands

Policy map load balancing HTTP class configuration mode commands allow you to specify the actions that the ACE should take when network traffic matches one or more match statements in the associated Layer 7 server load balancing (SLB) class map. To access policy map load balancing HTTP class configuration mode, use the **class** command in policy map load balancing HTTP configuration mode (see the **(config-pmap-lb) class** command for details). The prompt changes to (config-pmap-lb-c).

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

(config-pmap-lb-c) action

To associate an action list with an HTTP load-balancing policy map, use the **action** command. Use the **no** form of this command to remove the action list association.

action *name*

no action

Syntax Description

name	Identifier of an existing action list. Enter an unquoted text string with a maximum of 64 alphanumeric characters.

Command Modes

Policy map load balancing HTTP class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

You use action lists to group several ACE actions (for example, HTTP header insert, rewrite, or delete) together in a named list under a Layer 7 policy map. For information about action list commands, see the "Action List Modify Configuration Mode Commands" section.

Examples

To associate an action list for HTTP header rewrite, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# class HTTP_CLASS
host1/Admin(config-pmap-lb-c)# action HTTP_MODIFY_ACTLIST
```

To disassociate the action list from the policy map, enter:

```
host1/Admin(config-pmap-lb-c)# no action
```

Related Commands

This command has no related commands.

(config-pmap-lb-c) compress

To instruct the ACE to compress and encode packets that match a Layer 7 SLB policy map, use the **compress** command. Use the **no** form of this command to disable HTTP compression.

compress default-method {**deflate** | **gzip**}

no compress default-method {**deflate** | **gzip**}

Syntax Description

deflate	Specifies the deflate compression method as the method to use when the client browser supports both deflate and gzip compression methods.
gzip	Specifies the gzip compression method as the method to use when the client browser supports both deflate and gzip compression methods.

Command Modes

Policy map load balancing class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The **compress** command option displays only when you associate an HTTP-type class map with a policy map.

When a client request specifies deflate or gzip encoding in the Accept-Encoding field, the ACE uses either deflate or gzip to compress and encode the response content to the client. If both encoding formats are specified in the Accept-Encoding field, the response from the ACE will be encoded according to the **compress default-method** command in the Layer 7 SLB policy map.

HTTP compression is intended primarily for text-based content types. For example, the following are text-based content types:

- text/html
- text/plain
- text/xml
- text/css
- application/x-javascript

By default, the ACE supports HTTP compression at rates of 100 megabits per second (Mbps). Installing an optional HTTP compression license allows you to increase this value to a maximum of 2 Gbps. See the *Cisco 4700 Series Application Control Engine Appliance Administration Guide* for information on ACE licensing options.

When you enable HTTP compression, the ACE compresses the packets using the following default compression parameter values:

- Multipurpose Internet Mail Extension (MIME) type—All text formats (text/.*)
- Minimum content length size—512 bytes
- User agent exclusion—No user agent is excluded

You can create an HTTP parameter map to modify the compression parameters that the ACE uses (see the "Parameter Map Connection Configuration Mode Commands" section).

Examples

To enable compression and specify gzip as the HTTP compression method when both formats are included in the Accept-Encoding client request, enter, enter:

```
host1/Admin(config-pmap-lb-c)# compress default-method gzip
```

Related Commands

(config-parammap-http) compress

(config-pmap-lb-c) drop

To instruct the ACE to discard packets that match a particular load-balancing criteria in the class map, use the **drop** command. Use the **no** form of this command to reset the ACE to its default of accepting packets from the policy map.

drop

no drop

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map load balancing HTTP class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to discard packets that match the load-balancing criteria in the class map, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# class L7SLBCLASS
host1/Admin(config-pmap-lb-c)# drop
```

Related Commands

This command has no related commands.

(config-pmap-lb-c) forward

To instruct the ACE to forward requests that match a particular policy map without performing load balancing on the request, use the **forward** command. Use the **no** form of this command to reset the ACE to its default of load balancing packets from the policy map.

forward

no forward

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map load balancing HTTP class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to forward requests that match a particular policy map without performing load balancing on the request, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# class L7SLBCLASS
host1/Admin(config-pmap-lb-c)# forward
```

Related Commands

This command has no related commands.

(config-pmap-lb-c) insert-http

To specify the name and value of a generic header field that you want the ACE to insert in the HTTP header, use the **insert-http** command. Use the **no** form of this command to delete the HTTP header name and value from the policy map.

insert-http *name* **header-value** *expression*

no insert-http *name* **header-value** *expression*

Syntax Description

name	Name of the generic header field that you want the ACE to insert in the HTTP header. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters.
header-value *expression*	Specifies the header-value expression string to insert in the specified field in the HTTP header. Enter a text string with a maximum of 255 alphanumeric characters. See the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide* for details.

Command Modes

Policy map load balancing HTTP class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

To identify a client whose source IP address has been mapped to another IP address using NAT, you can instruct the ACE to insert a generic header and string value in the client HTTP request. (For information about NAT, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.)

For the *name* argument, you can specify any custom header name that you want, subject to the maximum character length. You can also enter any of the predefined header names described for the **(config-pmap-lb) match http header** command, regardless of whether that header name already exists in the client request header. The ACE does not overwrite any existing header information in the client request.

You can enter a maximum of 255 bytes of data for the header expression. If you enter more than 255 bytes, the ACE does not insert the header name and expression in the client request.

You can also specify the following special **header-value** expressions by using the following special parameter values:

- %is—Inserts the source IP address in the HTTP header.
- %id—Inserts the destination IP address in the HTTP header.
- %ps—Inserts the source port in the HTTP header.
- %pd—Inserts the destination port in the HTTP header.

For Microsoft Outlook Web Access (OWA), specify the field name as HTTP_FRONT_END_HTTPS with a value of ON.

If either TCP server reuse or persistence rebalance is enabled, the ACE inserts a header in every client request.

Examples

For example, to specify the **insert-http** command as an action in the Layer 7 load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# class L7SLBCLASS
host1/Admin(config-pmap-lb-c)# insert-http Host header-value www.cisco.com
```

Related Commands

(config-parammap-http) server-conn reuse
(config-parammap-http) persistence-rebalance

(config-pmap-lb-c) nat dynamic

To configure server farm-based dynamic NAT as an action in a Layer 7 load-balancing policy map, use the **nat dynamic** command.

The syntax of this command is as follows:

nat dynamic *pool_id* **vlan** *number* **serverfarm** {**primary** | **backup**}

no nat dynamic *pool_id* **vlan** *number* **serverfarm** {**primary** | **backup**}

Syntax Description

pool_id	Identifier of the NAT pool of global IP addresses. Enter an integer from 1 to 2147483647.
vlan *number*	Specifies the server interface for the global IP address. This interface must be different from the interface that the ACE uses to filter and receive traffic that requires NAT, unless the network design operates in one-arm mode. In that case, the VLAN number is the same.
serverfarm {**primary** | **backup**}	Specifies that the dynamic NAT applies to either the primary server farm or the backup server farm.

Command Modes

Policy map load balancing HTTP class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

Typically, you use dynamic NAT for SNAT. Dynamic NAT allows you to identify local traffic for address translation by specifying the source and destination addresses in an extended ACL, which is referenced as part of the class map traffic classification. The ACE applies dynamic NAT from the interface to which the traffic policy is attached (through the **service-policy** interface configuration command) to the interface specified in the **nat dynamic** command.

Examples

For example, to specify the **nat-dynamic** command as an action in the Layer 7 load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# class L7SLBCLASS
host1/Admin(config-pmap-lb-c)# nat dynamic serverfarm primary 1 vlan 200
```

Related Commands

show parameter-map
(config-if) nat-pool

(config-pmap-lb-c) serverfarm

To load balance a client request for content to a server farm, use the **serverfarm** command. Server farms are groups of networked real servers that contain the same content and reside in the same physical location. Use the **no** form of this command to remove the server-farm action from the Layer 7 load-balancing policy map.

serverfarm *name1* [**backup** *name2* [**aggregate-state**]]

no serverfarm *name1* [**backup** *name2* [**aggregate-state**]]

Syntax Description

name1	Unique identifier of the server farm. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
backup *name2*	(Optional) Specifies the identifier of an existing server farm that you want the ACE to use as a backup server farm. If the primary server farm goes down, the ACE sends all connections to the configured backup server farm. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
aggregate-state	(Optional) This option has been deprecated and no longer has an effect on the state of the VIP. By default, the ACE takes into account the state of all real servers in the backup server farm before taking the VIP out of service. If all real servers in the primary server farm fail, but there is at least one real server in the backup server farm that is operational, the ACE keeps the VIP in service.

Command Modes

Policy map load balancing HTTP class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	The **aggregate-state** option was deprecated.

Usage Guidelines

If all servers in the server farm fail and you do not configure a backup server farm, the ACE sends a reset (RST) to a client in response to a content request.

By default, the ACE takes into account the state of all the real servers in the backup server farm before taking the VIP out of service. If all the real servers in the primary server farm fail, but there is at least one real server in the backup server farm that is operational, the ACE keeps the VIP in service.

If all real servers in the primary server farm fail, the ACE sends client requests to the backup server farm.

Examples

To specify the **serverfarm** command as an action in the load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# class L7SLBCLASS
host1/Admin(config-pmap-lb-c)# serverfarm FARM2 backup FARM3
```

Related Commands

This command has no related commands.

(config-pmap-lb-c) set ip tos

To specify the IP differentiated services code point (DSCP) of packets in a server load balancing (SLB) policy map, use the **set ip tos** command. This command marks a packet by setting the IP DSCP bit in the Type of Service (ToS) byte. Once the IP DSCP bit is set, other Quality of Service (QoS) services can then operate on the bit settings. Use the **no** form of this command to reset the IP DSCP value to the default of 0.

set ip tos *value*

no set ip tos *value*

Syntax Description

value	IP DSCP value. Enter an integer from 0 to 255. The default is 0.

Command Modes

Policy map load balancing HTTP class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

For details about the ToS byte, see RFC 791, RFC 1122, RFC 1349, and RFC 3168.

Examples

The following example specifies the **set ip tos** command as a QoS action in the Layer 7 load-balancing policy map. All packets that satisfy the match criteria of L7SLBCLASS are marked with the IP DSCP value of 8. How packets marked with the IP DSCP value of 8 are treated is determined by the network configuration.

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# class L7SLBCLASS
host1/Admin(config-pmap-lb-c)# set ip tos 8
```

Related Commands

This command has no related commands.

(config-pmap-lb-c) ssl-proxy client

To specify a Secure Sockets Layer (SSL) proxy service in a Layer 7 load-balancing policy map, use the **ssl-proxy** command. The ACE uses an SSL proxy service in a Layer 7 policy map to load balance outbound SSL initiation requests to SSL servers. In this case, the ACE acts as an SSL client that sends an encrypted request to an SSL server. Use the **no** form of this command to remove the SSL proxy service from the policy map.

ssl-proxy client *name*

no ssl-proxy client *name*

Syntax Description

name	Name of an existing SSL proxy service. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Policy map load balancing HTTP class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

For more information about configuring SSL, see the *Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide*.

Examples

To associate an SSL proxy service with a Layer 7 load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# class L7SLBCLASS
host1/Admin(config-pmap-lb-c)# ssl-proxy client SSL_SERVER_PROXY_SERVICE
```

Related Commands

This command has no related commands.

(config-pmap-lb-c) sticky-serverfarm

To specify that all requests that match a Layer 7 policy map are load balanced to a sticky server farm, use the **sticky-serverfarm** command. Use the **no** form of this command to remove a sticky group from the policy map.

sticky-serverfarm *name*

no sticky-serverfarm *name*

Syntax Description

name	Name of an existing sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Policy map load balancing HTTP class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

For information about sticky groups, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To specify that all requests that match a Layer 7 policy map are load balanced to a sticky server farm, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# class L7SLBCLASS
host1/Admin(config-pmap-lb-c)# sticky-serverfarm STICKY_GROUP1
```

Related Commands

This command has no related commands.

Policy Map Load Balancing HTTP Match Configuration Mode Commands

Policy map load balancing HTTP match configuration mode commands allow you to specify the actions that the ACE should take when network traffic matches the specified inline **match** command. To access policy map load balancing HTTP match configuration mode, use one of the **match** commands in policy map load balancing HTTP configuration mode (see the "Policy Map Load Balancing HTTP Configuration Mode Commands" section for details). The prompt changes to (config-pmap-lb-m).

The inline Layer 7 policy map **match** commands allow you to include a single inline match criteria in the policy map without specifying a traffic class. The inline **match** commands function the same way as the Layer 7 server load balancing (SLB) class map **match** commands. However, when you use an inline **match** command, you can specify an action for only a single **match** command in the HTTP SLB policy map.

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

(config-pmap-lb-m) action

To associate an action list with an HTTP load-balancing policy map, use the **action** command. Use the **no** form of this command to remove the action list association.

action *name*

no action

Syntax Description

name	Identifier of an existing action list. Enter an unquoted text string with a maximum of 64 alphanumeric characters.

Command Modes

Policy map load balancing HTTP match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

You use action lists to group several ACE actions (for example, HTTP header insert, rewrite, or delete) together in a named list under a Layer 7 policy map. For information about action list commands, see the "Action List Modify Configuration Mode Commands" section.

Examples

To associate an action list for HTTP header rewrite, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# match match3 source-address 192.168.10.1 255.255.0.0
host1/Admin(config-pmap-lb-m)# action HTTP_MODIFY_ACTLIST
```

To disassociate the action list from the policy map, enter:

```
host1/Admin(config-pmap-lb-m)# no action
```

Related Commands

This command has no related commands.

(config-pmap-lb-m) compress

To instruct the ACE to compress and encode packets that match a Layer 7 SLB policy map, use the **compress** command. Use the **no** form of this command to disable HTTP compression.

compress default-method {**deflate** | **gzip**}

no compress default-method {**deflate** | **gzip**}

Syntax Description

deflate	Specifies the deflate compression method as the method to use when the client browser supports both deflate and gzip compression methods.
gzip	Specifies the gzip compression method as the method to use when the client browser supports both deflate and gzip compression methods.

Command Modes

Policy map load balancing class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The **compress** command option displays only when you associate an HTTP-type class map with a policy map.

When a client request specifies deflate or gzip encoding in the Accept-Encoding field, the ACE uses either deflate or gzip to compress and encode the response content to the client. If both encoding formats are specified in the Accept-Encoding field, the response from the ACE will be encoded according to the **compress default-method** command in the Layer 7 SLB policy map.

HTTP compression is intended primarily for text-based content types. For example, the following are text-based content types:

- text/html
- text/plain
- text/xml
- text/css
- application/x-javascript

By default, the ACE supports HTTP compression at rates of 100 megabits per second (Mbps). Installing an optional HTTP compression license allows you to increase this value to a maximum of 2 Gbps. See the *Cisco 4700 Series Application Control Engine Appliance Administration Guide* for information on ACE licensing options.

When you enable HTTP compression, the ACE compresses the packets using the following default compression parameter values:

- Multipurpose Internet Mail Extension (MIME) type—All text formats (text/.*)
- Minimum content length size—512 bytes
- User agent exclusion—No user agent is excluded

You can create an HTTP parameter map to modify the compression parameters that the ACE uses (see the "Parameter Map Connection Configuration Mode Commands" section).

Examples

To enable compression and specify gzip as the HTTP compression method when both formats are included in the Accept-Encoding client request, enter, enter:

```
host1/Admin(config-pmap-lb-c)# compress default-method gzip
```

Related Commands

(config-parammap-http) compress

(config-pmap-lb-m) drop

To instruct the ACE to discard packets that match a particular load-balancing criteria in an inline **match** command, use the **drop** command. Use the **no** form of this command to reset the ACE to its default of accepting packets from the policy map.

drop

no drop

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map load balancing HTTP match configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to discard packets that match the load-balancing criteria in the inline **match** command, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# match MATCH_SLB1 http header Host header-value .*cisco.com
host1/Admin(config-pmap-lb-m)# drop
```

Related Commands

This command has no related commands.

(config-pmap-lb-m) forward

To instruct the ACE to forward requests that match a particular policy map without performing load balancing on the request, use the **forward** command. Use the **no** form of this command to reset the ACE to its default of load balancing packets from the policy map.

forward

no forward

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map load balancing HTTP match configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to forward requests that match a particular policy map without performing load balancing on the request, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# match MATCH_SLB1 http header Host header-value .*cisco.com
host1/Admin(config-pmap-lb-m)# forward
```

Related Commands

This command has no related commands.

(config-pmap-lb-m) insert-http

To specify the name and value of a generic header field that you want the ACE to insert in the HTTP header, use the **insert-http** command. Use the **no** form of this command to delete the HTTP header name and value from the policy map.

insert-http *name* **header-value** *expression*

no insert-http *name* **header-value** *expression*

Syntax Description

name	Name of the generic header field that you want the ACE to insert in the HTTP header. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
header-value *expression*	Specifies the header-value expression string to insert in the specified field in the HTTP header. Enter a text string with a maximum of 255 alphanumeric characters. See the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide* for details.

Command Modes

Policy map load balancing HTTP match configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

To identify a client whose source IP address has been mapped to another IP address using NAT, you can instruct the ACE to insert a generic header and string value in the client HTTP request. (For information about NAT, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.)

For the *name* argument, you can specify any custom header name that you want, subject to the maximum character length. You can also enter any of the predefined header names described for the **(config-pmap-lb) match http header** command, regardless of whether that header name already exists in the client request header. The ACE does not overwrite any existing header information in the client request.

You can enter a maximum of 255 bytes of data for the header expression. If you enter more than 255 bytes, the ACE does not insert the header name and expression in the client request.

You can also specify the following special **header-value** expressions by using the following special parameter values:

- %is—Inserts the source IP address in the HTTP header.
- %id—Inserts the destination IP address in the HTTP header.
- %ps—Inserts the source port in the HTTP header.
- %pd—Inserts the destination port in the HTTP header.

For Microsoft Outlook Web Access (OWA), specify the field name as HTTP_FRONT_END_HTTPS with a value of ON.

If either TCP server reuse or persistence rebalance is enabled, the ACE inserts a header in every client request.

Examples

For example, to specify the **insert-http** command as an action in the Layer 7 load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# match MATCH_SLB1 http header Host header-value .*test.com
host1/Admin(config-pmap-lb-m)# insert-http Host header-value .*cisco.com
```

The header name and value will appear in the HTTP header as follows:

```
Host: www.cisco.com
```

Related Commands

(config-parammap-http) server-conn reuse
(config-parammap-http) persistence-rebalance

(config-pmap-lb-m) serverfarm

To load balance a client request for content to a server farm, use the **serverfarm** command. Server farms are groups of networked real servers that contain the same content and reside in the same physical location. Use the **no** form of this command to remove the server-farm action from the Layer 7 load balancing policy map.

serverfarm *name1* [**backup** *name2* [**aggregate-state**]]

no serverfarm *name1* [**backup** *name2* [**aggregate-state**]]

Syntax Description

name1	Unique identifier of the server farm. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
backup *name2*	(Optional) Specifies the identifier of an existing server farm that you want the ACE to use as a backup server farm. If the primary server farm goes down, the ACE sends all connections to the configured backup server farm. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
aggregate-state	This option has been deprecated and no longer has an effect on the state of the VIP. By default, the ACE takes into account the state of all real servers in the backup server farm before taking the VIP out of service. If all real servers in the primary server farm fail, but there is at least one real server in the backup server farm that is operational, the ACE keeps the VIP in service.

Command Modes

Policy map load balancing HTTP match configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	The **aggregate-state** option was deprecated.

Usage Guidelines

If all servers in the server farm fail and you do not configure a backup server farm, the ACE sends a reset (RST) to a client in response to a content request.

If all real servers in the primary server farm fail, the ACE sends client requests to the backup server farm.

Examples

To specify the **serverfarm** command as an action in the load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# match MATCH_SLB1 source-address 192.168.11.2 255.255.255.0
host1/Admin(config-pmap-lb-m)# serverfarm FARM2 backup FARM3
```

Related Commands

This command has no related commands.

(config-pmap-lb-m) set ip tos

To specify the IP differentiated services code point (DSCP) of packets in a server load balancing (SLB) policy map, use the **set ip tos** command. This command marks a packet by setting the IP DSCP bit in the Type of Service (ToS) byte. Once the IP DSCP bit is set, other Quality of Service (QoS) services can then operate on the bit settings. Use the **no** form of this command to reset the IP DSCP value to the default of 0.

set ip tos *value*

no set ip tos *value*

Syntax Description

value	IP DSCP value. Enter an integer from 0 to 255. The default is 0.

Command Modes

Policy map load balancing HTTP match configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

For details about the ToS byte, see RFC 791, RFC 1122, RFC 1349, and RFC 3168.

Examples To specify the **set ip tos** command as a QoS action in the Layer 7 load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# match MATCH_SLB1 http header Via header-value 192.*
host1/Admin(config-pmap-lb-m)# set ip tos 8
```

Related Commands This command has no related commands.

(config-pmap-lb-m) ssl-proxy client

To specify a Secure Sockets Layer (SSL) proxy service in a Layer 7 load-balancing policy map, use the **ssl-proxy client** command. The ACE uses an SSL proxy service in a Layer 7 policy map to load balance outbound SSL initiation requests to SSL servers. In this case, the ACE acts as an SSL client that sends an encrypted request to an SSL server. Use the **no** form of this command to remove the SSL proxy service from the policy map.

ssl-proxy client *name*

no ssl-proxy client *name*

Syntax Description

name	Name of an existing SSL proxy service. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes Policy map load balancing HTTP match configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines For more information about configuring SSL, see the *Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide*.

Examples To associate an SSL proxy service with a Layer 7 load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# match MATCH_SLB1 http header Host header-value .*cisco.com
host1/Admin(config-pmap-lb-m)# ssl-proxy client SSL_SERVER_PROXY_SERVICE
```

Related Commands This command has no related commands.

(config-pmap-lb-m) sticky-serverfarm

To specify that all requests that match a Layer 7 policy map are load balanced to a sticky server farm, use the **sticky-serverfarm** command. Use the **no** form of this command to remove a sticky group from the policy map.

sticky-serverfarm *name*

no sticky-serverfarm *name*

Syntax Description

name	Name of an existing sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Policy map load balancing HTTP match configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

For information about sticky groups, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To specify that all requests that match a Layer 7 policy map are load balanced to a sticky server farm, enter:

```
host1/Admin(config)# policy-map type loadbalance http first-match L7SLBPOLICY
host1/Admin(config-pmap-lb)# match MATCH_SLB1 source-address 192.168.11.2 255.255.255.0
host1/Admin(config-pmap-lb-m)# sticky-serverfarm STICKY_GROUP1
```

Related Commands

This command has no related commands.

Policy Map Load Balancing RADIUS Configuration Mode Commands

Policy map load balancing RADIUS configuration mode commands allow you to specify a RADIUS Layer 7 policy map for server load-balancing decisions. The ACE executes the specified action only against the first matching load-balancing classification.

To create a RADIUS Layer 7 server load balancing (SLB) policy map and access policy map load balancing RADIUS configuration mode, use the **policy-map type loadbalance radius first-match** command. When you access the policy map load balancing RADIUS configuration mode, the prompt changes to (config-pmap-lb-radius). Use the **no** form of this command to remove a RADIUS Layer 7 SLB policy map from the ACE.

policy-map type loadbalance radius first-match *map_name*

no policy-map type loadbalance radius first-match *map_name*

Syntax Description

map_name	Name assigned to the RADIUS SLB policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You associate the Layer 7 load balancing policy map with a Layer 3 and Layer 4 policy map to provide an entry point for the traffic classification. Layer 7 policy maps are considered to be child policies. Only a Layer 3 and Layer 4 policy map can be activated on a VLAN interface. A Layer 7 policy map cannot be directly applied on a VLAN (or any) interface.

To associate the Layer 7 load-balancing policy map, you nest it by using the Layer 3 and Layer 4 **(config-pmap-c) loadbalance policy** command.

Examples

To create a RADIUS SLB policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance radius first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-radius)#
```

Related Commands

show running-config
(config) policy-map

(config-pmap-lb-radius) class

To associate a Layer 7 server load balancing (SLB) class map with a Layer 7 SLB policy map, use the **class** command. The prompt changes from (config-pmap-lb-radius) to (config-pmap-lb-radius-c). For information about commands in this mode, see the "Policy Map Load Balancing RADIUS Class Configuration Mode Commands" section. Use the **no** form of this command to remove an associated class map from a policy map.

class {*name1* [**insert-before** *name2*] | **class-default**}

no class {*name1* [**insert-before** *name2*] | **class-default**}

Syntax Description

name1	Name of a previously defined Layer 7 SLB class map configured with the **class-map** command. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
insert-before *name2*	(Optional) Places the current named class map ahead of an existing class map or inline match condition specified by the *name2* argument in the policy map configuration. The ACE does not save the sequence reordering as part of the configuration.
class-default	Reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified under the **class class-default** command. The **class-default** class map has an implicit **match any** statement in it that enables it to match all traffic.

Command Modes

Policy map load balancing RADIUS configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To associate a Layer 7 SLB class map with a Layer 7 SLB policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance radius first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-radius)# class L7LOADBALNCE_CLASS
host1/Admin(config-pmap-lb-radius-c)#
```

Related Commands

(config-pmap-lb-radius) description

(config-pmap-lb-radius) description

To provide a brief description of the RADIUS server load balancing (SLB) policy map, use the **description** command. Use the **no** form of this command to remove the description from the policy map.

description *text*

no description

Syntax Description

text	Description for the policy map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Policy map load balancing RADIUS configuration mode

Admin role in any user context

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description that the policy map is to perform server load balancing, enter:

```
host/Admin(config-pmap-lb-radius)# description RADIUS_LOAD_BALANCE_PROTOCOL
```

Related Commands

(config-pmap-lb-radius) class

(config-pmap-lb-radius) match radius attribute

To make server load balancing (SLB) decisions based on the calling-station-ID or username RADIUS attribute, use the **match radius attribute** command. Use the **no** form of this command to remove the RADIUS attribute match statement from the policy map.

match *name* **radius attribute** {**calling-station-id** | **username**} *expression* [**insert-before** *map_name*]

no match *name* **radius attribute** {**calling-station-id** | **username**} *expression* [**insert-before** *map_name*]

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
calling-station-id	Specifies the unique identifier of the calling station.
username	Specifies the name of the RADIUS user who initiated the connection.
expression	Calling station ID or username to match. Enter a string from 1 to 64 alphanumeric characters. The ACE supports the use of regular expressions for matching strings. For a list of the supported characters that you can use in regular expressions, see Table 2-16.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map or other match statement specified by the *map_name* argument. The ACE does not save the sequence reordering as part of the configuration.

Command Modes

Policy map load balancing RADIUS configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

To specify actions for multiple match statements, use a class map as described in the "Class Map RADIUS Load Balancing Configuration Mode Commands" section.

When matching data strings, the period (.) and question mark (?) characters do not have a literal meaning in regular expressions. Use brackets ([]) to match these symbols (for example, enter www[.]xyz[.]com instead of www.xyz.com). You can also use a backslash (\) to escape a dot (.) or a question mark (?).

When you use the **match radius attribute** command, you access the policy map load balancing RADIUS match configuration mode and the prompt changes to (config-pmap-lb-radius-m). For information about commands in this mode, see the "Policy Map Load Balancing RADIUS Match Configuration Mode Commands" section.

Examples

To configure RADIUS match criteria for a RADIUS policy map based on the calling station ID attribute, enter:

```
host1/Admin(config)# policy-map type loadbalance radius first-match RADIUS_POLICY
host1/Admin(config-pmap-lb-radius)# match CALL_ID radius attribute calling-station-id 122*
host1/Admin(config-pmap-lb-radius-m)#
```

To remove the RADIUS attribute match statement from the RADIUS policy map, enter:

```
host1/Admin(config-pmap-lb-radius)# no match CALL_ID radius attribute calling-station-id
122*
```

Related Commands

(config-cmap-radius-lb) match radius attribute

Policy Map Load Balancing RADIUS Class Configuration Mode Commands

Policy map load balancing RADIUS class configuration mode commands allow you to specify the actions that the ACE should take when network traffic matches one or more match statements in the associated Layer 7 server load balancing (SLB) class map. To access policy map load balancing RADIUS class configuration mode, use the **class** command in policy map load balancing RADIUS configuration mode (see the **(config-pmap-lb-radius) class** command for details). The prompt changes to (config-pmap-lb-radius-c).

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

(config-pmap-lb-radius-c) drop

To instruct the ACE to discard packets that match a particular load-balancing criterion in the class map, use the **drop** command. Use the **no** form of this command to reset the ACE to its default of accepting packets from the policy map.

drop

no drop

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map load balancing RADIUS class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to discard packets that match the load-balancing criteria in the class map, enter:

```
host1/Admin(config)# policy-map type loadbalance radius first-match RAD_POLICY
host1/Admin(config-pmap-lb-radius)# class RAD_CLASS
host1/Admin(config-pmap-lb-radius-c)# drop
```

Related Commands

This command has no related commands.

(config-pmap-lb-radius-c) forward

To instruct the ACE to forward requests that match a particular policy map without performing load balancing on the request, use the **forward** command. Use the **no** form of this command to reset the ACE to its default of load balancing packets from the policy map.

forward

no forward

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map load balancing RADIUS class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to forward requests that match a particular policy map without performing load balancing on the request, enter:

```
host1/Admin(config)# policy-map type loadbalance radius first-match RAD_POLICY
host1/Admin(config-pmap-lb-radius)# class RAD_CLASS
host1/Admin(config-pmap-lb-radius-c)# forward
```

Related Commands

This command has no related commands.

(config-pmap-lb-radius-c) serverfarm

To load balance a client request for content to a server farm, use the **serverfarm** command. Server farms are groups of networked real servers that contain the same content and reside in the same physical location. Use the **no** form of this command to remove the server-farm action from the Layer 7 load-balancing policy map.

serverfarm *name1* [**backup** *name2* [**aggregate-state**]]

no serverfarm *name1* [**backup** *name2* [**aggregate-state**]]

Syntax Description

name1	Unique identifier of the server farm. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
backup *name2*	(Optional) Specifies the identifier of an existing server farm that you want the ACE to use as a backup server farm. If the primary server farm goes down, the ACE sends all connections to the configured backup server farm. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
aggregate-state	This option has been deprecated and no longer has an effect on the state of the VIP. By default, the ACE takes into account the state of all real servers in the backup server farm before taking the VIP out of service. If all real servers in the primary server farm fail, but there is at least one real server in the backup server farm that is operational, the ACE keeps the VIP in service.

Command Modes

Policy map load balancing RADIUS class configuration mode

Admin and user contexts

Command History

Release	Modification
A2(1.0)	This command was introduced.

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

If all servers in the server farm fail and you do not configure a backup server farm, the ACE sends a reset (RST) to a client in response to a content request.

If all real servers in the primary server farm fail, the ACE sends client requests to the backup server farm.

Examples To specify the **serverfarm** command as an action in the load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance radius first-match RAD_POLICY
host1/Admin(config-pmap-lb-radius)# class RAD_CLASS
host1/Admin(config-pmap-lb-radius-c)# serverfarm FARM2 backup FARM3
```

Related Commands This command has no related commands.

(config-pmap-lb-radius-c) set ip tos

To specify the IP differentiated services code point (DSCP) of packets in a server load balancing (SLB) policy map, use the **set ip tos** command. This command marks a packet by setting the IP DSCP bit in the Type of Service (ToS) byte. Once the IP DSCP bit is set, other Quality of Service (QoS) services can then operate on the bit settings. Use the **no** form of this command to reset the IP DSCP value to the default of 0.

set ip tos *value*

no set ip tos *value*

Syntax Description

value	IP DSCP value. Enter an integer from 0 to 255. The default is 0.

Command Modes Policy map load balancing RADIUS class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines For details about the ToS byte, see RFC 791, RFC 1122, RFC 1349, and RFC 3168.

Examples The following example specifies the **set ip tos** command as a QoS action in the Layer 7 load-balancing policy map. All packets that satisfy the match criteria of the class map RAD_CLASS are marked with the IP DSCP value of 8. How packets marked with the IP DSCP value of 8 are treated is determined by the network configuration.

```
host1/Admin(config)# policy-map type loadbalance radius first-match RAD_POLICY
host1/Admin(config-pmap-lb-radius)# class RAD_CLASS
host1/Admin(config-pmap-lb-radius-c)# set ip tos 8
```

Related Commands This command has no related commands.

(config-pmap-lb-radius-c) sticky-serverfarm

To specify that all requests that match a Layer 7 policy map are load balanced to a sticky server farm, use the **sticky-serverfarm** command. Use the **no** form of this command to remove a sticky group from the policy map.

sticky-serverfarm *name*

no sticky-serverfarm *name*

Syntax Description

name	Name of an existing sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Policy map load balancing RADIUS class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

For information about sticky groups, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To specify that all requests that match a RADIUS Layer 7 policy map are load balanced to a sticky server farm, enter:

```
host1/Admin(config)# policy-map type loadbalance radius first-match RAD_POLICY
host1/Admin(config-pmap-lb-radius)# class RAD_CLASS
host1/Admin(config-pmap-lb-radius-c)# sticky-serverfarm STICKY_GROUP1
```

Related Commands

This command has no related commands.

Policy Map Load Balancing RADIUS Match Configuration Mode Commands

Policy map load balancing RADIUS match configuration mode commands allow you to specify the actions that the ACE should take when network traffic matches the specified inline **match** command. To access policy map load balancing RADIUS match configuration mode, use one of the **match** commands in policy map load balancing RADIUS configuration mode (see the "Policy Map Load Balancing RADIUS Configuration Mode Commands" section for details). The prompt changes to (config-pmap-lb-radius-m).

The inline Layer 7 policy map **match** commands allow you to include a single inline match criteria in the policy map without specifying a traffic class. The inline **match** commands function the same way as the Layer 7 server load balancing (SLB) class map **match** commands. However, when you use an inline **match** command, you can specify an action for only a single **match** command in the RADIUS SLB policy map.

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

(config-pmap-lb-radius-m) drop

To instruct the ACE to discard packets that match a particular load-balancing criteria in an inline **match** command, use the **drop** command. Use the **no** form of this command to reset the ACE to its default of accepting packets from the policy map.

drop

no drop

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map load balancing RADIUS match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to discard packets that match the load-balancing criteria in the inline **match** command, enter:

```
host1/Admin(config)# policy-map type loadbalance radius first-match RADIUS_POLICY
host1/Admin(config-pmap-lb-radius)# match CALL_ID radius attribute calling-station-id 122*
host1/Admin(config-pmap-lb-radius-m)# drop
```

Related Commands

This command has no related commands.

(config-pmap-lb-radius-m) forward

To instruct the ACE to forward requests that match a particular load-balancing criteria in an inline **match** command without performing load balancing on the request, use the **forward** command. Use the **no** form of this command to reset the ACE to its default of load balancing packets from the policy map.

forward

no forward

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map load balancing RADIUS match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to forward requests that match a particular policy map without performing load balancing on the request, enter:

```
host1/Admin(config)# policy-map type loadbalance radius first-match RADIUS_POLICY
host1/Admin(config-pmap-lb-radius)# match CALL_ID radius attribute calling-station-id 122*
host1/Admin(config-pmap-lb-radius-m)# forward
```

Related Commands

This command has no related commands.

(config-pmap-lb-radius-m) serverfarm

To load balance a client request for content to a server farm, use the **serverfarm** command. Server farms are groups of networked real servers that contain the same content and reside in the same physical location. Use the **no** form of this command to remove the server-farm action from the Layer 7 load balancing policy map.

serverfarm *name1* [**backup** *name2* [**aggregate-state**]]

no serverfarm *name1* [**backup** *name2* [**aggregate-state**]]

Syntax Description

name1	Unique identifier of the server farm. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
backup *name2*	(Optional) Specifies the identifier of an existing server farm that you want the ACE to use as a backup server farm. If the primary server farm goes down, the ACE sends all connections to the configured backup server farm. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
aggregate-state	This option has been deprecated and no longer has an effect on the state of the VIP. By default, the ACE takes into account the state of all real servers in the backup server farm before taking the VIP out of service. If all real servers in the primary server farm fail, but there is at least one real server in the backup server farm that is operational, the ACE keeps the VIP in service.

Command Modes

Policy map load balancing RADIUS match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

If all servers in the server farm fail and you do not configure a backup server farm, the ACE sends a reset (RST) to a client in response to a content request.

If all real servers in the primary server farm fail, the ACE sends client requests to the backup server farm.

Examples

To specify the **serverfarm** command as an action in the RADIUS load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance radius first-match RADIUS_POLICY
host1/Admin(config-pmap-lb-radius)# match CALL_ID radius attribute calling-station-id 122*
host1/Admin(config-pmap-lb-radius-m)# serverfarm FARM2 backup FARM3
```

Related Commands

This command has no related commands.

(config-pmap-lb-radius-m) set ip tos

To specify the IP differentiated services code point (DSCP) of packets in a server load balancing (SLB) policy map, use the **set ip tos** command. This command marks a packet by setting the IP DSCP bit in the Type of Service (ToS) byte. Once the IP DSCP bit is set, other Quality of Service (QoS) services can then operate on the bit settings. Use the **no** form of this command to reset the IP DSCP value to the default of 0.

set ip tos *value*

no set ip tos *value*

Syntax Description

value	IP DSCP value. Enter an integer from 0 to 255. The default is 0.

Command Modes

Policy map load balancing RADIUS match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

For details about the ToS byte, see RFC 791, RFC 1122, RFC 1349, and RFC 3168.

Examples

To specify the **set ip tos** command as a QoS action in the Layer 7 load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance radius first-match RADIUS_POLICY
host1/Admin(config-pmap-lb-radius)# match CALL_ID radius attribute calling-station-id 122*
host1/Admin(config-pmap-lb-radius-m)# set ip tos 8
```

Related Commands

This command has no related commands.

(config-pmap-lb-radius-m) sticky-serverfarm

To specify that all requests that match a Layer 7 policy map are load balanced to a sticky server farm, use the **sticky-serverfarm** command. Use the **no** form of this command to remove a sticky group from the policy map.

sticky-serverfarm *name*

no sticky-serverfarm *name*

Syntax Description

name	Name of an existing sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Policy map load balancing RADIUS match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

For information about sticky groups, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To specify that all requests that match a RADIUS policy map are load balanced to a sticky server farm, enter:

```
host1/Admin(config)# policy-map type loadbalance radius first-match RADIUS_POLICY
host1/Admin(config-pmap-lb-radius)# match CALL_ID radius attribute calling-station-id 122*
host1/Admin(config-pmap-lb-radius-m)# sticky-serverfarm STICKY_GROUP1
```

Related Commands

This command has no related commands.

Policy Map Load Balancing RDP Configuration Mode Commands

Policy map load balancing Reliable Datagram Protocol (RDP) configuration mode commands allow you to specify an RDP Layer 7 policy map for server load-balancing decisions. The ACE executes the specified action only against the first matching load-balancing classification.

To create an RDP Layer 7 server load balancing (SLB) policy map and access policy map load balancing RDP configuration mode, use the **policy-map type loadbalance rdp first-match** command. When you access the policy map load balancing RDP configuration mode, the prompt changes to (config-pmap-lb-rdp). Use the **no** form of this command to remove an RDP Layer 7 SLB policy map from the ACE.

policy-map type loadbalance rdp first-match *map_name*

no policy-map type loadbalance rdp first-match *map_name*

Syntax Description

map_name	Name assigned to the RDP SLB policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You associate the Layer 7 load balancing policy map with a Layer 3 and Layer 4 policy map to provide an entry point for the traffic classification. Layer 7 policy maps are considered to be child policies. Only a Layer 3 and Layer 4 policy map can be activated on a VLAN interface. A Layer 7 policy map cannot be directly applied on a VLAN (or any) interface.

To associate the Layer 7 load-balancing policy map, you nest it by using the Layer 3 and Layer 4 **(config-pmap-c) loadbalance policy** command.

Examples

To create an RDP SLB policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance rdp first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-rdp)#
```

Related Commands

show running-config
(config) policy-map

(config-pmap-lb-rdp) class

To associate a Layer 7 server load balancing (SLB) class map with a Layer 7 SLB policy map, use the **class** command. The prompt changes from (config-pmap-lb-rdp) to (config-pmap-lb-rdp-c). For information about commands in this mode, see the "Policy Map Load Balancing RDP Class Configuration Mode Commands" section. Use the **no** form of this command to remove the associated class map from a policy map.

class class-default

no class class-default

Syntax Description

class-default	Reserved, well-known class map created by the ACE. You cannot delete or modify this class map. The **class-default** class map has an implicit **match any** statement in it that enables it to match all traffic.

Command Modes

Policy map load balancing RDP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

For RDP load-balancing policy maps, you can only assign the **class-default** class map.

Examples

To associate the Layer 7 **class-default** class map with the RDP SLB policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance rdp first-match RDP_POLICY
host/Admin(config-pmap-lb-rdp)# class class-default
host/Admin(config-pmap-lb-rdp-c)#
```

Related Commands

(config-pmap-lb-rdp) description

(config-pmap-lb-rdp) description

To provide a brief description of the RDP server load balancing (SLB) policy map, use the **description** command. Use the **no** form of this command to remove the description from the policy map.

description *text*

no description

Syntax Description

text	Description for the policy map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Policy map load balancing RDP configuration mode

Admin role in any user context

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description that the policy map is to perform server load balancing, enter:

```
host/Admin(config-pmap-lb-rdp)# description RDP_LOAD_BALANCE_PROTOCOL
```

Related Commands

(config-pmap-lb-rdp) class

Policy Map Load Balancing RDP Class Configuration Mode Commands

Policy map load balancing RDP class configuration mode commands allow you to specify the actions that the ACE should take when network traffic matches one or more match statements in the associated Layer 7 server load balancing (SLB) class map. To access policy map load balancing RDP class configuration mode, use the **class** command in policy map load balancing RDP configuration mode (see the **(config-pmap-lb-rdp) class** command for details). The prompt changes to (config-pmap-lb-rdp-c).

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

(config-pmap-lb-rdp-c) drop

To instruct the ACE to discard packets that match a particular load-balancing criterion in the class map, use the **drop** command. Use the **no** form of this command to reset the ACE to its default of accepting packets from the policy map.

drop

no drop

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map load balancing RDP class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to discard packets that match the load-balancing criteria in the class map, enter:

```
host1/Admin(config)# policy-map type loadbalance rdp first-match RDP_POLICY
host1/Admin(config-pmap-lb-rdp)# class class-default
host1/Admin(config-pmap-lb-rdp-c)# drop
```

Related Commands

This command has no related commands.

(config-pmap-lb-rdp-c) forward

To instruct the ACE to forward requests that match a particular policy map without performing load balancing on the request, use the **forward** command. Use the **no** form of this command to reset the ACE to its default of load balancing packets from the policy map.

forward

no forward

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map load balancing RDP class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to forward requests that match a particular policy map without performing load balancing on the request, enter:

```
host1/Admin(config)# policy-map type loadbalance rdp first-match RDP_POLICY
host1/Admin(config-pmap-lb-rdp)# class class-default
host1/Admin(config-pmap-lb-rdp-c)# forward
```

Related Commands

This command has no related commands.

(config-pmap-lb-rdp-c) serverfarm

To load balance a client request for content to a server farm, use the **serverfarm** command. Server farms are groups of networked real servers that contain the same content and reside in the same physical location. Use the **no** form of this command to remove the server-farm action from the Layer 7 load-balancing policy map.

serverfarm *name1* [**backup** *name2* [**aggregate-state**]]

no serverfarm *name1* [**backup** *name2* [**aggregate-state**]]

Syntax Description

name1	Unique identifier of the server farm. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
backup *name2*	(Optional) Specifies the identifier of an existing server farm that you want the ACE to use as a backup server farm. If the primary server farm goes down, the ACE sends all connections to the configured backup server farm. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
aggregate-state	This option has been deprecated and no longer has an effect on the state of the VIP. By default, the ACE takes into account the state of all real servers in the backup server farm before taking the VIP out of service. If all real servers in the primary server farm fail, but there is at least one real server in the backup server farm that is operational, the ACE keeps the VIP in service.

Command Modes

Policy map load balancing RDP class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

If all servers in the server farm fail and you do not configure a backup server farm, the ACE sends a reset (RST) to a client in response to a content request.

If all real servers in the primary server farm fail, the ACE sends client requests to the backup server farm.

Examples

To specify the **serverfarm** command as an action in the load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance rdp first-match RDP_POLICY
host1/Admin(config-pmap-lb-rdp)# class class-default
host1/Admin(config-pmap-lb-rdp-c)# serverfarm FARM2 backup FARM3
```

Related Commands

This command has no related commands.

(config-pmap-lb-rdp-c) set ip tos

To specify the IP differentiated services code point (DSCP) of packets in a server load balancing (SLB) policy map, use the **set ip tos** command. This command marks a packet by setting the IP DSCP bit in the Type of Service (ToS) byte. Once the IP DSCP bit is set, other Quality of Service (QoS) services can then operate on the bit settings. Use the **no** form of this command to reset the IP DSCP value to the default of 0.

set ip tos *value*

no set ip tos *value*

Syntax Description

value	IP DSCP value. Enter an integer from 0 to 255. The default is 0.

Command Modes

Policy map load balancing RDP class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

For details about the ToS byte, see RFC 791, RFC 1122, RFC 1349, and RFC 3168.

Examples

The following example specifies the **set ip tos** command as a QoS action in the Layer 7 load-balancing policy map. All packets that satisfy the match criteria of the class-default class map are marked with the IP DSCP value of 8. How packets marked with the IP DSCP value of 8 are treated is determined by the network configuration.

```
host1/Admin(config)# policy-map type loadbalance rdp first-match RDP_POLICY
host1/Admin(config-pmap-lb-rdp)# class class-default
host1/Admin(config-pmap-lb-rdp-c)# set ip tos 8
```

Related Commands

This command has no related commands.

(config-pmap-lb-rdp-c) sticky-serverfarm

To specify that all requests that match a Layer 7 policy map are load balanced to a sticky server farm, use the **sticky-serverfarm** command. Use the **no** form of this command to remove a sticky group from the policy map.

sticky-serverfarm *name*

no sticky-serverfarm *name*

Syntax Description

name	Name of an existing sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Policy map load balancing RDP class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

For information about sticky groups, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To specify that all requests that match an RDP Layer 7 policy map are load balanced to a sticky server farm, enter:

```
host1/Admin(config)# policy-map type loadbalance rdp first-match RDP_POLICY
host1/Admin(config-pmap-lb-rdp)# class class-default
host1/Admin(config-pmap-lb-rdp-c)# sticky-serverfarm STICKY_GROUP1
```

Related Commands

This command has no related commands.

Policy Map Load Balancing RTSP Configuration Mode Commands

Policy map load balancing RTSP configuration mode commands allow you to specify a Real-Time Streaming Protocol (RTSP) Layer 7 policy map for server load-balancing decisions. The ACE executes the specified action only against the first matching load-balancing classification.

To create an RTSP Layer 7 server load balancing (SLB) policy map and access policy map load balancing RTSP configuration mode, use the **policy-map type loadbalance rtsp first-match** command. When you access the policy map load balancing RTSP configuration mode, the prompt changes to (config-pmap-lb-rtsp). Use the **no** form of this command to remove an RTSP SLB policy map from the ACE.

policy-map type loadbalance rtsp first-match *map_name*

no policy-map type loadbalance rtsp first-match *map_name*

Syntax Description

map_name	Name assigned to the RTSP SLB policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You associate the Layer 7 load balancing policy map with a Layer 3 and Layer 4 policy map to provide an entry point for the traffic classification. Layer 7 policy maps are considered to be child policies. Only a Layer 3 and Layer 4 policy map can be activated on a VLAN interface. A Layer 7 policy map cannot be directly applied on a VLAN (or any) interface.

To associate the Layer 7 load-balancing policy map, you nest it by using the Layer 3 and Layer 4 **(config-pmap-c) loadbalance policy** command.

Examples

To create an RTSP SLB policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance rtsp first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-rtsp)#
```

Related Commands

show running-config
(config) policy-map

(config-pmap-lb-rtsp) class

To associate a Layer 7 server load balancing (SLB) class map with a Layer 7 SLB policy map, use the **class** command. The prompt changes from (config-pmap-lb-rtsp) to (config-pmap-lb-rtsp-c). For information about commands in this mode, see the "Policy Map Load Balancing RTSP Class Configuration Mode Commands" section. Use the **no** form of this command to remove an associated class map from a policy map.

class {*name1* [**insert-before** *name2*] | **class-default**}

no class {*name1* [**insert-before** *name2*] | **class-default**}

Syntax Description

name1	Name of a previously defined Layer 7 SLB class map configured with the **class-map** command. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
insert-before *name2*	(Optional) Places the current named class map ahead of an existing class map or inline match condition specified by the *name2* argument in the policy map configuration. The ACE does not save the sequence reordering as part of the configuration.
class-default	Reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified under the **class class-default** command. The **class-default** class map has an implicit **match any** statement in it that enables it to match all traffic.

Command Modes

Policy map load balancing RTSP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To associate a Layer 7 SLB class map with a Layer 7 SLB policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance rtsp first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-rtsp)# class L7LOADBALNCE_CLASS
host1/Admin(config-pmap-lb-rtsp-c)#
```

Related Commands

(config-pmap-lb-rtsp) description

(config-pmap-lb-rtsp) description

To provide a brief description of the RTSP server load balancing (SLB) policy map, use the **description** command. Use the **no** form of this command to remove the description from the policy map.

description *text*

no description

Syntax Description

text	Description for the policy map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Policy map load balancing RTSP configuration mode

Admin role in any user context

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description that the policy map is to perform server load balancing, enter:

```
host1/Admin(config)# policy-map type loadbalance rtsp first-match L7SLBPOLICY
host/Admin(config-pmap-lb-rtsp)# description RTSP_LOAD_BALANCE_PROTOCOL
```

Related Commands

(config-pmap-lb-rtsp) class

(config-pmap-lb-rtsp) match rtsp header

To make server load balancing (SLB) decisions based on the name and value of an RTSP header, use the **match rtsp header** command. The ACE performs regular expression matching against the received packet data from a particular connection based on the RTSP header expression. Use the **no** form of this command to clear an RTSP header match criteria from the policy map.

match *name* **rtsp header** *header_name* **header-value** *expression* [**insert-before** *map_name*]

no match *name* **rtsp header** *header_name* **header-value** *expression*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
header_name	Name of the field in the RTSP header. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. You can enter a text string with spaces if you enclose the entire string in quotation marks (“ ”). You can enter any header field name, including a standard RTSP header field name or any user-defined header field name. Because RTSP is similar in syntax and operation to HTTP/1.1, you can use any HTTP header listed in Table 2-6 if the RTSP server supports it. For a complete list of RTSP headers, see RFC 2326.
header-value *expression*	Specifies the expression string to compare against the value in the specified field in the RTSP header. Enter a text string with a maximum of 255 alphanumeric characters. The ACE supports the use of regular expressions for header matching. Header expressions allow spaces if the entire string that contains spaces is quoted. For a list of the supported characters that you can use in regular expressions, see Table 2-16.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map load balancing RTSP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

When you use the **match rtsp header** command, you access the policy map load balancing RTSP match configuration mode and the prompt changes from (config-pmap-lb-rtsp) to (config-pmap-lb-rtsp-m). For information about commands in this mode, see the "Policy Map Load Balancing RTSP Match Configuration Mode Commands" section.

The ACE supports regular expressions for matching. Expressions are stored in a header map in the form *header-name: expression*. Header expressions allow spaces if the spaces are escaped or quoted. For a list of supported characters that you can use in regular expressions, see Table 2-16.

Examples

To specify that the Layer 7 SLB policy map load balances on an RTSP header named Host, enter:

```
host1/Admin(config)# policy-map type loadbalance rtsp first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-rtsp)# match match3 rtsp header Host header-value .*cisco.com
host1/Admin(config-pmap-lb-rtsp-m)#
```

Related Commands

(config-parammap-rtsp) set header-maxparse-length

(config-pmap-lb-rtsp) match rtsp source-address

To specify a client source host IP address and subnet mask from which the ACE accepts traffic as the network traffic matching criteria, use the **match rtsp source-address** command. You configure the associated policy map to permit or restrict management traffic to the ACE from the specified source network or host. Use the **no** form of this command to clear the source IP address and subnet mask match criteria from the policy map.

match *name* **rtsp source-address** *ip_address mask* [**insert-before** *map_name*]

no match *name* **rtsp source-address** *ip_address mask*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
ip_address	Source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
mask	Subnet mask of the client entry in dotted-decimal notation (for example, 255.255.255.0).
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map load balancing RTSP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

When you use the **match rtsp source-address** command, you access the policy map load balancing RTSP match configuration mode and the prompt changes from (config-pmap-lb-rtsp) to (config-pmap-lb-rtsp-m). For information about commands in this mode, see the "Policy Map Load Balancing RTSP Match Configuration Mode Commands" section.

Examples

To specify that the Layer 7 SLB policy map matches on source IP address 192.168.10.1 255.255.0.0, enter:

```
host1/Admin(config)# policy-map type loadbalance rtsp first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-rtsp)# match match3 rtsp source-address 192.168.10.1
255.255.0.0
host1/Admin(config-pmap-lb-rtsp-m)#
```

Related Commands

(config-cmap-rtsp-lb) match source-address

(config-pmap-lb-rtsp) match rtsp url

To make server load balancing (SLB) decisions based on the URL name and, optionally, the RTSP method, use the **match rtsp url** command. The ACE performs regular expression matching against the received packet data from a particular connection based on the RTSP URL string. Use the **no** form of this command to remove a URL match statement from the policy map.

match *name* **rtsp url** *expression* [**method** *name*] [**insert-before** *map_name*]

no match *name* **rtsp url** *expression* [**method** *name*]

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
expression	URL, or portion of a URL, to match. Enter a URL string from 1 to 255 alphanumeric characters. The ACE supports the use of regular expressions for matching URL strings. For a list of supported characters that you can use in regular expressions, see Table 2-16.
method *name*	(Optional) Specifies the RTSP method to match. Enter a method name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. The method can either be one of the standard RTSP method names (OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, or CONNECT) or it can be a text string that must be matched exactly (for example, STINGRAY).
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map load balancing RTSP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

When you use the **match rtsp url** command, you access the policy map load balancing RTSP match configuration mode and the prompt changes from (config-pmap-lb-rtsp) to (config-pmap-lb-rtsp-m). For information about commands in this mode, see the "Policy Map Load Balancing RTSP Match Configuration Mode Commands" section.

When matching data strings, note that the period (.) and question mark (?) characters do not have a literal meaning in regular expressions. Use brackets ([]) to match these symbols (for example, enter www[.]xyz[.]com instead of www.xyz.com). You can also use a backslash (\) to escape a dot (.) or a question mark (?).

Examples

To specify that the Layer 7 SLB policy map load balances on a specific URL, enter:

```
host1/Admin(config)# policy-map type loadbalance rtsp first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-rtsp)# match match3 rtsp url whatsnew/latest.*
host1/Admin(config-pmap-lb-rtsp-m)#
```

To use regular expressions to emulate a wildcard search to match on any .gif file, enter:

```
host1/Admin(config)# policy-map type loadbalance rtsp first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-rtsp)# match match3 rtsp url .*.gif
```

Related Commands

(config-cmap-rtsp-lb) match rtsp url

Policy Map Load Balancing RTSP Class Configuration Mode Commands

Policy map load balancing RTSP class configuration mode commands allow you to specify the actions that the ACE should take when network traffic matches one or more match statements in the associated Layer 7 server load balancing (SLB) class map. To access policy map load balancing RTSP class configuration mode, use the **class** command in policy map load balancing RTSP configuration mode (see the **(config-pmap-lb-rtsp) class** command for details). The prompt changes to (config-pmap-lb-rtsp-c).

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

(config-pmap-lb-rtsp-c) drop

To instruct the ACE to discard packets that match a particular load-balancing criteria in the class map, use the **drop** command. Use the **no** form of this command to reset the ACE to its default of accepting packets from the policy map.

drop

no drop

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map load balancing RTSP class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to discard packets that match the load-balancing criteria in the class map, enter:

```
host1/Admin(config)# policy-map type loadbalance rtsp first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-rtsp)# class L7SLBCLASS
host1/Admin(config-pmap-lb-rtsp-c)# drop
```

Related Commands

This command has no related commands.

(config-pmap-lb-rtsp-c) forward

To instruct the ACE to forward requests that match a particular policy map without performing load balancing on the request, use the **forward** command. Use the **no** form of this command to reset the ACE to its default of load balancing packets from the policy map.

forward

no forward

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map load balancing RTSP class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to forward requests that match a particular policy map without performing load balancing on the request, enter:

```
host1/Admin(config)# policy-map type loadbalance rtsp first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-rtsp)# class L7SLBCLASS
host1/Admin(config-pmap-lb-rtsp-c)# forward
```

Related Commands

This command has no related commands.

(config-pmap-lb-rtsp-c) serverfarm

To load balance a client request for content to a server farm, use the **serverfarm** command. Server farms are groups of networked real servers that contain the same content and reside in the same physical location. Use the **no** form of this command to remove the server-farm action from the Layer 7 load-balancing policy map.

serverfarm *name1* [**backup** *name2* [**aggregate-state**]]

no serverfarm *name1* [**backup** *name2* [**aggregate-state**]]

Syntax Description

name1	Unique identifier of the server farm. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
backup *name2*	(Optional) Specifies the identifier of an existing server farm that you want the ACE to use as a backup server farm. If the primary server farm goes down, the ACE sends all connections to the configured backup server farm. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
aggregate-state	This option has been deprecated and no longer has an effect on the state of the VIP. By default, the ACE takes into account the state of all real servers in the backup server farm before taking the VIP out of service. If all real servers in the primary server farm fail, but there is at least one real server in the backup server farm that is operational, the ACE keeps the VIP in service.

Command Modes

Policy map load balancing RTSP class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

If all servers in the server farm fail and you do not configure a backup server farm, the ACE sends a reset (RST) to a client in response to a content request.

If all real servers in the primary server farm fail, the ACE sends client requests to the backup server farm.

Examples

To specify the **serverfarm** command as an action in the load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance rtsp first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-rtsp)# class L7SLBCLASS
host1/Admin(config-pmap-lb-rtsp-c)# serverfarm FARM2 backup FARM3
```

Related Commands

This command has no related commands.

(config-pmap-lb-rtsp-c) set ip tos

To specify the IP differentiated services code point (DSCP) of packets in a server load balancing (SLB) policy map, use the **set ip tos** command. This command marks a packet by setting the IP DSCP bit in the Type of Service (ToS) byte. Once the IP DSCP bit is set, other Quality of Service (QoS) services can then operate on the bit settings. Use the **no** form of this command to reset the IP DSCP value to the default of 0.

set ip tos *value*

no set ip tos *value*

Syntax Description

value	IP DSCP value. Enter an integer from 0 to 255. The default is 0.

Command Modes

Policy map load balancing RTSP class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

For details about the ToS byte, see RFC 791, RFC 1122, RFC 1349, and RFC 3168.

Examples

The following example specifies the **set ip tos** command as a QoS action in the Layer 7 load-balancing policy map. All packets that satisfy the match criteria of L7SLBCLASS are marked with the IP DSCP value of 8. How packets marked with the IP DSCP value of 8 are treated is determined by the network configuration.

```
host1/Admin(config)# policy-map type loadbalance rtsp first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-rtsp)# class L7SLBCLASS
host1/Admin(config-pmap-lb-rtsp-c)# set ip tos 8
```

Related Commands

This command has no related commands.

(config-pmap-lb-rtsp-c) sticky-serverfarm

To specify that all requests that match a Layer 7 policy map are load balanced to a sticky server farm, use the **sticky-serverfarm** command. Use the **no** form of this command to remove a sticky group from the policy map.

sticky-serverfarm *name*

no sticky-serverfarm *name*

Syntax Description

name	Name of an existing sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Policy map load balancing RTSP class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

For information about sticky groups, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To specify that all requests that match a Layer 7 policy map are load balanced to a sticky server farm, enter:

```
host1/Admin(config)# policy-map type loadbalance rtsp first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-rtsp)# class L7SLBCLASS
host1/Admin(config-pmap-lb-rtsp-c)# sticky-serverfarm STICKY_GROUP1
```

Related Commands

This command has no related commands.

Policy Map Load Balancing RTSP Match Configuration Mode Commands

Policy map load balancing RTSP match configuration mode commands allow you to specify the actions that the ACE should take when network traffic matches the specified inline **match** command. To access policy map load balancing RTSP match configuration mode, use one of the **match** commands in policy map load balancing RTSP configuration mode (see the "Policy Map Load Balancing RTSP Configuration Mode Commands" section for details). The prompt changes to (config-pmap-lb-rtsp-m).

The inline Layer 7 policy map **match** commands allow you to include a single inline match criteria in the policy map without specifying a traffic class. The inline **match** commands function the same way as the Layer 7 server load balancing (SLB) class map **match** commands. However, when you use an inline **match** command, you can specify an action for only a single **match** command in the RTSP SLB policy map.

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

(config-pmap-lb-rtsp-m) drop

To instruct the ACE to discard packets that match a particular load-balancing criteria in an inline **match** command, use the **drop** command. Use the **no** form of this command to reset the ACE to its default of accepting packets from the policy map.

drop

no drop

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map load balancing RTSP match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to discard packets that match the load-balancing criteria in the inline **match** command, enter:

```
host1/Admin(config)# policy-map type loadbalance rtsp first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-rtsp)# match MATCH_SLB1 rtsp header Host header-value
.*cisco.com
host1/Admin(config-pmap-lb-rtsp-m)# drop
```

Related Commands

This command has no related commands.

(config-pmap-lb-rtsp-m) forward

To instruct the ACE to forward requests that match a particular policy map without performing load balancing on the request, use the **forward** command. Use the **no** form of this command to reset the ACE to its default of load balancing packets from the policy map.

forward

no forward

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map load balancing RTSP match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to forward requests that match the criteria in the inline **match** command without performing load balancing on the request, enter:

```
host1/Admin(config)# policy-map type loadbalance rtsp first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-rtsp)# match MATCH_SLB1 rtsp header Host header-value
.*cisco.com
host1/Admin(config-pmap-lb-rtsp-m)# forward
```

Related Commands

This command has no related commands.

(config-pmap-lb-rtsp-m) serverfarm

To load balance a client request for content to a server farm, use the **serverfarm** command. Server farms are groups of networked real servers that contain the same content and reside in the same physical location. Use the **no** form of this command to remove the server-farm action from the Layer 7 load balancing policy map.

serverfarm *name1* [**backup** *name2*] [**aggregate-state**]

no serverfarm *name1* [**backup** *name2*] [**aggregate-state**]

Syntax Description

name1	Unique identifier of the server farm. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
backup *name2*	(Optional) Specifies the identifier of an existing server farm that you want the ACE to use as a backup server farm. If the primary server farm goes down, the ACE sends all connections to the configured backup server farm. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
aggregate-state	This option has been deprecated and no longer has an effect on the state of the VIP. By default, the ACE takes into account the state of all real servers in the backup server farm before taking the VIP out of service. If all real servers in the primary server farm fail, but there is at least one real server in the backup server farm that is operational, the ACE keeps the VIP in service.

Command Modes

Policy map load balancing RTSP match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

If all servers in the server farm fail and you do not configure a backup server farm, the ACE sends a reset (RST) to a client in response to a content request.

If all real servers in the primary server farm fail, the ACE sends client requests to the backup server farm.

Examples

To specify the **serverfarm** command as an action in the load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance rtsp first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-rtsp)# match MATCH_SLB1 rtsp source-address 192.168.11.2
255.255.255.0
host1/Admin(config-pmap-lb-rtsp-m)# serverfarm FARM2 backup FARM3
```

Related Commands

This command has no related commands.

(config-pmap-lb-rtsp-m) set ip tos

To specify the IP differentiated services code point (DSCP) of packets in a server load balancing (SLB) policy map, use the **set ip tos** command. This command marks a packet by setting the IP DSCP bit in the Type of Service (ToS) byte. Once the IP DSCP bit is set, other Quality of Service (QoS) services can then operate on the bit settings. Use the **no** form of this command to reset the IP DSCP value to the default of 0.

set ip tos *value*

no set ip tos *value*

Syntax Description

value	IP DSCP value. Enter an integer from 0 to 255. The default is 0.

Command Modes

Policy map load balancing RTSP match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

For details about the ToS byte, see RFC 791, RFC 1122, RFC 1349, and RFC 3168.

Examples

To specify the **set ip tos** command as a QoS action in the Layer 7 load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance rtsp first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-rtsp)# match MATCH_SLB1 rtsp header Via header-value 192.*
host1/Admin(config-pmap-lb-rtsp-m)# set ip tos 8
```

Related Commands

This command has no related commands.

(config-pmap-lb-rtsp-m) sticky-serverfarm

To specify that all requests that match a Layer 7 policy map are load balanced to a sticky server farm, use the **sticky-serverfarm** command. Use the **no** form of this command to remove a sticky group from the policy map.

sticky-serverfarm *name*

no sticky-serverfarm *name*

Syntax Description

name	Name of an existing sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Policy map load balancing RTSP match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

For information about sticky groups, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To specify that all requests that match a Layer 7 policy map are load balanced to a sticky server farm, enter:

```
host1/Admin(config)# policy-map type loadbalance rtsp first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-rtsp)# match MATCH_SLB1 rtsp source-address 192.168.11.2
255.255.255.0
host1/Admin(config-pmap-lb-rtsp-m)# sticky-serverfarm STICKY_GROUP1
```

Related Commands

This command has no related commands.

Policy Map Load Balancing SIP Configuration Mode Commands

Policy map load balancing SIP configuration mode commands allow you to specify a SIP Layer 7 policy map for server load-balancing decisions. The ACE executes the specified action only against the first matching load-balancing classification.

To create a SIP Layer 7 server load balancing (SLB) policy map and access policy map load balancing SIP configuration mode, use the **policy-map type loadbalance sip first-match** command. When you access the policy map load balancing SIP configuration mode, the prompt changes to (config-pmap-lb-sip). Use the **no** form of this command to remove a SIP SLB policy map from the ACE.

policy-map type loadbalance sip first-match *map_name*

no policy-map type loadbalance sip first-match *map_name*

Syntax Description

map_name	Name assigned to the SIP SLB policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You associate the Layer 7 load balancing policy map with a Layer 3 and Layer 4 policy map to provide an entry point for the traffic classification. Layer 7 policy maps are considered to be child policies. Only a Layer 3 and Layer 4 policy map can be activated on a VLAN interface. A Layer 7 policy map cannot be directly applied on a VLAN (or any) interface.

To associate the Layer 7 load-balancing policy map, you nest it by using the Layer 3 and Layer 4 **(config-pmap-c) loadbalance policy** command.

Examples

To create a SIP SLB policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance sip first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-sip)#
```

Related Commands

show running-config
(config) policy-map

(config-pmap-lb-sip) class

To associate a Layer 7 server load balancing (SLB) class map with a Layer 7 SLB policy map, use the **class** command. The prompt changes from (config-pmap-lb-sip) to (config-pmap-lb-sip-c). For information about commands in this mode, see the "Policy Map Load Balancing SIP Class Configuration Mode Commands" section. Use the **no** form of this command to remove an associated class map from a policy map.

class {*name1* [**insert-before** *name2*] | **class-default**}

no class {*name1* [**insert-before** *name2*] | **class-default**}

Syntax Description

name1	Name of a previously defined Layer 7 SLB class map configured with the **class-map** command. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
insert-before *name2*	(Optional) Places the current named class map ahead of an existing class map or inline match condition specified by the *name2* argument in the policy map configuration. The ACE does not save the sequence reordering as part of the configuration.
class-default	Reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified under the **class class-default** command. The **class-default** class map has an implicit **match any** statement in it that enables it to match all traffic.

Command Modes

Policy map load balancing SIP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To associate a Layer 7 SLB class map with a Layer 7 SLB policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance sip first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-sip)# class L7LOADBALNCE_CLASS
host1/Admin(config-pmap-lb-sip-c)#
```

Related Commands

(config-pmap-lb-sip) description

(config-pmap-lb-sip) description

To provide a brief description of the SIP server load balancing (SLB) policy map, use the **description** command. Use the **no** form of this command to remove the description from the policy map.

description *text*

no description

Syntax Description

text	Description for the policy map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Policy map load balancing SIP configuration mode

Admin role in any user context

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description that the policy map is to perform server load balancing, enter:

```
host1/Admin(config)# policy-map type loadbalance sip first-match L7SLBPOLICY
host/Admin(config-pmap-lb-sip)# description SIP_LOAD_BALANCE_PROTOCOL
```

Related Commands

(config-pmap-lb-sip) class

(config-pmap-lb-sip) match sip header

To make server load balancing (SLB) decisions based on the name and value of a SIP header, use the **match sip header** command. The ACE performs regular expression matching against the received packet data from a particular connection based on the SIP header expression. Use the **no** form of this command to clear a SIP header match criteria from the policy map.

match *name* **sip header** *header_name* **header-value** *expression* [**insert-before** *map_name*]

no match *name* **sip header** *header_name* **header-value** *expression*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
header_name	Name of the field in the SIP header. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. You can enter a text string if you enclose the entire string in quotation marks (“ ”). You can enter any header field name, including a standard SIP header field name or any user-defined header field name. For a list of standard SIP header field names, see Table 2-7. Because SIP is similar in syntax and operation to HTTP/1.1, you can use any HTTP header listed in Table 2-6 if the SIP server supports it. For a complete list of SIP headers, see RFC 3261.
header-value *expression*	Specifies the expression string to compare against the value in the specified field in the SIP header. Enter a text string with a maximum of 255 alphanumeric characters. The ACE supports the use of regular expressions for header matching. Header expressions allow spaces if the entire string that contains spaces is quoted. For a list of the supported characters that you can use in regular expressions, see Table 2-16.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map load balancing SIP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

When you use the **match sip header** command, you access the policy map load balancing SIP match configuration mode and the prompt changes from (config-pmap-lb-sip) to (config-pmap-lb-sip-m). For information about commands in this mode, see the "Policy Map Load Balancing SIP Match Configuration Mode Commands" section.

The ACE supports regular expressions for matching. Expressions are stored in a header map in the form *header-name: expression*. Header expressions allow spaces if the spaces are escaped or quoted. For a list of supported characters that you can use in regular expressions, see Table 2-16.

Examples

To specify that the Layer 7 SLB policy map load balances on the standard SIP header Via, enter:

```
host1/Admin(config)# policy-map type loadbalance sip first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-sip)# match SIP_MATCH sip header Via header-value 192.*
host1/Admin(config-pmap-lb-sip-m)#
```

Related Commands

(config-cmap-sip-lb) match sip header

(config-pmap-lb-sip) match source-address

To specify a client source host IP address and subnet mask from which the ACE accepts traffic as the network traffic matching criteria, use the **match source-address** command. You configure the associated policy map to permit or restrict management traffic to the ACE from the specified source network or host. Use the **no** form of this command to clear the source IP address and subnet mask match criteria from the policy map.

match *name* **source-address** *ip_address mask* [**insert-before** *map_name*]

no match *name* **source-address** *ip_address mask*

Syntax Description

name	Name of the inline match condition. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
ip_address	Source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
mask	Subnet mask of the client entry in dotted-decimal notation (for example, 255.255.255.0).
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map load balancing SIP configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

When you use the **match source-address** command, you access the policy map load balancing SIP match configuration mode and the prompt changes from (config-pmap-lb-sip) to (config-pmap-lb-sip-m). For information about commands in this mode, see the "Policy Map Load Balancing SIP Match Configuration Mode Commands" section.

Examples

To specify that the Layer 7 SLB policy map matches on source IP address 192.168.10.1 255.255.0.0, enter:

```
host1/Admin(config)# policy-map type loadbalance sip first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-sip)# match match3 source-address 192.168.10.1 255.255.0.0
host1/Admin(config-pmap-lb-sip-m)#
```

Related Commands

(config-cmap-sip-lb) match source-address

Policy Map Load Balancing SIP Class Configuration Mode Commands

Policy map load balancing SIP class configuration mode commands allow you to specify the actions that the ACE should take when network traffic matches one or more match statements in the associated Layer 7 server load balancing (SLB) class map. To access policy map load balancing SIP class configuration mode, use the **class** command in policy map load balancing SIP configuration mode (see the **(config-pmap-lb-sip) class** command for details). The prompt changes to (config-pmap-lb-sip-c).

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

(config-pmap-lb-sip-c) drop

To instruct the ACE to discard packets that match a particular load-balancing criteria in the class map, use the **drop** command. Use the **no** form of this command to reset the ACE to its default of accepting packets from the policy map.

drop

no drop

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map load balancing SIP class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to discard packets that match the load-balancing criteria in the class map, enter:

```
host1/Admin(config)# policy-map type loadbalance sip first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-sip)# class L7SLBCLASS
host1/Admin(config-pmap-lb-sip-c)# drop
```

Related Commands

This command has no related commands.

(config-pmap-lb-sip-c) forward

To instruct the ACE to forward requests that match a particular policy map without performing load balancing on the request, use the **forward** command. Use the **no** form of this command to reset the ACE to its default of load balancing packets from the policy map.

forward

no forward

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map load balancing SIP class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to forward requests that match a particular policy map without performing load balancing on the request, enter:

```
host1/Admin(config)# policy-map type loadbalance sip first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-sip)# class L7SLBCLASS
host1/Admin(config-pmap-lb-sip-c)# forward
```

Related Commands

This command has no related commands.

(config-pmap-lb-sip-c) serverfarm

To load balance a client request for content to a server farm, use the **serverfarm** command. Server farms are groups of networked real servers that contain the same content and reside in the same physical location. Use the **no** form of this command to remove the server-farm action from the Layer 7 load-balancing policy map.

serverfarm *name1* [**backup** *name2* [**aggregate-state**]]

no serverfarm *name1* [**backup** *name2* [**aggregate-state**]]

Syntax Description

name1	Unique identifier of the server farm. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
backup *name2*	(Optional) Specifies the identifier of an existing server farm that you want the ACE to use as a backup server farm. If the primary server farm goes down, the ACE sends all connections to the configured backup server farm. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
aggregate-state	This option has been deprecated and no longer has an effect on the state of the VIP. By default, the ACE takes into account the state of all real servers in the backup server farm before taking the VIP out of service. If all real servers in the primary server farm fail, but there is at least one real server in the backup server farm that is operational, the ACE keeps the VIP in service.

Command Modes

Policy map load balancing SIP class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

If all servers in the server farm fail and you do not configure a backup server farm, the ACE sends a reset (RST) to a client in response to a content request.

If all real servers in the primary server farm fail, the ACE sends client requests to the backup server farm.

Examples

To specify the **serverfarm** command as an action in the load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance sip first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-sip)# class L7SLBCLASS
host1/Admin(config-pmap-lb-sip-c)# serverfarm FARM2 backup FARM3
```

Related Commands

This command has no related commands.

(config-pmap-lb-sip-c) set ip tos

To specify the IP differentiated services code point (DSCP) of packets in a server load balancing (SLB) policy map, use the **set ip tos** command. This command marks a packet by setting the IP DSCP bit in the Type of Service (ToS) byte. Once the IP DSCP bit is set, other Quality of Service (QoS) services can then operate on the bit settings. Use the **no** form of this command to reset the IP DSCP value to the default of 0.

set ip tos *value*

no set ip tos *value*

Syntax Description

value	IP DSCP value. Enter an integer from 0 to 255. The default is 0.

Command Modes

Policy map load balancing SIP class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

For details about the ToS byte, see RFC 791, RFC 1122, RFC 1349, and RFC 3168.

Examples

The following example specifies the **set ip tos** command as a QoS action in the Layer 7 load-balancing policy map. All packets that satisfy the match criteria of L7SLBCLASS are marked with the IP DSCP value of 8. How packets marked with the IP DSCP value of 8 are treated is determined by the network configuration.

```
host1/Admin(config)# policy-map type loadbalance sip first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-sip)# class L7SLBCLASS
host1/Admin(config-pmap-lb-sip-c)# set ip tos 8
```

Related Commands

This command has no related commands.

(config-pmap-lb-sip-c) sticky-serverfarm

To specify that all requests that match a Layer 7 policy map are load balanced to a sticky server farm, use the **sticky-serverfarm** command. Use the **no** form of this command to remove a sticky group from the policy map.

sticky-serverfarm *name*

no sticky-serverfarm *name*

Syntax Description

name	Name of an existing sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Policy map load balancing SIP class configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

For information about sticky groups, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To specify that all requests that match a Layer 7 policy map are load balanced to a sticky server farm, enter:

```
host1/Admin(config)# policy-map type loadbalance sip first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-sip)# class L7SLBCLASS
host1/Admin(config-pmap-lb-sip-c)# sticky-serverfarm STICKY_GROUP1
```

Related Commands

This command has no related commands.

Policy Map Load Balancing SIP Match Configuration Mode Commands

Policy map load balancing SIP match configuration mode commands allow you to specify the actions that the ACE should take when network traffic matches the specified inline **match** command. To access policy map load balancing SIP match configuration mode, use one of the **match** commands in policy map load balancing SIP configuration mode (see the "Policy Map Load Balancing SIP Configuration Mode Commands" section for details). The prompt changes to (config-pmap-lb-sip-m).

The inline Layer 7 policy map **match** commands allow you to include a single inline match criteria in the policy map without specifying a traffic class. The inline **match** commands function the same way as the Layer 7 server load balancing (SLB) class map **match** commands. However, when you use an inline **match** command, you can specify an action for only a single **match** command in the SLB policy map.

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

(config-pmap-lb-sip-m) drop

To instruct the ACE to discard packets that match a particular load-balancing criteria in an inline **match** command, use the **drop** command. Use the **no** form of this command to reset the ACE to its default of accepting packets from the policy map.

drop

no drop

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map load balancing SIP match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to discard packets that match the load-balancing criteria in the inline **match** command, enter:

```
host1/Admin(config)# policy-map type loadbalance sip first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-sip)# match SIP_MATCH sip header Via header-value 192.*
host1/Admin(config-pmap-lb-sip-m)# drop
```

Related Commands

This command has no related commands.

(config-pmap-lb-sip-m) forward

To instruct the ACE to forward requests that match a particular policy map without performing load balancing on the request, use the **forward** command. Use the **no** form of this command to reset the ACE to its default of load balancing packets from the policy map.

forward

no forward

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map load balancing SIP match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To instruct the ACE to forward requests that match the criteria in the inline **match** command without performing load balancing on the request, enter:

```
host1/Admin(config)# policy-map type loadbalance sip first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-sip)# match SIP_MATCH sip header Via header-value 192.*
host1/Admin(config-pmap-lb-sip-m)# forward
```

Related Commands

This command has no related commands.

(config-pmap-lb-sip-m) serverfarm

To load balance a client request for content to a server farm, use the **serverfarm** command. Server farms are groups of networked real servers that contain the same content and reside in the same physical location. Use the **no** form of this command to remove the server-farm action from the Layer 7 load balancing policy map.

serverfarm *name1* [**backup** *name2* [**aggregate-state**]]

no serverfarm *name1* [**backup** *name2* [**aggregate-state**]]

Syntax Description

name1	Unique identifier of the server farm. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
backup *name2*	(Optional) Specifies the identifier of an existing server farm that you want the ACE to use as a backup server farm. If the primary server farm goes down, the ACE sends all connections to the configured backup server farm. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
aggregate-state	This option has been deprecated and no longer has an effect on the state of the VIP. By default, the ACE takes into account the state of all real servers in the backup server farm before taking the VIP out of service. If all real servers in the primary server farm fail, but there is at least one real server in the backup server farm that is operational, the ACE keeps the VIP in service.

Command Modes

Policy map load balancing SIP match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

If all servers in the server farm fail and you do not configure a backup server farm, the ACE sends a reset (RST) to a client in response to a content request.

If all real servers in the primary server farm fail, the ACE sends client requests to the backup server farm.

Examples

To specify the **serverfarm** command as an action in the load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance sip first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-sip)# match MATCH_SLB1 source-address 192.168.11.2
255.255.255.0
host1/Admin(config-pmap-lb-sip-m)# serverfarm FARM2 backup FARM3
```

Related Commands

This command has no related commands.

(config-pmap-lb-sip-m) set ip tos

To specify the IP differentiated services code point (DSCP) of packets in a server load balancing (SLB) policy map, use the **set ip tos** command. This command marks a packet by setting the IP DSCP bit in the Type of Service (ToS) byte. Once the IP DSCP bit is set, other Quality of Service (QoS) services can then operate on the bit settings. Use the **no** form of this command to reset the IP DSCP value to the default of 0.

set ip tos *value*

no set ip tos *value*

Syntax Description

value	IP DSCP value. Enter an integer from 0 to 255. The default is 0.

Command Modes

Policy map load balancing SIP match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

For details about the ToS byte, see RFC 791, RFC 1122, RFC 1349, and RFC 3168.

Examples

To specify the **set ip tos** command as a QoS action in the Layer 7 load-balancing policy map, enter:

```
host1/Admin(config)# policy-map type loadbalance sip first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-sip)# match MATCH_SLB1 sip header Via header-value 192.*
host1/Admin(config-pmap-lb-sip-m)# set ip tos 8
```

Related Commands

This command has no related commands.

(config-pmap-lb-sip-m) sticky-serverfarm

To specify that all requests that match a Layer 7 policy map are load balanced to a sticky server farm, use the **sticky-serverfarm** command. Use the **no** form of this command to remove a sticky group from the policy map.

sticky-serverfarm *name*

no sticky-serverfarm *name*

Syntax Description

name	Name of an existing sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Policy map load balancing SIP match configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

For information about sticky groups, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To specify that all requests that match a Layer 7 policy map are load balanced to a sticky server farm, enter:

```
host1/Admin(config)# policy-map type loadbalance sip first-match L7SLBPOLICY
host1/Admin(config-pmap-lb-sip)# match MATCH_SLB1 source-address 192.168.11.2
255.255.255.0
host1/Admin(config-pmap-lb-sip-m)# sticky-serverfarm STICKY_GROUP1
```

Related Commands

This command has no related commands.

Policy Map Management Configuration Mode Commands

Policy map management configuration mode commands allow you to specify a Layer 3 and Layer 4 policy map that identifies the network management protocols that can be received by the ACE. The ACE executes the specified action only for traffic that meets the first matching classification with a policy map. The ACE does not execute any additional actions.

To create a Layer 3 and Layer 4 network management policy map and access the policy map management configuration mode, use the **policy-map type management first-match** command in configuration mode. You can classify network traffic based on the following management protocols: HTTP, HTTPS, ICMP, SNMP, SSH, or Telnet. When you access this mode, the prompt changes to (config-pmap-mgmt). Use the **no** form of this command to remove a Layer 3 and Layer 4 network management policy map from the ACE.

policy-map type management first-match *map_name*

no policy-map type management first-match *map_name*

Syntax Description

map_name	Name assigned to the Layer 3 and Layer 4 network management policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the context Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To create a Layer 3 and Layer 4 network traffic management policy map, enter:

```
host1/Admin(config)# policy-map type management first-match L4_REMOTE_MGMT_ALLOW_POLICY
host1/Admin(config-pmap-mgmt)#
```

Related Commands

(config) class-map

(config-pmap-mgmt) class

To associate a Layer 3 and Layer 4 management protocol class map with a Layer 3 and Layer 4 traffic management policy map, use the **class** command. The prompt changes from (config-pmap-mgmt) to (config-pmap-mgmt-c). For information about commands in this mode, see the "Policy Map Management Class Configuration Mode Commands" section. Use the **no** form of this command to remove an associated class map from a policy map.

class {*name1* [**insert-before** *name2*] | **class-default**}

no class {*name1* [**insert-before** *name2*] | **class-default**}

Syntax Description

name1	Name of a previously defined Layer 3 and Layer 4 management protocol class map configured with the **class-map** command. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
insert-before *name2*	(Optional) Places the current class map ahead of an existing class map or inline match condition specified by the *name2* argument in the policy map configuration. The ACE does not save the sequence reordering as part of the configuration. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
class-default	Reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified under the **class class-default** command. The **class-default** class map has an implicit **match any** statement in it enabling it to match all traffic.

Command Modes

Management policy map configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To permit remote Secure Shell (SSH) access, enter:

```
host1/Admin(config)# policy-map type management first-match L4_REMOTE_MGMT_ALLOW_POLICY
host1/Admin(config-pmap-mgmt)# class SSH-ALLOW_CLASS
```

Related Commands

(config) class-map
(config-pmap-mgmt) description

(config-pmap-mgmt) description

To provide a brief summary about the Layer 3 and Layer 4 management protocol policy map, use the **description** command. Use the **no** form of this command to remove the description from the class map.

description *text*

no description

Syntax Description

text	Description for the policy map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Policy map configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description that the policy map is to allow remote Telnet access, enter:

```
host1/Admin(config-pmap-mgmt)# description Allow Telnet access to the ACE
```

Related Commands

(config-pmap-mgmt) class

Policy Map Management Class Configuration Mode Commands

Policy map management class configuration mode commands allow you to specify the actions that the ACE should take when network traffic matches one or more match statements in the associated Layer 3 and Layer 4 network management protocol class map. To access policy map management class configuration mode, use the **class** command in policy map management configuration mode (see the **(config-pmap-mgmt) class** command for details). The prompt changes from (config-pmap-mgmt) to (config-pmap-mgmt-c).

The commands in this mode require the context Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

(config-pmap-mgmt-c) deny

To deny the specified IP network management protocol, use the **deny** command. Use the **no** form of this command to allow the specified IP network management protocol to be received by the ACE.

deny

no deny

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map management class configuration mode

Admin and user contexts

Command History

Release	Modification
3.0(0)A1(2)	This command was introduced.

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To deny the specified IP network management protocol by the ACE, enter:

```
host1/Admin(config-pmap-mgmt)# class SSH_CLASS
host1/Admin(config-pmap-mgmt-c)# deny
```

Related Commands

This command has no related commands.

(config-pmap-mgmt-c) permit

To allow the IP network management protocols listed in the associated Layer 3 and Layer 4 management class map to be received by the ACE, use the **permit** command. Use the **no** form of this command to disallow the specified IP network management protocols to be received by the ACE.

permit

no permit

Syntax Description

This command has no keywords or arguments.

Command Modes

Policy map management class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To permit the specified IP network management protocol by the ACE, enter:

```
host1/Admin(config-pmap-mgmt)# class SSH_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
```

Related Commands

This command has no related commands.

Policy Map Optimization Configuration Mode Commands

Policy map optimization configuration mode commands allow you to associate an HTTP optimization action list and, optionally, a parameter map to perform the specified application acceleration optimization actions. The ACE executes the specified action only for traffic that meets the first matching classification with a policy map. The ACE does not execute any additional actions.

To create a Layer 7 optimization policy map and access the policy map optimization configuration mode, use the **policy-map type optimization http first-match** command in configuration mode. When you access this mode, the prompt changes to (config-pmap-optmz). Use the **no** form of the command to remove a Layer 3 and Layer 4 network management policy map from the ACE.

policy-map type optimization http first-match *map_name*

no policy-map type optimization http first-match *map_name*

Syntax Description

map_name	Name assigned to the Layer 7 optimization HTTP policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To create a Layer 7 optimization HTTP policy map named L7OPTIMIZATION_POLICY, enter:

```
host/Admin(config)# policy-map type optimization http first-match L7OPTIMIZATION_POLICY
host/Admin(config-pmap-optmz)#
```

Related Commands

(config) class-map

(config-pmap-optmz) class

To associate a Layer 7 SLB class map with a Layer 7 optimization HTTP policy map, use the **class** command. The prompt changes from (config-pmap-optmz) to (config-pmap-optmz-c). For information on commands in this mode, see the "Policy Map Optimization Class Configuration Mode Commands" section. Use the **no** form of this command to remove an associated class map from a policy map.

class {*name1* [**insert-before** *name2*] | **class-default**}

no class {*name1* [**insert-before** *name2*] | **class-default**}

Syntax Description

name1	Name of a previously defined Layer 7 SLB class map configured with the **class-map** command. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
insert-before *name2*	(Optional) Places the current class map ahead of an existing class map or inline match condition specified by the *name2* argument in the policy map configuration. The ACE does not save the sequence reordering as part of the configuration. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
class-default	Reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified under the **class class-default** command. The **class-default** class map has an implicit **match any** statement in it that enables it to match all traffic.

Command Modes

Policy map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To specify an existing Layer SLB class map, enter:

```
host1/Admin(config-pmap-optmz)# class L7SLBCLASS
host1/Admin(config-pmap-optmz-c)#
```

Related Commands

(config) class-map
(config-pmap-optmz) description

(config-pmap-optmz) description

To provide a brief summary about the Layer 7 optimization HTTP policy map, use the **description** command. Use the **no** form of the command to remove the description from the class map.

description *text*

no description

Syntax Description

text	Description for the policy map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Policy map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description that the policy map is to perform delta optimization, enter:

```
host1/Admin(config-pmap-optmz)# description This policy map performs delta optimization
```

To remove the description from the policy map, enter:

```
host1/Admin(config-pmap-optmz)# no description
```

Related Commands

(config-pmap-mgmt) class

(config-pmap-optmz) match http cookie

To make server load balancing (SLB) decisions based on the name and string of a cookie, use the **match http cookie** command. Use the **no** form of the command to remove an HTTP cookie match statement from the policy map.

match *name1* **http cookie** {*name2* | **secondary** *name3*} **cookie-value** *expression* [**insert-before** *map_name*]

no match *name1* **http cookie** {*name2* | **secondary** *name3*} **cookie-value** *expression*

Syntax Description

name1	Name assigned to the inline **match** command. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
name2	A unique cookie name. Enter an unquoted text string with no spaces and a maximum of 63 alphanumeric characters.
secondary *name3*	Specifies a cookie in a URL string. You can specify the delimiters for cookies in a URL string using a command in an HTTP parameter map.
cookie-value *expression*	Specifies a unique cookie value expression. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. For a list of supported characters that you can use for matching string expressions, see the "Usage Guidelines" section for the **(config-pmap-ins-http) match content** command.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

When you use the **match http cookie** command, you access the policy map optimization match configuration mode and the prompt changes from (config-pmap-optmz) to (v-m). For information on the load-balancing commands in this mode, see the "Policy Map Load Balancing HTTP Match Configuration Mode Commands" section.

The ACE performs regular expression matching against the received packet data from a particular connection based on the cookie expression. You can configure a maximum of five cookie names per VIP.

The ACE supports regular expressions for matching string expressions. For a list of supported characters that you can use for matching string expressions, see the "Usage Guidelines" section for the **(config-pmap-ins-http) match content** command.

For details on defining a list of ASCII-character delimiter strings that you can use to separate the cookies in a URL string, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To specify that the Layer 7 optimization policy map load balances on a cookie with the name of testcookie1, enter:

```
host/Admin(config)# policy-map type optimization http first-match L7OPTIMIZATION_POLICY
host/Admin(config-pmap-optmz)# match MATCH2 http cookie testcookie1 cookie-value 123456
```

Related Commands

(config-parammap-http) set content-maxparse-length
(config-parammap-http) set secondary-cookie-delimiters

(config-pmap-optmz) match http header

To define application inspection decisions based on the name and value in an HTTP header, use the **match http header** command. Use the **no** form of the command to clear an HTTP header match criteria from the policy map.

match *name* **http header** {*header_name* | *header_field*} **header-value** *expression* [**insert-before** *map_name*]

no match *name* **http header** {*header_name* | *header_field*} **header-value** *expression*

Syntax Description

name	Name assigned to the inline **match** command. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
header_name	Name of the HTTP header to match (for example, www.example1.com.) The range is from 1 to 64 alphanumeric characters. **Note** The *header_name* argument cannot include the colon in the name of the HTTP header; the ACE rejects the colon as an invalid token.
header_field	A standard HTTP/1.1 header field. Valid selections include request-header fields, general-header fields, and the entity-header field. Selections also include two lower-level header-matching commands: "length" and "mime-type." The supported selections are the following: • **Accept**—Specifies a semicolon-separated list of representation schemes (content type metainformation values) that will be accepted in the response to the request.

- **Accept-Charset**—Specifies the character sets that are acceptable for the response. This field allows clients capable of understanding more comprehensive or special-purpose character sets to signal that capability to a server that can represent documents in those character sets.
- **Accept-Encoding**—Restricts the content encoding that a user will accept from the server.
- **Accept-Language**—Specifies the ISO code for the language in which the document is written. The language code is an ISO 3316 language code with an optional ISO639 country code to specify a national variant.
- **Authorization**—Specifies that the user agent wants to authenticate itself with a server, usually after receiving a 401 response.
- **Cache-Control**—Specifies the irectives that must be obeyed by all caching mechanisms in the request/response chain. The directives specify behavior intended to prevent caches from adversely interfering with the request or response.
- **Connection**—Allows the sender to specify connection options.
- **Content-MD5**—Specifies the MD5 digest of the entity body that provides an end-to-end integrity check. Only a client or an origin server can generate this header field.
- **Expect**—Used by a client to inform the server about the behaviors that the client requires.
- **From**—Contains the e-mail address of the person who controls the requesting user agent.
- **Host**—Specifies the internet host and port number of the resource that is requested, as obtained from the original URI given by the user or referring resource. The Host field value must represent the naming authority of the origin server or gateway given by the original URL.
- **If-Match**—Used with a method to make it conditional. A client that has one or more entities previously obtained from the resource can verify that one of those entities is current by including a list of their associated entity tags in the If-Match header field. This feature allows efficient updates of cached information with a minimum amount of transaction overhead. It is also used on updating requests to prevent inadvertent modification of the wrong version of a resource. As a special case, the value "*" matches any current entity of the resource.
- **Pragma**—Specifies the pragma directives that are understood by servers to whom the directives are relevant. The syntax is the same as for other multiple-value fields in HTTP. For example, the Accept field is a comma-separated list of entries for which the optional parameters are separated by semicolons.

	• **Referer**—Specifies the address (URI) of the resource from which the URI in the request was obtained. • **Transfer-Encoding**—Indicates what (if any) type of transformation has been applied to the message body in order to safely transfer it between the sender and the recipient. • **User-Agent**—Specifies the information about the user agent (for example, a software program that originates the request). This information is for statistical purposes, the tracing of protocol violations, and automated recognition of user agents. • **Via**—Used by gateways and proxies to indicate the intermediate protocols and recipients between the user agent and the server on requests and between the origin server and the client on responses.
header-value *expression*	Specifies the header value expression string to compare against the value in the specified field in the HTTP header. The range is from 1 to 255 alphanumeric characters. For a list of supported characters that you can use in regular expressions, see the "Usage Guidelines" section for the **(config-pmap-ins-http) match content** command.
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The ACE performs regular expression matching against the received packet data from a particular connection based on the HTTP header expression.

When you use the **match http header** command, you access the policy map optimization match configuration mode and the prompt changes from (config-pmap-optmz) to (config-pmap-optmz-m). For information on the load-balancing commands in this mode, see the "Policy Map Load Balancing HTTP Match Configuration Mode Commands" section.

The ACE supports regular expressions for matching. Expressions are stored in a header map in the form *header-name: expression*. Header expressions allow spaces, if the spaces are escaped or quoted. For a list of supported characters that you can use in regular expressions, see the "Usage Guidelines" section for the **(config-pmap-ins-http) match content** command.

Examples

To specify that the Layer 7 optimization policy map load balances on an HTTP header named Host, enter:

```
host/Admin(config)# policy-map type optimization http first-match L7OPTIMIZATION_POLICY
host1/Admin(config-pmap-optmz)# match match3 http header Host header-value .*cisco.com
```

Related Commands

(config-parammap-http) set content-maxparse-length

(config-pmap-optmz) match http url

To make server load balancing (SLB) decisions based on the URL name and, optionally, the HTTP method, use the **match http url** command. Use the **no** form of the command to remove a URL match statement from the policy map.

match *name* **http url** *expression* [**method** *name*] [**insert-before** *map_name*]

no match *name* **http url** *expression* [**method** *name*]

Syntax Description

name	Name assigned to the inline **match** command. Enter an unquoted text string with no spaces. The length of the inline match statement name plus the length of the policy map name with which it is associated cannot exceed a total maximum of 64 alphanumeric characters. For example, if the policy map name is L7_POLICY (nine characters), an inline match statement name under this policy cannot exceed 55 alphanumeric characters (64 - 9 = 55).
expression	URL, or portion of a URL, to match. Enter a URL string from 1 to 255 alphanumeric characters. Include only the portion of the URL that follows www.*hostname*.*domain* in the match statement. For a list of supported characters that you can use in regular expressions, see the "Usage Guidelines" section for the **(config-pmap-ins-http) match content** command.
method *name*	(Optional) Specifies the HTTP method to match. Enter a method name as an unquoted text string with no spaces and a maximum of 15 alphanumeric characters. The method can either be one of the standard HTTP 1.1 method names (OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, or CONNECT) or a text string that must be matched exactly (for example, PROTOPLASM).
insert-before *map_name*	(Optional) Places the inline **match** command ahead of an existing class map in the policy map configuration.

Command Modes

Policy map optimization configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The ACE performs regular expression matching against the received packet data from a particular connection based on the HTTP URL string.

When you use the **match http url** command, you access the policy map optimization match configuration mode and the prompt changes from (config-pmap-optmz) to (config-pmap-optmz-m). For information on the load-balancing commands in this mode, see the "Policy Map Load Balancing HTTP Match Configuration Mode Commands" section.

Include only the portion of the URL that follows www.*hostname.domain* in the match statement. For example, in the URL www.anydomain.com/latest/whatsnew.html, include only /latest/whatsnew.html. To match the www.anydomain.com portion, the URL string can take the form of a URL regular expression. For a list of supported characters that you can use in regular expressions, see the "Usage Guidelines" section for the **(config-pmap-ins-http) match content** command.

The period (.) does not have a literal meaning in regular expressions. Use either brackets ([]) or the backslash (\) character to match this symbol. For example, specify www[.]xyz[.]com instead of www.xyz.com.

Examples

To specify that the Layer 7 optimization policy map load balances on a specific URL, enter:

```
host/Admin(config)# policy-map type optimization http first-match L7OPTIMIZATION_POLICY
host1/Admin(config-pmap-optmz)# match match3 http url whatsnew/latest.*
```

To use regular expressions to emulate a wildcard search to match on any .gif file, enter:

```
host/Admin(config)# policy-map type optimization http first-match L7OPTIMIZATION_POLICY
host1/Admin(config-pmap-optmz)# match match3 http url .*.gif
```

Related Commands

(config-parammap-http) set content-maxparse-length

Policy Map Optimization Class Configuration Mode Commands

Policy map optimization class configuration mode commands allow you to specify the actions that the ACE should take when network traffic matches the Layer 7 optimization HTTP action statement. To access policy map optimization class configuration mode, use the **class** command in policy map optimization configuration mode (see the **(config-pmap-optmz) class** command for details). The prompt changes from (config-pmap-optmz) to (config-pmap-optmz-c).

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

(config-pmap-optmz-c) action

To perform a specific set of application acceleration actions, use the **action** command. The Layer 7 optimization HTTP policy map activates the use of an optimization HTTP action list to configure the specified application acceleration and optimization actions. See *Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide* for details on creating an optimization HTTP action list. Use the **no** form of the command to remove the action list from the policy map.

action *list_name* [**parameter** *map_name*]

no action *list_name* [**parameter** *map_name*]

Syntax Description

list_name	Unique name of an existing action list as an unquoted text string with a maximum of 64 alphanumeric characters. The **action** command groups the application acceleration functions associated with the specified action list that apply to a specific type of operation.
parameter *map_name*	(Optional) Specifies optimization-related commands that pertain to application acceleration performed by the ACE. A parameter map groups the application acceleration functions that adjust or control the actions specified in an associated action list. The *map_name* argument specifies a unique name of an existing parameter map as an unquoted text string with a maximum of 64 alphanumeric characters.

Command Modes

Policy map optimization class configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Optionally, you can specify an optimization HTTP parameter list in an optimization HTTP policy map to identify the association between the action list and the parameter map. The optimization HTTP action list defines what to do while the optimization HTTP parameter map defines the specific details about how to accomplish the application acceleration action. Refer to *Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide* for details on creating an optimization HTTP parameter map.

Examples

To associate an existing action list with an existing parameter map to control the actions in the Layer 7 HTTP optimization policy map, enter:

```
host/Admin(config)# policy-map type optimization http first-match L7OPTIMIZATION_POLICY
host1/Admin(config-pmap-optmz)# class L7SLBCLASS
host1/Admin(config-pmap-optmz-c)# action ACT_LIST1 parameter OPTIMIZE_PARAM_MAP
```

To remove the action list from the Layer 7 HTTP optimization policy map, enter:

```
host1/Admin(config-pmap-optmz-c)# no action ACT_LIST1 parameter OPTIMIZE_PARAM_MAP
```

Related Commands

(config) action-list type modify http
(config) parameter-map type

Policy Map Optimization Match Configuration Mode Commands

Policy map optimization match configuration mode commands allow you to specify the actions that the ACE should take when network traffic matches the Layer 7 optimization HTTP action statement. To access policy map optimization match configuration mode, use a **match** command in policy map optimization configuration mode (see the "Policy Map Optimization Match Configuration Mode Commands" section). The prompt changes from (config-pmap-optmz) to (config-pmap-optmz-m).

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

(config-pmap-optmz-m) action

To perform a specific set of application acceleration actions, use the **action** command. The Layer 7 optimization HTTP policy map activates the use of an optimization HTTP action list to configure the specified application acceleration optimization actions. Refer to the *Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide* for details on creating an optimization HTTP action list. Use the **no** form of the command to remove the action list from the policy map.

action *list_name* [**parameter** *map_name*]

no action *list_name* [**parameter** *map_name*]

Syntax Description

list_name	Unique name of an existing action list as an unquoted text string with a maximum of 64 alphanumeric characters. The **action** command groups the application acceleration functions associated with the specified action list that apply to a specific type of operation.
parameter *map_name*	(Optional) Specifies optimization-related commands that pertain to application acceleration performed by the ACE. A parameter map groups the application acceleration functions that adjust or control the actions specified in an associated action list. The *map_name* argument specifies a unique name of an existing parameter map as an unquoted text string with a maximum of 64 alphanumeric characters.

Command Modes

Policy map optimization match configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Optionally, you can specify an optimization HTTP parameter list in an optimization HTTP policy map to identify the association between the action list and the parameter map. In this case, the optimization HTTP action list defines what to do while the optimization HTTP parameter map defines the specific details about how to accomplish the application acceleration action. Refer to the *Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide* for details on creating an optimization HTTP parameter map.

Examples

To associate an existing action list with an existing parameter map to control the **match** command action in the Layer 7 HTTP optimization policy map, enter:

```
host/Admin(config)# policy-map type optimization http first-match L7OPTIMIZATION_POLICY
host1/Admin(config-pmap-optmz)# match match3 http url .*.gif
host1/Admin(config-pmap-optmz-m)# action ACT_LIST1 parameter OPTIMIZE_PARAM_MAP
```

To remove the action list from the Layer 7 HTTP optimization policy map, enter:

```
host1/Admin(config-pmap-optmz-m)# no action ACT_LIST1 parameter OPTIMIZE_PARAM_MAP
```

Related Commands

(config) action-list type modify http
(config) parameter-map type

Probe Configuration Mode Commands

Probe configuration mode commands allow you to configure health monitoring on the ACE to track the state of a server by sending out probes. Also referred to as out-of-band health monitoring, the ACE verifies the server response or checks for any network problems that can prevent a client from reaching a server. Based on the server response, the ACE can place the server in or out of service and can make reliable load-balancing decisions. You can also use health monitoring to detect failures for a gateway or host in high availability configurations. The ACE identifies the health of a server in the following categories:

- Passed—The server returns a valid response.
- Failed—The server fails to provide a valid response to the ACE or the ACE is unable to reach a server for a specified number of retries.

The ACE supports 4000 unique probe configurations and 256 scripted probes. The ACE also allows the opening of 1000 sockets simultaneously.

You can associate the same probe with multiple real servers or server farms. Each time that you use the same probe again, the ACE counts it as another probe instance. You can allocate a maximum of 16384 probe instances.

To configure probes and access probe configuration mode for that probe type, use the **probe** command. The CLI prompt changes to (config-probe-*probe_type*). For information about the commands in all probe configuration modes, see the commands in this section. See the "Command Modes" section for each command to find out to which probe-type configuration modes a specific command applies.

Use the **no** form of this command to remove a probe from the configuration.

probe *probe_type probe_name*

no probe *probe_type probe_name*

Syntax Description

probe_type	Type of probe to configure. The probe type determines what the probe sends to the server. Enter one of the following types: • **dns**—Sends a request to a DNS server that passes a configured domain to the server (by default, the domain is www.cisco.com). To determine whether the server is up, the ACE must receive one of the configured IP addresses for that domain. • **echo** {**tcp** | **udp**}—Sends a specified string to the server and compares the response to the original string. You must configure the string that needs to be echoed. If the response string matches the original string, the server is marked as passed. If you do not configure a string, the probe behaves like a TCP or UDP probe. • **finger**—Uses a Finger query to a server for an expected response string. The ACE searches the response for the configured string. If the ACE finds the expected response string, the server is marked as passed. If you do not configure an expected response string, the ACE ignores the server response. • **ftp** —Establishes a TCP connection to the server and then issues a **quit** command.

- **http**—Establishes a TCP connection and issues an HTTP request to the server for an expected string and status code. The ACE can compare the received response with configured codes, looking for a configured string in the received HTTP page, or verifying hash for the HTTP page. If any of these checks fail, the server is marked as failed.

  For example, if you configure an expected string and status code and the ACE finds them both in the server response, the server is marked as passed. However, if the ACE does not receive either the server response string or the expected status code, it marks the server as failed.

  If you do not configure a status code, any response code from the server is marked as failed.
- **https**—Similar to an HTTP probe except that it uses Secure Sockets Layer (SSL) to generate encrypted data.
- **icmp**—Sends an ICMP echo request and listens for a response. If a server returns a response, the ACE marks the server as passed. If the server does not send a response, causing the probe to time out, or if the server sends an unexpected ICMP echo response type, the ACE marks the probe as failed.
- **imap**—Makes a server connection and sends user credential (login, password, and mailbox) information. The ACE can send a configured command. Based on the server response, the ACE marks the probe as passed or failed.
- **pop**—Initiates a session and sends the configured credentials. The ACE can send a configured command. Based on the server response, the ACE marks the probe as passed or failed.
- **radius**—Sends a query using a configured username, password, and shared secret to a RADIUS server. If the server is up, it is marked as passed. If you configure a Network Access Server (NAS) address, the ACE uses it in the outgoing packet. Otherwise, the ACE uses the IP address associated with the outgoing interface as the NAS address.
- **rtsp**—Establishes a TCP connection and sends a request packet to the server. The ACE compares the response with the configured response code to determine whether the probe has succeeded.
- **scripted**—Allows you to run a script to execute the probe that you created for health monitoring. You can author specific scripts with features not present in standard health probes.
- **sip** {**tcp** | **udp**}—Establishes a TCP or UDP connection and sends an OPTIONS request packet to the user agent on the server. The ACE compares the response with the configured response code or expected string, or both, to determine whether the probe has succeeded. If you do not configure an expected status code, any response from the server is marked as failed.
- **smtp**—Initiates an SMTP session by logging into the server, sends a HELLO message, and then disconnects from the server.

	• **snmp**—Establishes a UDP connection and sends a maximum of eight SMNP OID queries to probe the server. The ACE weighs and averages the load information that is retrieved and uses it as input to the least-loaded algorithm for load-balancing decisions. If the retrieved value is within the configured threshold, the server is marked as passed. If the threshold is exceeded, the server is marked as failed. • **tcp**—Initiates a TCP 3-way handshake (SYN, SYN-ACK, ACK) and expects the server to send a response. By default, a successful response causes the probe to mark the server as passed and send a FIN to end the session. If the response is not valid or if there is no response, the probe marks the server as failed. • **telnet**—Establishes a connection to the server and verifies that a greeting from the application was received. • **udp**—Sends a UDP packet to a server and marks the server as failed only if the server returns an ICMP Port Unreachable message. If the ACE does not receive any ICMP errors for the UDP request that was sent, the probe is marked as passed. Optionally, you can configure this probe to send specific data and expect a specific response to mark the server as passed. If the IP interface of the server is down or disconnected, the UDP probe by itself would not know that the UDP application is not reachable.
probe_name	Identifier for the probe. Use the probe name to associate the probe to the server. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised.

Usage Guidelines

This command requires the probe feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To define a TCP probe named PROBE, and access its mode, enter:

```
host1/Admin(config)# probe tcp PROBE1
host1/Admin(config-probe-tcp)#
```

To delete the TCP probe named PROBE1 for TCP and access its mode, enter:

```
host1/Admin(config)# probe tcp PROBE1
```

Related Commands

clear stats
show probe
show running-config
show stats

(config-probe-*probe_type*) community

To change the community string used by an SNMP probe, use the **community** command. Use the **no** form of this command to remove the community string.

community *text*

no community

Syntax Description

text	Name of the SNMP community string for the server. Enter a text string with a maximum of 255 alphanumeric characters.

Command Modes

SNMP probe configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was revised.

Usage Guidelines

An ACE Simple Network Management Protocol (SNMP) probe accesses the server through its community string. By default, the community string is not set.

Examples

To configure the private community string, enter:

```
host1/Admin(config-probe-snmp)# community private
```

To reset the community string to its default value of public, enter:

```
host1/Admin(config-probe-snmp)# no community
```

Related Commands

show probe

(config-probe-*probe_type*) connection term

To configure the ACE to terminate a TCP connection by sending a RST, use the **connection term** command. Use the **no** form of this command to reset its default of graceful termination.

connection term forced

no connection term forced

Syntax Description

This command has no keywords or arguments.

Command Modes

ECHO TCP, Finger, FTP, HTTP, HTTPS, IMAP, POP, RTSP, SIP TCP, SMTP, TCP, and Telnet probe configuration modes

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

This command applies only to TCP-based probes. By default, the ACE terminates a TCP connection gracefully by sending a FIN to the server.

Examples

To terminate a TCP connection by sending a RST for a TCP probe, enter:

```
host1/Admin(config-probe-tcp)# connection term forced
```

To reset the method to terminate a connection gracefully, enter:

```
host1/Admin(config-probe-tcp)# no connection term forced
```

Related Commands

show probe

(config-probe-*probe_type*) credentials

To configure the credentials for username and password authentication of a probe to access a server, use the **credentials** command. For a Remote Authentication Dial-In User Service (RADIUS) probe, a shared secret may also be required. For an Internet Message Access Protocol (IMAP) probe, you can provide a mailbox username. Use the **no** form of this command to remove the credentials from the configuration.

For HTTP, HTTPS, and POP probes, the syntax is as follows:

credentials *username* [*password*]

For RADIUS probes, the syntax is as follows:

credentials *username password* [**secret** *shared_secret*]

For IMAP probes, the syntax is as follows:

credentials {*username password*} | {**mailbox** *name*}

For HTTP, HTTPS, POP, and RADIUS probes, the syntax is as follows:

no credentials

For IMAP probes, the syntax is as follows:

no credentials {*username* | **mailbox**}

Syntax Description

username	User identifier used for authentication. Enter an unquoted text string with a maximum of 64 alphanumeric characters.
password	(Optional except for RADIUS and IMAP probes) Password used for authentication. Enter an unquoted text string with a maximum of 64 alphanumeric characters.
mailbox *name*	(IMAP probe) Specifies the user mailbox name from which to retrieve e-mail for an IMAP probe. Enter an unquoted text string with a maximum of 64 alphanumeric characters.
secret *shared_secret*	(RADIUS probe) Specifies the password used for the MD5 hash encryption algorithm. Enter an unquoted text string with a maximum of 64 alphanumeric characters.

Command Modes

HTTP, HTTPS, IMAP, POP, and RADIUS probe configuration modes

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

You must configure the credentials for an IMAP probe using the **credentials** command before you configure the mailbox or the ACE will ignore the specified user mailbox name.

Examples

To configure the username ENG1 and a password TEST for an HTTP probe, enter:

```
host1/Admin(config-probe-http)# credentials ENG1 TEST
```

To delete the credentials for a probe, enter:

```
host1/Admin(config-probe-http)# no credentials
```

To configure the user mailbox LETTERS for an IMAP probe, enter:

```
host1/Admin(config-probe-imap)# credentials mailbox LETTERS
```

To delete the mailbox for the IMAP probe, enter:

```
host1/Admin(config-probe-imap)# no credentials mailbox
```

Related Commands show probe

(config-probe-*probe_type*) description

To provide a description for a probe, use the **description** command. Use the **no** form of this command to remove the description for the probe.

description *text*

no description

Syntax Description

text	Description for the probe. Enter a text string with a maximum of 240 alphanumeric characters.

Command Modes

All probe-type configuration modes

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

This command has no usage guidelines.

Examples

To configure a description THIS PROBE IS FOR TCP SERVERS for a TCP probe, enter:

```
host1/Admin(config-probe-tcp)# description THIS PROBE IS FOR TCP SERVERS
```

To remove the description THIS PROBE IS FOR TCP SERVERS for a TCP probe, enter:

```
host1/Admin(config-probe-tcp)# no description
```

Related Commands show probe

(config-probe-*probe_type*) domain

To configure the domain name that the probe sends to the DNS server to resolve, use the **domain** command. Use the **no** form of this command to reset the default domain (www.cisco.com) that the probe sends to the server.

domain *name*

no domain

Syntax Description

name	Domain that the probe sends to the DNS server. Enter an unquoted text string with a maximum of 255 alphanumeric characters.

Command Modes

DNS probe configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

The DNS probe sends a domain name for the DNS server to resolve. By default, the probe uses the www.cisco.com domain name.

Examples

To configure the domain name of MARKET, enter:

```
host1/Admin(config-probe-dns)# domain MARKET
```

To reset the default domain that the probe sends to the DNS server, enter:

```
host1/Admin(config-probe-dns)# no domain
```

Related Commands

show probe

(config-probe-*probe_type*) expect address

To configure one or more IP addresses that the ACE expects as a server response to a DNS request, use the **expect address** command. The probe matches the received IP address with the configured addresses. Use the **no** form of this command to remove the expected IP address from the configuration.

expect address *ip_address*

no expect address *ip_address*

Syntax Description

ip_address	IP address expected from the DNS server in response to the DNS probe request for a domain. Enter a unique IPv4 address in dotted-decimal notation (for example, 192.168.12.15).

Command Modes

DNS probe configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

A DNS probe sends a request for a domain to a DNS server. The ACE uses the IP address specified in the **expect address** command to decide whether to pass or fail the DNS probe for the server based on the server response. You can specify multiple IP addresses with this command by entering the command with a different address separately.

Examples

To configure expected IP addresses of 192.8.12.15 and 192.8.12.23, enter:

```
host1/Admin(config-probe-dns)# expect address 192.8.12.15
host1/Admin(config-probe-dns)# expect address 192.8.12.23
```

To remove an IP address, enter:

```
host1/Admin(config-probe-dns)# no expect address 192.168.12.15
```

Related Commands

show probe

(config-probe-*probe_type*) expect regex

To configure what the ACE expects as a response from the probe destination server, use the **expect regex** command. Use the **no** form of this command to remove the expectation of a response expression.

expect regex *string* [**offset** *number*]

For TCP and UDP probes, the syntax is as follows:

no expect

For Finger, HTTP, HTTPS, and SIP probes, the syntax is as follows:

no expect regex

Syntax Description

string	Expected response string from the probe destination. Enter an unquoted text string with no spaces. If the string includes spaces, enclose the string in quotes. The string can be a maximum of 255 alphanumeric characters.
offset *number*	(Optional) Sets the number of characters into the received message or buffer where the probe starts searching for the defined expression. Enter a number from 1 to 4000.

Command Modes

Finger, HTTP, HTTPS, SIP, TCP, and UDP probe configuration modes

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

When you configure a probe to expect a string from a server, it searches the response for a configured string. If the ACE finds the expected string, the server is marked as passed. If you do not configure an expected string, the ACE ignores the server response.

If you configure the **expect regex** command for TCP probes, you must configure the **send-data** command. Otherwise, the probe performs a connection open and close without checking the response from the server.

Examples

To configure a TCP probe to expect an ACK response, enter:

```
host1/Admin(config-probe-tcp)# expect regex ack
```

To remove the expectation of a response expression for a TCP probe, enter:

```
host1/Admin(config-probe-tcp)# no expect
```

To remove the expectation of a response expression for an HTTP probe, enter:

```
host1/Admin(config-probe-http)# no expect regex
```

Related Commands

show probe

(config-probe-*probe_type*) expect status

To configure a single status code or a range of status code responses that the ACE expects from the probe destination, use the **expect status** command. You can specify multiple status code ranges with this command by entering the command with different ranges separately. Use the **no** form of this command to remove the expected status code or codes from the configuration.

expect status *min_number max_number*

no expect status *min_number max_number*

Syntax Description

min_number	Single status code or the lower limit of a range of status codes. Enter an integer from 0 to 999.
max_number	Upper limit of a range of status codes. Enter an integer from 0 to 999. When configuring a single code, reenter the *min_number* value.

Command Modes

FTP, HTTP, HTTPS, RTSP, SIP, and SMTP probe configuration modes

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

When the ACE receives a response from the server, it expects a status code to mark a server as passed. By default, no status codes are configured on the ACE. If you do not configure a status code, any response code from the server is marked as failed.

You can specify multiple status code ranges with this command by entering the command with different ranges one at a time. Both the *min_number* and the *max_number* values can be any integer between 0 and 999 if the *max_number* is greater than or equal to the *min_number*. When the *min_number* and *max_number* values are the same, the ACE uses a single status code number.

Examples

To configure an expected status code of 200 that indicates that the HTTP request was successful, enter:

```
host1/Admin(config-probe-http)# expect status 200 200
```

To configure a range of expected status codes from 200 to 202, enter:

```
host1/Admin(config-probe-rtsp)# expect status 200 202
```

To configure multiple ranges of expected status codes from 200 to 202 and 204 to 205, configure each range separately. Enter:

```
host1/Admin(config-probe-http)# expect status 200 202
host1/Admin(config-probe-http)# expect status 204 205
```

To remove a single expected status code of 200, enter:

```
host1/Admin(config-probe-sip-udp)# no expect status 200 200
```

To remove a range of expected status codes, enter:

```
host1/Admin(config-probe-http)# no expect status 200 202
```

To remove multiple ranges of expected status codes, you must remove each range separately. If you have set two different ranges (200 to 202 and 204 to 205), enter:

```
host1/Admin(config-probe-http)# no expect status 200 202
host1/Admin(config-probe-http)# no expect status 204 205
```

Related Commands show probe

(config-probe-*probe_type*) faildetect

To change the number of consecutive failed probes, use the **faildetect** command. Use the **no** form of this command to reset the number of probe retries to its default.

faildetect *retry-count*

no faildetect

Syntax Description

retry_count	Consecutive number of failed probes before marking the server as failed. Enter a number from 1 to 65535. The default is 3.

Command Modes

All probe-type configuration modes

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

Before the ACE marks a server as failed, it must detect that probes have failed a consecutive number of times. By default, when three consecutive probes have failed, the ACE marks the server as failed.

Examples

To set the number of failed probes to 5 before declaring the server as failed for a TCP probe, enter:

```
host1/Admin(config-probe-tcp)# faildetect 5
```

To reset the number of probe failures to the default of 3, enter:

```
host1/Admin(config-probe-tcp)# no faildetect
```

Related Commands

show probe

(config-probe-*probe_type*) hash

To configure the ACE to dynamically generate the MD5 hash value or manually configure the value, use the **hash** command. By default, no hash value is configured on the ACE. Use the **no** form of this command to configure the ACE to no longer compare the referenced hash value to the computed hash value.

hash [*value*]

no hash

Syntax Description

value	(Optional) The MD5 hash value that you want to manually configure. Enter the MD5 hash value as a hexadecimal string with exactly 32 characters (16 bytes).

Command Modes

HTTP and HTTPS probe configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

If you do not use this command to configure the hash value, the ACE does not calculate a hash value on the HTTP data returned by the probe.

When you enter this command with no argument, the ACE generates the hash on the HTTP data returned by the first successful probe. If subsequent HTTP server hash responses match the generated hash value, the ACE marks the server as passed. If a mismatch occurs due to changes to the HTTP data, the probe fails and the **show probe ... detail** command displays an MD5 mismatch error in the Last disconnect error field.

To clear the reference hash and have the ACE recalculate the hash value at the next successful probe, change the URL or method by using the **request method** command.

The server response must include the Content-Length header for the **hash** command to function. Otherwise, the probe does not attempt to parse the hash value.

You can configure the **hash** command on a probe using the HEAD method, however there is no data to hash and has no effect causing the probe to always succeed.

Examples

To configure the ACE to generate the hash on the HTTP data returned by the first successful probe, enter:

```
host1/Admin(config-probe-http)# hash
```

To manually configure a hash value, enter:

```
host1/Admin(config-probe-http)# hash 0123456789abcdef0123456789abcdef
```

To configure the ACE to no longer compare the referenced hash value to the computed hash value, enter:

```
host1/Admin(config-probe-http)# no hash
```

Related Commands

show probe

(config-probe-probe_type) request method

(config-probe-*probe_type*) header

To configure a header field value for a probe, use the **header** command. Use the **no** form of this command to remove the header field from the probe configuration.

For HTTP and HTTPS probes, the syntax is as follows:

header *field_name* **header-value** *field_value*

no header *field_name*

For RTSP probes, the syntax is as follows:

header {**require** | **proxy-require**} **header-value** *field_value*

no header {**require** | **proxy-require**}

Syntax Description

field_name (HTTP and HTTPS probes) Identifier for a standard header field. Enter a text string with a maximum of 64 alphanumeric characters. If the header field includes spaces, enclose the string in quotation marks (“). You can also enter one of the following header keywords:

- **Accept**—Accept request header
- **Accept-Charset**—Accept-Charset request header
- **Accept-Encoding**—Accept-Encoding request header
- **Accept-Language**—Accept-Language request header
- **Authorization**—Authorization request header
- **Cache-Control**—Cache-Control general header
- **Connection**—Connection general header
- **Content-MD5**—Content-MD5 entity header
- **Expect**—Expect request header
- **From**—From request header
- **Host**—Host request header
- **If-Match**—If-Match request header

	• **Pragma**—Pragma general header • **Referer**—Referer request header • **Transfer-Encoding**—Transfer-Encoding general header • **User-Agent**—User-Agent request header • **Via**—Via general header
header-value *field_value*	(HTTP and HTTPS probes) Specifies the value assigned to the header field. Enter a text string with a maximum of 255 alphanumeric characters. If the value string includes spaces, enclose the string in quotation marks (“).
require	(RTSP probes) Specifies the Require header.
proxy-require	(RTSP probes) Specifies the Proxy-Require header.
header-value *field_value*	(RTSP probes) Specifies the value assigned to the header field. Enter an alphanumeric string with no spaces and a maximum of 255 characters.

Command Modes

HTTP, HTTPS, and RTSP probe configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.
A3(1.0)	This command was revised.

Usage Guidelines

For each HTTP or HTTPS probe in your configuration, you can configure multiple header fields.

Examples

To configure the Accept-Encoding HTTP header with a value of identity, enter:

```
host1/Admin(config-probe-http)# header Accept-Encoding header-value identity
```

To remove the header with the Accept-Encoding field name from the probe, enter:

```
host1/Admin(config-probe-http)# no header Accept-Encoding
```

To configure the RTSP REQUIRE header with a field value of implicit-play, enter:

```
host1/Admin(config-probe-rtsp)# header require header-value implicit-play
```

To remove the header configuration for the RTSP probe, enter:

```
host1/Admin(config-probe-rtsp)# no header require
```

To remove a Proxy-Require header, enter:

```
host1/Admin(config-probe-rtsp)# no header proxy-require
```

Related Commands

show probe

(config-probe-*probe_type*) interval

To change the time interval between probes, use the **interval** command. The time interval between probes is the frequency that the ACE sends probes to the server marked as passed. Use the **no** form of this command to reset the default time interval of 15 seconds.

interval *seconds*

no interval

Syntax Description

seconds	Time interval in seconds. Enter a number from 2 to 65535. The default is 15.

Command Modes

All probe-type configuration modes

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

The open timeout value for TCP-based probes and the receive timeout value can impact the execution time for a probe. When the probe interval is less than or equal to these timeout values and the server takes a long time to respond or it fails to reply within the timeout values, the probe is skipped. When the probe is skipped, the No. Probes skipped counter through the **show probe detail** command increments.

Examples

To configure a time interval of 50 seconds for a TCP probe, enter:

```
host1/Admin(config-probe-tcp)# interval 50
```

To reset the time interval to the default of 15 seconds, enter:

```
host1/Admin(config-probe-tcp)# no interval
```

Related Commands

show probe

(config-probe-*probe_type*) ip address

To override the destination address that the probe uses, use the **ip address** command. By default, the probe uses the IP address from the real server or server farm configuration for the destination IP address. Use the **no** form of this command to reset the default of the probe.

ip address *ip_address* [**routed**]

no ip address

Syntax Description

ip_address	Destination IP address. The default is the IP address from the real server or server farm configuration. Enter a unique IPv4 address in dotted-decimal notation (for example, 192.168.12.15).
routed	(Optional) Routes the address according to the ACE internal routing table.

Command Modes

All probe-type configuration modes except scripted probe configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

This command has no usage guidelines.

Examples

To configure a TCP probe destination IP address 192.168.12.15, enter:

```
host/Admin1(config-probe-tcp)# ip address 192.168.12.15
```

To reset the default of the probe using the IP address from the real server or server farm configuration, enter:

```
host1/Admin(config-probe-tcp)# no ip address
```

Related Commands

show probe

(config-probe-*probe_type*) nas ip address

To configure a Network Access Server (NAS) address, use the **nas ip address** command. Use the **no** form of this command to remove the NAS address.

nas ip address *ip_address*

no nas ip address

Syntax Description

ip_address	NAS IP address. Enter a unique IPv4 address in dotted-decimal notation (for example, 192.168.12.15). By default, if a NAS address is not configured for the Remote Authentication Dial-In User Service (RADIUS) probe, the ACE uses the IP address associated with the outgoing interface as the NAS address.

Command Modes

RADIUS probe configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

If a NAS address is not configured for the RADIUS probe, the ACE performs a route lookup on the RADIUS server IP address.

Examples

To configure a NAS address of 192.168.12.15, enter:

```
host1/Admin(config-probe-radius)# nas ip address 192.168.12.15
```

To remove the NAS IP address, enter:

```
host1/Admin(config-probe-radius)# no nas ip address
```

Related Commands

show probe

(config-probe-*probe_type*) oid

To configure an Object Identifier (OID) for an SNMP probe, use the **oid** command. When you enter this command, the CLI prompt changes to (config-probe-snmp-oid). For information about the commands available in probe SNMP OID configuration mode, see the Probe SNMP OID Configuration Mode Commands section. Use the **no** form of this command to remove the OID from the probe configuration.

oid *string*

no oid *string*

Syntax Description

string	OID that the probe uses to query the server for a value. Enter an unquoted string with a maximum of 255 alphanumeric characters in dotted-decimal notation. The OID string is based on the server type.

Command Modes

SNMP probe configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was revised.

Usage Guidelines

When the ACE sends a probe with an SNMP OID query, the ACE uses the retrieved value as input to the least-loaded algorithm for load-balancing decisions. Least-loaded load balancing bases the server selection on the server with the lowest load value. If the retrieved value is within the configured threshold, the server is marked as passed. If the threshold is exceeded, the server is marked as failed.

You can configure a maximum of eight OID queries to probe the server.

Examples

To configure the OID string .1.3.6.1.4.1.2021.10.1.3.1 and access probe SNMP OID configuration mode, enter:

```
host1/Admin(config-probe-snmp)# oid .1.3.6.1.4.1.2021.10.1.3.1
host1/Admin(config-probe-snmp-oid)#
```

To remove the OID string, enter:

```
host1/Admin(config-probe-snmp)# no oid .1.3.6.1.4.1.2021.10.1.3.1
```

Related Commands

show probe
(config-probe-snmp-oid) threshold
(config-probe-snmp-oid) type absolute max
(config-probe-snmp-oid) weight

(config-probe-*probe_type*) open

To configure the time interval for a connection to be established through a TCP three-way handshake, use the **open** command. By default, when the ACE sends a probe, it waits 10 seconds to open and establish the connection with the server. Use the **no** form of this command to reset its default of 1 second.

open *timeout*

no open

Syntax Description

timeout	Time in seconds. Enter an integer from 1 to 65535. The default is 1.

Command Modes

Echo TCP, Finger, FTP, HTTP, HTTPS, IMAP, POP, RTSP, scripted, SIP TCP, SMTP, TCP, and Telnet probe configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

The open timeout value for TCP-based probes and the receive timeout value can impact the execution time for a probe. When the probe interval is less than or equal to these timeout values and the server takes a long time to respond or it fails to reply within the timeout values, the probe is skipped. When the probe is skipped, the No. Probes skipped counter increments through the **show probe detail** command.

Examples

To configure the wait time interval to 25 seconds for a TCP probe, enter:

```
host1/Admin(config-probe-tcp)# open 25
```

To reset the time interval to its default of 1 second, enter:

```
host1/Admin(config-probe-tcp)# no open
```

Related Commands

show probe

(config-probe-*probe_type*) passdetect

To configure the time interval to send a probe to a failed server and the number of consecutive successful probe responses required to mark the server as passed, use the **passdetect** command. Use the **no** form of this command to reset the default of waiting 60 seconds before sending out a probe to a failed server and marking a server as passed if it receives 3 consecutive successful responses.

passdetect {**interval** *seconds* | **count** *number*}

no passdetect {**interval** | **count**}

Syntax Description

interval *seconds*	Specifies the wait time interval in seconds. Enter a number from 2 to 65535. The default is 60.
count *number*	Specifies the number of successful probe responses from the server. Enter a number from 1 to 65535. The default is 3.

Command Modes

All probe-type configuration modes except scripted probe configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

For best results, we recommend that you do not configure a **passdetect interval** value of less than 30 seconds. If you configure a **passdetect interval** value of less than 30 seconds, the **open timeout** and **receive timeout** values are set to their default values, and a real server fails to respond to a probe, overlapping probes may result, which can cause management resources to be consumed unnecessarily and the No. Probes skipped counter to increase.

After the ACE marks a server as failed, it waits a period of time and then sends a probe to the failed server. When the ACE receives a number of consecutive successful probes, it marks the server as passed. By default, the ACE waits 60 seconds before sending out a probe to a failed server and marks a server as passed if it receives 3 consecutive successful responses.

The receive timeout value can impact the execution time for a probe. When the probe interval is less than or equal to this timeout value and the server takes a long time to respond or it fails to reply within the timeout value, the probe is skipped. When the probe is skipped, the No. Probes skipped counter increments through the **show probe detail** command.

Examples

To configure a wait interval of 10 seconds for a TCP probe, enter:

```
host1/Admin(config-probe-tcp)# passdetect interval 10
```

To configure five success probe responses from the server before declaring it as passed, enter:

```
host1/Admin(config-probe-tcp)# passdetect count 5
```

To reset the wait interval to its default, enter:

```
host1/Admin(config-probe-tcp)# no passdetect interval
```

To reset the successful probe responses to its default, enter:

```
host1/Admin(config-probe-tcp)# no passdetect count
```

Related Commands

show probe

(config-probe-*probe_type*) port

To configure the port number that the probe uses, use the **port** command. Use the **no** form of this command to reset the port number based on the probe type.

port *port-number*

no port

Syntax Description

port-number	Port number for the probe. Enter an integer from 1 to 65535.

Command Modes

All probe-type configuration modes except ICMP probe configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

Table 2-17 lists the default port numbers for each probe type.

Table 2-17 Default Port Numbers for Probe Types

Probe Type	Default Port Number
DNS	53
Echo	7
Finger	79
FTP	21
HTTP	80
HTTPS	443
ICMP	Not applicable
IMAP	143
POP	110
RADIUS	1812
RTSP	554
SIP (TCP and UDP)	5060
SMTP	25
Telnet	23
TCP	80
UDP	53

If you choose not to specify a port number for a probe, the ACE can dynamically inherit the port number specified:

- From the real server specified in a server farm (see the **(config-sfarm-host) rserver** command).
- From the VIP specified in a Layer 3 and Layer 4 class map (see the **(config-cmap) match virtual-address** command).

In this case, all you need is a single probe configuration, which will be sufficient to probe a real server on multiple ports or on all VIP ports. The same probe inherits all of the real server's ports or all of the VIP ports and creates probe instances for each port.

Note Probe port inheritance is not applicable for the server farm predictor method, a probe assigned to a standalone real server, or a probe configured on the active FT group member in a redundant configuration.

For a Layer 3 and Layer 4 class map, a VIP port will be inherited only if a **match** command consists of a single port. If you specify a wildcard value for the IP protocol value (the **any** keyword) or a port range for the port, port inheritance does not apply for those match statements.

The order of precedence for inheriting the probe's port number is as follows:

1. Probe's configured port
2. Server farm real server's configured port
3. VIP's configured port
4. Probe's default port

For example, if the configured probe does not contain a specified port number, the ACE will look for the configured port associated with the real server specified in a server farm. If a port number is not configured, the ACE looks for the configured port associated with the VIP specified in a Layer 3 and Layer 4 class map. If a port number is also not configured, the ACE then uses the probe's default port to perform health monitoring on the back-end real server.

Examples

To configure a port number of 88 for an HTTP probe, enter:

```
host1/Admin(config-probe-HTTP)# port 88
```

To reset the port number to its default, in this case, port 80 for an HTTP probe, enter:

```
host1/Admin(config-probe-HTTP)# no port
```

Related Commands

show probe

(config-probe-*probe_type*) receive

To configure the time period that the ACE expects to receive a server response to the probe, use the **receive** command. Use the **no** form of this command to reset its default of 10 seconds.

receive *seconds*

no receive

Syntax Description

seconds	Time to wait in seconds. Enter an integer from 1 to 65535. The default is 10.

Command Modes

All probe-type configuration modes

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

By default, when the ACE sends a probe, it expects a response within a time period of 10 seconds. For example, for an HTTP probe, the timeout period is the number of seconds to receive an HTTP reply for a GET or HEAD request. If the server fails to respond to the probe, the ACE marks the server as failed.

The open timeout value for TCP-based probes and the receive timeout value can impact the execution time for a probe. When the probe interval is less than or equal to these timeout values and the server takes a long time to respond or it fails to reply within the timeout values, the probe is skipped. When the probe is skipped, the No. Probes skipped counter increments through the **show probe detail** command.

Examples

To configure the timeout period for a response at 5 seconds for a TCP probe, enter:

```
host1/Admin(config-probe-TCP)# receive 5
```

To reset the time period to receive a response from the server to its default of 10 seconds, enter:

```
host1/Admin(config-probe-TCP)# no receive
```

Related Commands

show probe

(config-probe-*probe_type*) request command

To configure the request command used by an Internet Message Access Protocol (IMAP) or POP probe, use the **request command** command. Use the **no** form of this command to remove the request command from the configuration.

request command *command*

no request

Syntax Description

command	Request command for the probe. Enter a text string with a maximum of 32 alphanumeric characters with no spaces.

Command Modes

IMAP and POP probe configuration modes

Admin and user context

Command History

Release	Modification
A1(7)	This command was revised.
A3(1.0)	This command was revised.

Usage Guidelines

You must configure the name of the mailbox using the **(config-probe-probe_type) credentials** command before you configure the request command used by an IMAP probe or the ACE will ignore the specified request command.

Examples

To configure the last request command for an IMAP probe, enter:

```
host1/Admin(config-probe-imap)# request command last
```

To remove the request command for the probe, enter:

```
host1/Admin(config-probe-imap)# no request
```

Related Commands

show probe

(config-probe-*probe_type*) request method

To configure the request method and URL used by a probe, use the **request method** command. Use the **no** form of this command to reset the default request method.

For HTTP and HTTPS probes, the syntax is as follows:

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

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

For RTSP probes, the syntax is as follows:

request method {**options** | **describe url** *url_string*}

no request method

For SIP probes, the syntax is as follows:

request method options

no request method

Syntax Description

get	(HTTP or HTTPS probe) Configures the HTTP GET request method to direct the server to get the page. This method is the default.
head	(HTTP or HTTPS probe) Configures the HTTP HEAD request method to direct the server to get only the header for the page.
url *url_string*	(HTTP or HTTPS probe) Specifies the URL string used by the probe. Enter an alphanumeric string with a maximum of 255 characters. The default string is a forward slash (/).
options	(RTSP or SIP probe) Specifies the OPTIONS request method. This is the default method. The ACE uses the asterisk (*) request URL for this method.
describe url *url_string*	(RTSP probe) Specifies the DESCRIBE request method. The *url_string* is the URL request for the RTSP media stream on the server. Enter an alphanumeric string with a maximum of 255 characters.

Command Modes

HTTP, HTTPS, RTSP, and SIP probe configuration modes

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised.

Usage Guidelines

By default, the HTTP request method is a GET with the URL of a forward slash (/). If you do not configure a URL, the HTTP or HTTPS probe functions as a TCP probe.

By default, the RTSP request method is the OPTIONS method. You can also configure the DESCRIBE method.

By default, the SIP request method is the OPTIONS method; this method is the only method available for SIP probes.

Examples

To configure the HTTP HEAD request method and the /digital/media/graphics.html URL used by an HTTP probe, enter:

```
host1/Admin(config-probe-http)# request method head url /digital/media/graphics.html
```

To reset the HTTP method for the probe to HTTP GET with a URL of "/", enter:

```
host1/Admin(config-probe-http)# no request method head url /digital/media/graphics.html
```

To configure an RTSP probe to use the URL rtsp:///media/video.smi, enter:

```
host1/Admin(config-probe-rtsp)# request method describe url
rtsp://192.168.10.1/media/video.smi
```

To reset the default RTSP request method (OPTIONS), use the **no request method** or the **request method options** command. For example, enter:

```
host1/Admin(config-probe-rtsp)# no request method
```

Related Commands

show probe

(config-probe-probe_type) hash

(config-probe-*probe_type*) script

To specify the script name and the arguments to be passed to a scripted probe, use the **script** command. Use the **no** form of this command to remove the script and its arguments from the configuration.

script *script_name* [*script_arguments*]

no script

Syntax Description

script_name	Name of the script. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters.
script_arguments	(Optional) Data sent to the script. Enter a text string with a maximum of 255 alphanumeric characters including spaces and quotes. Separate each argument by a space. If a single argument contains spaces, enclose the argument string in quotes.

Command Modes

Scripted probe configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

Scripted probes run probes from a configured script to perform health probing. You can also configure arguments that are passed to the script. Before you can associate a script file with a probe, you must copy and load the script on the ACE. For information about TCL scripts and instructions for copying and loading script files on the ACE, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

The ACE allows the configuration of 256 unique script files.

The ACE can simultaneously execute only 200 scripted probe instances. When this limit is exceeded, the **show probe detail** command displays the "Out-of Resource: Max. script-instance limit reached" error message in the Last disconnect err field and the out-of-sockets counter increments.

Examples

To configure the script name of PROBE-SCRIPT and arguments of double question marks (??), enter:

```
host1/Admin(config-probe-scrptd)# script PROBE-SCRIPT ??
```

To remove the script and its arguments from the configuration, enter:

```
host1/Admin(config-probe-scrptd)# no script
```

Related Commands

show probe
show script
(config) script file name

(config-probe-*probe_type*) send-data

To configure the ASCII data that the probe sends when the ACE connects to the server, use the **send-data** command. Use the **no** form of this command to remove the data from the configuration.

send-data *expression*

no send-data

Syntax Description

expression	ASCII data that the probe sends. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters.

Command Modes

ECHO, Finger, TCP, and UDP probe configuration modes

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines If you do not configure the **send-data** command for a UDP probe, the probe sends one byte, 0x00.

Examples To configure a TCP probe to send TEST as the data, enter:

```
host1/Admin(config-probe-tcp)# send-data TEST
```

To remove the data, enter:

```
host1/Admin(config-probe-tcp)# no send-data
```

Related Commands **show probe**

(config-probe-*probe_type*) ssl cipher

To configure the probe to expect a specific type of RSA cipher suite from the back-end server, use the **ssl cipher** command. Use the **no** form of this command to reset its default of accepting any RSA configured cipher suites.

ssl cipher {**RSA_ANY** | *cipher_suite*}

no ssl cipher

Syntax Description

RSA_ANY	Specifies that the probe accepts any of the RSA configured cipher suites. This is the default.
cipher_suite	RSA cipher suite that the probe expects from the back-end server. Enter one of the following keywords: **RSA_EXPORT1024_WITH_DES_CBC_SHA** **RSA_EXPORT1024_WITH_RC4_56_MD5** **RSA_EXPORT1024_WITH_RC4_56_SHA** **RSA_EXPORT_WITH_DES40_CBC_SHA** **RSA_EXPORT_WITH_RC4_40_MD5** **RSA_WITH_3DES_EDE_CBC_SHA** **RSA_WITH_AES_128_CBC_SHA** **RSA_WITH_AES_256_CBC_SHA** **RSA_WITH_DES_CBC_SHA** **RSA_WITH_RC4_128_MD5** **RSA_WITH_RC4_128_SHA**

Command Modes HTTPS probe configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

This command has no usage guidelines.

Examples

To configure the HTTPS probes with the RSA_WITH_RC4_128_SHA cipher suite, enter:

```
host1/Admin(config-probe-https)# ssl cipher RSA_WITH_RC4_128_SHA
```

To reset the default of the HTTPS probes accepting any RSA cipher suite, enter:

```
host1/Admin(config-probe-https)# ssl cipher RSA_ANY
```

To reset the default by using the **no ssl cipher** command, enter:

```
host1/Admin(config-probe-https)# no ssl cipher
```

Related Commands

show probe

(config-probe-*probe_type*) ssl version

To configure the version of Secure Sockets Layer (SSL) that the probe supports, use the **ssl version** command. Use the **no** form of this command to reset the default to SSL version 3.

ssl version {**all** | **SSLv3** | **TLSv1**}

no ssl version

Syntax Description

all	Configures the probe to support all SSL versions.
SSLv3	Configures the probe to support SSL version 3. This is the default.
TLSv1	Configures the probe to support TLS version 1.

Command Modes

HTTPS probe configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

The version in the ClientHello message sent to the server indicates the highest supported version.

Examples

To configure the probe to support all SSL versions, enter:

```
host1/Admin(config-probe-https)# ssl version all
```

To reset the default of SSL version 3, enter:

```
host1/Admin(config-probe-https)# no ssl version
```

Related Commands show probe

(config-probe-*probe_type*) version

To configure the version of SNMP that the probe supports, use the **version** command. Use the **no** form of this command to reset the version to its default value of SNMP version 1.

version {**1** | **2c**}

no version

Syntax Description

1	Configures the probe to support SNMP version 1. This is the default.
2c	Configures the probe to support SNMP version 2c.

Command Modes

SNMP probe configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was revised.

Usage Guidelines

The version in the SNMP OID query sent to the server indicates the supported SNMP version. By default, the probe supports SNMP version 1.

Examples

To configure the probe to use SNMP version 2c, enter:

```
host1/Admin(config-probe-snmp)# version 2c
```

To reset the version of SNMP to the default value, SNMP version 1, enter:

```
host1/Admin(config-probe-snmp)# no version
```

Related Commands show probe

Probe SNMP OID Configuration Mode Commands

Probe SNMP OID configuration mode commands allow you to configure an OID for an SNMP probe. To configure an OID for an SNMP probe and access probe SNMP OID configuration mode, use the **oid** command in SNMP probe configuration mode. The CLI prompt changes to (config-probe-snmp-oid). For information about the commands in this mode, see the following commands. Use the **no** form of this command to remove the OID from the SNMP probe configuration.

oid *string*

no oid *string*

Syntax Description

string	OID that the probe uses to query the server for a value. Enter an unquoted string with a maximum of 255 alphanumeric characters in dotted-decimal notation. The OID string is based on the server type.

Command Modes

SNMP probe configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was revised.

Usage Guidelines

When the ACE sends a probe with an SNMP OID query, the ACE uses the retrieved value as input to the least-loaded algorithm for load-balancing decisions. Least-loaded load balancing bases the server selection on the server with the lowest load value. If the retrieved value is within the configured threshold, the server is marked as passed. If the threshold is exceeded, the server is marked as failed.

You can configure a maximum of eight OID queries to probe the server.

Examples

To configure the OID string .1.3.6.1.4.2021.10.1.3.1 and access probe SNMP OID configuration mode, enter:

```
host1/Admin(config-probe-snmp)# oid .1.3.6.1.4.2021.10.1.3.1
host1/Admin(config-probe-snmp-oid)#
```

To remove the OID string, enter:

```
host1/Admin(config-probe-snmp)# no oid .1.3.6.1.4.2021.10.1.3.1
```

Related Commands

show probe
(config-probe-snmp-oid) threshold
(config-probe-snmp-oid) type absolute max
(config-probe-snmp-oid) weight

(config-probe-snmp-oid) threshold

To specify the threshold value for an OID, use the **threshold** command. Use the **no** form of this command to remove the threshold value.

threshold *integer*

no threshold *integer*

Syntax Description

integer	Threshold value to take the server out of service. When the OID value is based on a percentile, enter an integer from 0 to 100, with a default value of 100. When the OID is based on an absolute value, the threshold range is from 1 to the maximum value specified using the **type absolute max** command.

Command Modes

Probe SNMP OID configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was revised.

Usage Guidelines

You can configure a threshold for an OID value so that when the threshold is exceeded, the server is taken out of service.

When the ACE sends a probe with an SNMP OID query, the ACE uses the retrieved value as input to the least-loaded algorithm for load-balancing decisions. Least-loaded load balancing bases the server selection on the server with the lowest load value. If the retrieved value is within the configured threshold, the server is marked as passed. If the threshold is exceeded, the server is marked as failed.

By default, the OID value is based on a percentile. If you use the **type absolute maximum** command to base the OID on an absolute value, the threshold range is from 1 to the maximum value specified with the **type absolute maximum** command.

Examples

To configure a threshold of 90 for the OID, enter:

```
host1/Admin(config-probe-snmp-oid)# threshold 90
```

To remove the threshold from the OID, enter:

```
host1/Admin(config-probe-snmp-oid)# no threshold
```

Related Commands

show probe
(config-probe-probe_type) oid
(config-probe-snmp-oid) type absolute max
(config-probe-snmp-oid) weight

(config-probe-snmp-oid) type absolute max

To specify that the retrieved OID value is an absolute value, use the **type absolute max** command. Use the **no** form of this command to remove the absolute value.

type absolute max *integer*

no type

Syntax Description

integer	Expected OID value. Enter an integer from 1 through 4294967295.

Command Modes

Probe SNMP OID configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was revised.

Usage Guidelines

When the ACE sends a probe with an SNMP OID query, the ACE uses the retrieved value as input to the least-loaded algorithm for load-balancing decisions. By default, the ACE assumes that the retrieved OID value is a percentile value.

Least-loaded load balancing bases the server selection on the server with the lowest load value. If the retrieved value is within the configured threshold, the server is marked as passed. If the threshold is exceeded, the server is marked as failed.

When you configure the **type absolute max** command, we recommend that you also configure the value for the **threshold** command because the default threshold value is 100 and is not automatically adjusted with respect to the **type absolute max** value.

The **no type** command resets the values of both the **type absolute max** command and the **threshold** command to a value of 100.

Examples

To specify that the retrieved maximum OID value is 597, enter:

```
host1/Admin(config-probe-snmp-oid)# type absolute max 597
```

To remove the OID value and reset the expected OID to a percentile, enter:

```
host1/Admin(config-probe-snmp-oid)# no type
```

Related Commands

show probe
(config-probe-probe_type) oid
(config-probe-snmp-oid) threshold
(config-probe-snmp-oid) weight

(config-probe-snmp-oid) weight

To configure the weight to be assigned to this OID for the SNMP probe, use the **weight** command. Use the **no** form of this command to remove the weight.

weight *number*

no weight

Syntax Description

number	Weight value assigned to this OID for the SNMP probe. Enter an integer from 0 to 16000.

Command Modes

Probe SNMP OID configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was revised.

Usage Guidelines

If you configure more than one OID and they are used in a load-balancing decision, you must configure a weight value.

When the ACE sends a probe with an SNMP OID query, the ACE uses the retrieved value as input to the least-loaded algorithm for load-balancing decisions. Least-loaded load balancing bases the server selection on the server with the lowest load value. If the retrieved value is within the configured threshold, the server is marked as passed. If the threshold is exceeded, the server is marked as failed.

Examples

To configure a weight of 90 for the OID, enter:

```
host1/Admin(config-probe-snmp-oid)# weight 90
```

To remove the threshold from the OID, enter:

```
host1/Admin(config-probe-snmp-oid)# no weight
```

Related Commands

show probe
(config-probe-probe_type) oid
(config-probe-snmp-oid) threshold
(config-probe-snmp-oid) type absolute max

RADIUS Configuration Mode Commands

RADIUS configuration mode commands allow you to configure multiple Remote Access Dial-In User Service (RADIUS) servers as a named AAA server group. You specify the IP address of one or more previously configured RADIUS servers that you want added to or removed from a AAA server group, along with a dead-time interval for the RADIUS server group.

For details about creating a RADIUS server group, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

To create a RADIUS server group and access RADIUS server configuration mode, enter the **aaa group server radius** command. The CLI prompt changes to (config-radius). Use the **no** form of this command to remove a RADIUS server group.

aaa group server radius *group_name*

no aaa group server radius *group_name*

Syntax Description

group_name	Group of RADIUS servers. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

A server group is a list of server hosts. The ACE allows you to configure multiple AAA servers as a named server group. You group the different AAA server hosts into distinct lists. The ACE searches for the server hosts in the order in which you specify them within a group. You can configure a maximum of 10 server groups for each context in the ACE.

You can configure server groups at any time, but you must enter the **aaa authentication login** or the **aaa accounting default** command to apply them to the AAA service.

Examples

To create a RADIUS server group, enter:

```
host1/Admin(config) aaa group server radius RADIUS_Server_Group1
host1/Admin(config-radius)# server 172.16.56.76
host1/Admin(config-radius)# server 172.16.56.79
host1/Admin(config-radius)# server 172.16.56.82
```

Related Commands

(config) aaa accounting default
(config) aaa authentication login

(config-radius) deadtime

To specify a dead-time interval for the Remote Authentication Dial-In User Service (RADIUS) server group, use the **deadtime** command. Use the **no** form of this command to reset the RADIUS server group dead-time request to its default of 0.

deadtime *minutes*

no deadtime *minutes*

Syntax Description

minutes	Length of time that the ACE skips a nonresponsive RADIUS server for transaction requests. Valid entries are from 0 to 1440 (24 hours). The default is 0.

Command Modes

RADIUS configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Use of the **deadtime** command causes the ACE to mark as dead any RADIUS servers that fail to respond to authentication requests. Entering this command prevents the wait for the request to time out before trying the next configured server. The ACE skips a RADIUS server that is marked as dead by additional requests for the duration of minutes.

During the dead-time interval, the ACE sends probe access-request packets to verify that the RADIUS server is available and can receive authentication requests. The dead-time interval starts when the server does not respond to an authentication request transmission. When the server responds to a probe access-request packet, the ACE retransmits the authentication request to the server.

Examples

To globally configure a 15-minute dead-time interval for RADIUS servers that fail to respond to authentication requests, enter:

```
host1/Admin(config) aaa group server radius RADIUS_Server_Group1
host1/Admin(config-radius)# deadtime 15
```

To reset the RADIUS server dead-time request to the default of 0, enter:

```
host1/Admin(config-radius)# no deadtime 15
```

Related Commands

(config) aaa group server

(config-radius) server

To specify the IP address of one or more previously configured Remote Authentication Dial-In User Service (RADIUS) servers that you want added to or removed from a server group, use the **server** command. Use the **no** form of this command to remove the RADIUS server from the AAA server group.

server *ip_address*

no server *ip_address*

Syntax Description

ip_address	IP address of the RADIUS server. Enter the address in dotted-decimal IP notation (for example, 192.168.11.1).

Command Modes

RADIUS configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You can add multiple RADIUS servers to the AAA server group by entering multiple **server** commands in this mode. The same server can belong to multiple server groups.

Examples

To add servers to a RADIUS server group, enter:

```
host1/Admin(config-radius)# server 172.16.56.76
host1/Admin(config-radius)# server 172.16.56.79
host1/Admin(config-radius)# server 172.16.56.82
```

To remove a server from a RADIUS server group, enter:

```
host1/Admin(config) aaa group server radius RADIUS_Server_Group1
host1/Admin(config-radius)# no server 172.16.56.76
```

Related Commands

(config) aaa group server

Real Server Host Configuration Mode Commands

Real server host configuration mode commands allow you to create and configure host real servers that are used in server load balancing (SLB). The parameters that you configure determine how the ACE interacts with the servers used for web content and services. For details about SLB, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

To create a host real server and access real server host configuration mode, use the **rserver host** command in configuration mode. The CLI prompt changes to (config-rserver-host). For information about commands available in this mode, see the following commands.

Use the **no** form of this command to remove an existing real server from the configuration.

rserver [**host**] *name*

no rserver *name*

Syntax Description

name	Unique identifier of the real server. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
host	(Optional) Specifies that the real server is a typical server that provides web services and content.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

The commands in this mode require the rserver feature in your user role unless otherwise specified. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

All servers in a server farm should be of the same type: **host** or **redirect**.

Examples

To create a host server named SERVER1, enter:

```
host1/Admin(config)# rserver SERVER1
host1/Admin(config-rserver-host)#
```

To delete the host server named SERVER1, enter:

```
host1/Admin(config)# no rserver SERVER1
```

Related Commands

(config-sfarm-host) rserver

(config-rserver-host) conn-limit

To configure the maximum and minimum number of connections that you want to allow for a host real server, use the **conn-limit** command. Use the **no** form of this command to reset the maximum number of connections and the minimum connection threshold for a real server to the default of 4000000.

conn-limit max *max-conns* **min** *min-conns*

no conn-limit max

Syntax Description

max *maxconns*	Specifies the maximum number of connections allowed for this real server. Enter an integer from 2 to 4000000. The default is 4000000.
min *minconns*	Specifies the connection threshold below which the real server will start accepting connections again after the number of connections exceeds the configured maximum number of connections. Enter an integer from 2 to 4000000. The default is *minconns* equal to *maxconns*.

Command Modes

Real server host configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

Use this command to specify the maximum number of connections and the minimum connection threshold for a real server. The *minconns* value must be less than or equal to the *maxconns* value. When the number of connections to a real server reaches the maxconns value, the ACE stops sending connections to that server and assigns it a state of OUTOFSERVICE. The ACE uses the *minconns* value as a threshold for load balancing to start accepting connections again after the *maxconns* limit is reached.

Examples

To configure the maximum number of connections and the minimum connection threshold for a real server, enter:

```
host1/Admin(config-rserver-host)# conn-limit max 65535 min 40000
```

To reset the maximum number of connections and the minimum connection threshold for a real server to the default of 4000000, enter:

```
host1/Admin(config-rserver-host)# no conn-limit
```

Related Commands

(config-rserver-host) rate-limit

(config-rserver-host) description

To configure a description for a real server, use the **description** command. Use the **no** form of this command to remove the real server description from the configuration.

description *text*

no description

Syntax Description

text	User-defined description of the real server and related information. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Real server host configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

This command has no usage guidelines.

Examples

To configure a description for a real server, enter:

```
host1/Admin(config-rserver-host)# description database application server
```

To delete a description for a real server, enter:

```
host1/Admin(config-rserver-host)# no description
```

Related Commands

This command has no related commands.

(config-rserver-host) fail-on-all

To configure a real server to remain in the OPERATIONAL state unless all probes associated with it fail (AND logic), use the **fail-on-all** command in real server host configuration mode. This command is applicable to all probe types. The syntax of this command is:

fail-on-all

no fail-on-all

Syntax Description

This command has no keywords or arguments.

Command Modes

Real server host configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was revised.

Usage Guidelines

This command has no usage guidelines.

Examples

To configure the SERVER1 real server to remain in the OPERATIONAL state unless all associated probes fail, enter the following commands:

```
host1/Admin(config)# rserver SERVER1
host1/Admin(config-rserver-host)# ip address 192.168.12.15
host1/Admin(config-rserver-host)# probe HTTP_PROBE
host1/Admin(config-rserver-host)# probe ICMP_PROBE
host1/Admin(config-rserver-host)# fail-on-all
```

To remove the AND probe logic from the real server and return the behavior to the default of OR logic, enter the following command:

```
host1/Admin(config-rserver-host)# no fail-on-all
```

Related Commands

This command has no related commands.

(config-rserver-host) inservice

To place a real server in service, use the **inservice** command in real server host configuration mode. Use the **no** form of this command to gracefully shut down a real server.

inservice

no inservice

Syntax Description

This command has no keywords or arguments.

Command Modes

Real server host configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

This command requires the real-inservice feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Use the **no** form of this command to shut down a real server gracefully for maintenance or software upgrades. When you enter this command, the ACE tears down all non-TCP connections. For TCP connections, the ACE allows existing connections to end before taking the server out of service. No new connections are allowed. To place the real server back in service, use the **inservice** command.

The ACE resets all SSL connections to a particular real server when you enter the **no inservice** command for that server.

Examples

To place a real server in service, enter:

```
host1/Admin(config-rserver-host)# inservice
```

To take a real server out of service, enter:

```
host1/Admin(config-rserver-host)# no inservice
```

Related Commands

This command has no related commands.

(config-rserver-host) ip address

To configure an IP address for a real server, use the **ip address** command in real server host configuration mode. Use the **no** form of this command to remove the real server IP address from the configuration.

ip address *ip-address*

no ip address

Syntax Description

ip-address	IP address for the real server of type host. Enter an IP address in dotted-decimal notation (for example, 192.168.12.6).

Command Modes

Real server host configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

Use this command to provide a unique IP address for a real server. The address that you choose must not be a VIP of an existing virtual server.

Examples

To configure the IP address of a real server, enter:

```
host1/Admin(config-rserver-host)# ip address 192.168.12.6
```

To delete the real server IP address from the configuration, enter:

```
host1/Admin(config-rserver-host)# no ip address 192.168.12.6
```

Related Commands

This command has no related commands.

(config-rserver-host) probe

To configure a probe to monitor the health of a real server, use the **probe** command. Use the **no** form of this command to remove the probe from the real server.

probe *probe-name*

no probe *probe-name*

Syntax Description

probe-name	Identifier of an existing probe that you want to assign to a real server to monitor its health. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Real server host configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

You can associate multiple probes with each real server.

Examples

To configure a probe for a real server of type **host**, enter:

```
host1/Admin(config-rserver-host)# probe SERVER1_PROBE
```

To remove a probe from a real server of type **host**, enter:

```
host1/Admin(config-rserver-host)# no probe SERVER1_PROBE
```

Related Commands

This command has no related commands.

(config-rserver-host) rate-limit

To configure a limit for the connection rate and the bandwidth rate of a real server, use the **rate-limit** command. The connection rate is the number of connections per second received by the ACE and applies only to the new connections destined to a real server. The bandwidth rate is the number of bytes per second and applies to the network traffic exchanged between the ACE and the real server in both directions. Use the **no** form of this command to revert to the ACE default of not limiting the connection rate or bandwidth rate of real servers.

rate-limit {**connection** *number1* | **bandwidth** *number2*}

no rate-limit {**connection** | **bandwidth**}

Syntax Description

connection *number1*	Specifies the real server connection-rate limit in connections per second. Enter an integer from 2 to 350000. There is no default value.
bandwidth *number2*	Specifies the real server bandwidth-rate limit in bytes per second. Enter an integer from 2 to 300000000. There is no default value.

Command Modes

Real server host configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was revised.

Usage Guidelines

For a real server that is associated with more than one server farm, the ACE uses the aggregated connection rate or bandwidth rate to determine whether the real server has exceeded its rate limits. If the connection rate or the bandwidth rate of incoming traffic destined for a particular server exceeds the configured rate of the server, the ACE blocks any further traffic destined to that real server until the connection rate or bandwidth rate drops below the configured limit. Also, the ACE removes the blocked real server from future load-balancing decisions.

You can also limit the connection rate and the bandwidth rate at the virtual server level in a connection parameter map. For details, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

Examples

To limit the connection rate of a real server to 100,000 connections per second, enter:

```
host1/Admin(config-rserver-host)# rate-limit connection 100000
```

To revert to the ACE default of not limiting the real-server connection rate, enter:

```
host1/Admin(config-rserver-host)# no rate-limit connection
```

To limit the real-server bandwidth rate to 5,000,000 bytes per second, enter:

```
host1/Admin(config-rserver-host)# rate-limit bandwidth 5000000
```

To revert to the ACE default of not limiting real-server bandwidth, enter:

```
host1/Admin(config-rserver-host)# no rate-limit bandwidth
```

Related Commands **(config-rserver-host) conn-limit**

(config-rserver-host) weight

To configure the capacity of a real server in relation to other servers in a server farm, use the **weight** command. The weight value that you specify for a server is used in the weighted round-robin and least-connections predictor load-balancing methods. Use the **no** form of this command to reset the real server weight to the default.

weight *number*

no weight

Syntax Description

number	Weight value assigned to a real server in a server farm. This value is used in the weighted round-robin and least-connections predictor load-balancing algorithms. Enter an integer from 0 to 100. The default is 8.

Command Modes

Real server host configuration mode.

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

Servers with a higher configured weight value have a higher priority with respect to connections than servers with a lower weight. For example, a server with a weight of 5 would receive five connections for every one connection received by a server with a weight of 1.

To specify different weight values for a real server in a server farm, you can assign multiple IP addresses to the server. You can also use the same IP address of a real server with different port numbers.

Server weights take effect only when there are open connections to the servers. When there are no sustained connections to any of the servers, the leastconns predictor method behaves like the roundrobin method.

Examples

To configure a weight value for a real server, enter:

```
host1/Admin(config-rserver-host)# weight 50
```

To reset the weight of a real server to the default of 8, enter:

```
host1/Admin(config-rserver-host)# no weight
```

Related Commands

This command has no related commands.

Real Server Redirect Configuration Mode Commands

Real server redirect configuration mode commands allow you to configure parameters for redirection real servers used in server load balancing (SLB). A redirection real server is used only for redirecting network traffic to another server as indicated in the Webhost redirection string. See the **(config-rserver-redir) webhost-redirection** command. The parameters that you configure determine how the ACE interacts with the servers used for redirection. Redirection servers are useful for content that has physically moved to another location, either temporarily or permanently. For details about SLB and redirection, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

To create a redirect real server and access real server configuration mode, use the **rserver redirect** command in configuration mode. The CLI prompt changes to (config-rserver-redir). For information about commands available in this mode, see the commands that follow this section.

Use the **no** form of this command to remove an existing real server from the configuration.

rserver redirect *name*

no rserver redirect *name*

Syntax Description

name	Unique identifier of the real server. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

All commands in this mode require the Real feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

All servers in a server farm should be of the same type: **host** or **redirect.**

Examples

To create a redirect server named SERVER1, enter:

```
host1/Admin(config)# rserver redirect SERVER1
```

To delete the redirect server named SERVER1, enter:

```
host1/Admin(config)# no rserver redirect SERVER1
```

Related Commands

(config-rserver-redir) webhost-redirection

(config-rserver-redir) conn-limit

To configure the maximum and minimum number of connections that you want to allow for a real server, use the **conn-limit** command. Use the **no** form of this command to reset the maximum number of connections and the minimum connection threshold for a real server to the default of 4000000.

conn-limit max *max-conns* **min** *min-conns*

no conn-limit max

Syntax Description

max *max-conns*	Specifies the maximum number of connections allowed for this real server. Enter an integer from 2 to 4000000. The default is 4000000.
min *min-conns*	Specifies the connection threshold below which the real server will start accepting connections again after the number of connections exceeds the configured maximum number of connections. Enter an integer from 2 to 4000000. The default is *minconns* equal to *maxconns*.

Command Modes

Real server redirect configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

Use this command to specify the maximum number of connections and the minimum connection threshold for a real server. The *minconns* value must be less than or equal to the *maxconns* value. When the number of connections to a real server reaches the maxconns value, the ACE stops sending connections to that server and assigns it a state of OUTOFSERVICE. The ACE uses the *minconns* value as a threshold for load balancing to start accepting connections again after the *maxconns* limit is reached.

Examples

To configure the maximum number of connections and the minimum connection threshold for a real server, enter:

```
host1/Admin(config-rserver-redir)# conn-limit maxconns 65535 minconns 40000
```

To reset the maximum number of connections and the minimum connection threshold for a real server of type **redirect** to the default of 4000000, enter:

```
host1/Admin(config-rserver-redir)# no conn-limit
```

Related Commands

This command has no related commands.

(config-rserver-redir) description

To configure a description for a real server, use the **description** command. Use the **no** form of this command to remove the real server description from the configuration.

description *text*

no description

Syntax Description

text	User-defined description of the real server and related information. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Real server redirect configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

Use this command to provide a unique description for the real server with a maximum of 240 characters.

Examples

To configure a real server description, enter:

```
host1/Admin(config-rserver-redir)# description database application server
```

To delete a real server description, enter:

```
host1/Admin(config-rserver-redir)# no description
```

Related Commands

This command has no related commands.

(config-rserver-redir) inservice

To place a real server in service, use the **inservice** command. Use the **no** form of this command to remove the real server from service.

inservice

no inservice

Syntax Description

This command has no keywords or arguments.

Command Modes

Real server redirect configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

This command requires the real-inservice feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Use the **no** form of this command to shut down a real server gracefully for maintenance or software upgrades. When you enter this command, the ACE tears down all non-TCP connections. For TCP connections, the ACE allows existing connections to end before taking the server out of service. No new connections are allowed. To place the real server back in service, use the **inservice** command.

Examples

To place a real server in service, enter:

```
host1/Admin(config-rserver-redir)# inservice
```

To take a real server out of service, enter:

```
host1/Admin(config-rserver-redir)# no inservice
```

Related Commands

This command has no related commands.

(config-rserver-redir) rate-limit

To configure a limit for the connection rate and the bandwidth rate of a real server, use the **rate-limit** command. The connection rate is the number of connections per second received by the ACE and applies only to the new connections destined to a real server. The bandwidth rate is the number of bytes per second and applies to the network traffic exchanged between the ACE and the real server in both directions. Use the **no** form of this command to revert to the ACE default of not limiting the connection rate or bandwidth rate of real servers.

rate-limit {**connection** *number1* | **bandwidth** *number2*}

no rate-limit {**connection** | **bandwidth**}

Syntax Description

connection *number1*	Specifies the real server connection-rate limit in connections per second. Enter an integer from 2 to 350000. There is no default value.
bandwidth *number2*	Specifies the real server bandwidth-rate limit in bytes per second. Enter an integer from 2 to 300000000. There is no default value.

Command Modes

Real server redirect configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was revised.

Usage Guidelines

For a real server that is associated with more than one server farm, the ACE uses the aggregated connection rate or bandwidth rate to determine whether the real server has exceeded its rate limits. If the connection rate or the bandwidth rate of incoming traffic destined for a particular server exceeds the configured rate of the server, the ACE blocks any further traffic destined to that real server until the connection rate or bandwidth rate drops below the configured limit. Also, the ACE removes the blocked real server from future load-balancing decisions.

You can also limit the connection rate and the bandwidth rate at the virtual server level in a connection parameter map. For details, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

Examples

To limit the connection rate of a real server to 100,000 connections per second, enter:

```
host1/Admin(config-rserver-redir)# rate-limit connection 100000
```

To revert to the ACE default of not limiting the real-server connection rate, enter:

```
host1/Admin(config-rserver-redir)# no rate-limit connection
```

To limit the real-server bandwidth rate to 5,000,000 bytes per second, enter:

```
host1/Admin(config-rserver-redir)# rate-limit bandwidth 5000000
```

To revert to the ACE default of not limiting real-server bandwidth, enter:

```
host1/Admin(config-rserver-redir)# no rate-limit bandwidth
```

Related Commands (config-rserver-redir) conn-limit

(config-rserver-redir) webhost-redirection

To configure the relocation URL string used for redirection, use the **webhost-redirection** command. You can configure a port number to redirect a request in the relocation string. Use the **no** form of this command to remove the real server redirection URL string from the configuration.

webhost-redirection *relocation_string* [**301** | **302**]

no webhost-redirection

Syntax Description

relocation_string	URL string used to redirect requests to another server. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters. The redirection string supports the following special characters: • **%h**—Inserts the hostname from the request Host header • **%p**—Inserts the URL path string from the request **Note** To insert a question mark (?) in the relocation string, press **Ctrl-v** before you type the question mark.
[**301** | **302**]	(Optional) Specifies the redirection status code returned to a client. The codes indicate the following: • **301**—The requested resource has been moved permanently. For future references to this resource, the client should use one of the returned URIs. • **302**—(Default) The requested resource has been found but has been moved temporarily to another location. For future references to this resource, the client should continue to use the request URI because the resource may be moved to other locations from time to time. For more information about redirection status codes, see RFC 2616.

Command Modes

Real server redirect configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was revised.

Usage Guidelines

Enter this command only on a real server that you have configured as a redirection server.

Examples

To configure a redirection string on a real server, enter:

```
host1/Admin(config-rserver-redir)# webhost-redirection www.acme.com/common/images/*.jpg
301
```

To remove the redirection string from a real server, enter:

```
host1/Admin(config-rserver-redir)# no webhost-redirection
```

Related Commands

This command has no related commands.

Resource Configuration Mode Commands

Resource configuration mode commands allow you to limit the usage of resources by one or more contexts. To create a resource class and access resource configuration mode, enter the **resource-class** command. The CLI prompt changes to (config-resource). For information about the commands in resource configuration mode, see the commands in this section. Use the **no** form of this command to delete a resource class.

resource-class *name*

no resource-class *name*

Syntax Description

name	Name assigned to the new resource class. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. You can also use the resource class called **default**.

Command Modes

Configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

After you create and configure the class, use the **(config-context) member** command in context configuration mode to assign a context to the class.

Examples

To create a resource-class called RC1 and enter resource configuration mode, enter:

```
host1/C1(config)# resource-class RC1
host1/C1(config-resource)
```

To remove the RC1 resource class from the configuration, enter:

```
host1/C1(config)# no resource-class RC1
```

Related Commands

(config-context) member

(config-resource) limit-resource

To limit system resources for all members of a resource class, use the **limit-resource** command. Use the **no** form of this command to restore the default resource settings for all resources or individual resources for all members (contexts) of a resource class.

limit-resource {**acc-connections** | **acl-memory** | **all** | **buffer** {**syslog**} | **conc-connections** | **http-comp** | **mgmt-connections** | **proxy-connections** | **rate** {**bandwidth** | **connections** | **inspect-conn** | **mac-miss** | **mgmt-traffic** | **ssl-connections** | **syslog**} | **regexp** | **sticky** | **xlates**} {**minimum** *number*} {**maximum** {**equal-to-min** | **unlimited**}}

no limit-resource {**acc-connections** | **acl-memory** | **all** | **buffer** {**syslog**} | **conc-connections** | **http-comp** | **mgmt-connections** | **proxy-connections** | **rate** {**bandwidth** | **connections** | **inspect-conn** | **mac-miss** | **mgmt-traffic** | **ssl-connections** | **syslog**} | **regexp** | **sticky** | **xlates**} {**minimum** *number*} {**maximum** {**equal-to-min** | **unlimited**}}

Syntax Description

acc-connections	Limits the number of application acceleration connections.
acl-memory	Limits memory allocated for ACLs.
all	Limits all resources to the specified value for all contexts assigned to this resource class.
buffer syslog	Limits the amount of buffering for syslog messages.
conc-connections	Limits the number of simultaneous connections.
http-comp	Limits the HTTP compression rate.
mgmt-connections	Limits the number of management connections.
proxy-connections	Limits the number of proxy connections.
rate	Limits the resource as a number per second for the following: • **bandwidth**—Limits context throughput in bytes per second. • **connections**—Limits the number of connections of any kind per second. • **inspect conn**—Limits the number of application protocol inspection connections per second for File Transfer Protocol (FTP) and Real-Time Streaming Protocol (RTSP) only. • **mac-miss**—Limits the ACE traffic sent to the control plane when the encapsulation is not correct in packets per second. • **mgmt-traffic**—Limits the management traffic in bytes per second. • **ssl-connections**—Limits the number of SSL connections per second. • **syslog**—Limits the number of syslog messages per second.
regexp	Limits the amount of regular expression memory.
sticky	Limits the number of entries in the sticky table. You must configure a minimum value for sticky to allocate resources for sticky entries, because the sticky software receives no resources under the unlimited setting.
xlates	Limits the number of network and port address translations entries.

minimum *number*	Specifies the lowest acceptable value. Enter an integer from 0.00 to 100.00 percent (two-decimal places of granularity). The *number* argument specifies a percentage value for all contexts that are members of the class. When used with the **rate** keyword, the *number* argument specifies a value per second.
maximum {**equal-to-min** | **unlimited**}	Specifies the maximum resource value: either the same as the minimum value or no limit.

Command Modes

Resource configuration mode

Admin context only

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You can limit all resources or individual resources for all members (contexts) of a resource class. For example, you can limit only concurrent connections, probes, or sticky table entries.

For details about the system resource maximum values when you use the **limit-resource** command, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*

To use the stickiness feature, you must configure a minimum limit for sticky resources. For more information, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

If you lower the limits for one context (context A) to increase the limits of another context (context B), you may experience a delay in the configuration change because the ACE will not lower the limits of context A until the resources are no longer being used by the context.

The limit that you set for individual resources when you use the **limit-resource** command overrides the limit that you set for all resources when you use the **limit-resource all** command.

Examples

To allocate 20 percent of all resources (minimum and maximum) to all member contexts of the resource class, enter:

```
(config-resource)# limit-resource all minimum 20% maximum equal-to-min
```

To restore resource allocation to the default of 0 percent minimum and 100 percent maximum for all resources to all member contexts, enter:

```
(config-resource)# no limit-resource all
```

Related Commands

This command has no related commands.

Role Configuration Mode Commands

Role configuration mode commands allow you to define various rules for users who are assigned a role and optionally, to describe a role definition. Roles determine the privileges that a user has, the commands a user can enter, and the actions that a user can perform in a particular context.

To assign a role and access role configuration mode, enter the **role** command in configuration mode. The CLI prompt changes to (config-role). For information about the commands in role configuration mode, see the commands in this section. Use the **no** form of this command to remove the user role assignment.

role *name*

no role *name*

Syntax Description

name	Identifier associated with a user role. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the context Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

If you do not assign a user role to a new user, the default user role is Network-Monitor. For users that you create in the Admin context, the default scope of access is the entire device. For users that you create in other contexts, the default scope of access is the entire context. If you need to restrict a user's access, you must assign a role-domain pair using the **(config) username** command.

Examples

To assign a role, enter:

```
host1/C1(config)# role TECHNICIAN
host1/C1(config-role)#
```

To remove the role from the configuration, enter:

```
host1/C1(config)# no role TECHNICIAN
```

Related Commands

This command has no related commands.

(config-role) description

To enter a description for the role, use the **description** command. Use the **no** form of this command to remove the role description from the configuration.

description *text*

no description

Syntax Description

text	Description for the role. Enter a description as an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Role configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

This example shows how to provide an additional description about a role:

```
host1/C1(config-role)# description DEFINES TECHNICIAN ROLE
```

To remove the description from the configuration, enter:

```
host1/C1(config)# no description DEFINES TECHNICIAN ROLE
```

Related Commands

This command has no related commands.

(config-role) rule

To assign privileges on a per-feature basis to a role, use the **rule** command. You can limit the features that a user has access to and the commands that the user can enter for that feature by configuring rules for roles. Use the **no** form of this command to remove the rule from a user role.

rule *number* {{**permit** | **deny**} {**create** | **modify** | **debug** | **monitor**} [**feature** {**AAA** | **access-list** | **changeto** | **config-copy** | **connection** | **dhcp** | **exec-commands** | **fault-tolerant** | **inspect** | **interface** | **loadbalance** | **nat** | **pki** | **probe** | **real-inservice** | **routing** | **rserver** | **serverfarm** | **sticky** | **syslog** | **vip**}]}

no rule *number*

Syntax Description

number	Identifier of the rule and order of precedence. Enter a unique integer from 1 to 16. The rule number determines the order in which the ACE applies the rules, with a higher-numbered rule applied after a lower-numbered rule.
permit	Allows the role to perform the operations defined by the rest of the command keywords.
deny	Disallows the role to perform the operations defined by the rest of the command keywords.
create	Specifies commands for the creation of new objects or the deletion of existing objects (includes **modify**, **debug**, and **monitor** commands).
debug	Specifies commands for debugging problems (includes **monitor** commands).
modify	Specifies commands for modifying existing configurations (includes **debug** and **monitor** commands).
monitor	Specifies commands for monitoring resources and objects (**show** commands).
feature	(Optional) Specifies a particular ACE feature for which you are configuring this rule. The available features are listed below.
AAA	Specifies commands for authentication, authorization, and accounting.
access-list	Specifies commands for access control lists (ACLs). Includes ACL configuration, class maps for ACLs, and policy maps that contain ACL class maps.
changeto	Specifies the **changeto** command for user-defined roles. Users retain their privileges when accessing different contexts. By default, this command is disabled for user-defined roles.
config-copy	Specifies commands for copying the running-config to the startup-config, startup-config to the running-config, and copying both config files to the Flash disk (disk0:) or a remote server.
connection	Specifies commands for network connections.
dhcp	Specifies commands for Dynamic Host Configuration Protocol (DHCP).
exec-commands	Specifies the following command for user-defined roles: **capture**, **debug**, **delete**, **gunzip**, **mkdir**, **move**, **rmdir**, **set**, **setup**, **system**, **tac-pac**, **untar**, **write**, and **undebug** commands. By default, these command are disabled for user-defined roles.
fault-tolerant	Specifies commands for redundancy.
inspect	Specifies commands for packet inspection used in data-center security.

interface	Specifies all interface commands.
loadbalance	Specifies commands for load balancing (including the application acceleration and optimization functions). Allows adding a load-balancing action in a policy map.
nat	Specifies commands for Network Address Translation (NAT) associated with a class map in a policy map used in data-center security.
pki	Specifies commands for Public Keyword Infrastructures (PKIs).
probe	Specifies commands for keepalives for real servers.
real-inservice	Specifies commands for placing a real server in service.
routing	Specifies all commands for routing, both global and per interface.
rserver	Specifies commands for physical servers.
serverfarm	Specifies commands for server farms.
sticky	Specifies commands for server persistence.
syslog	Specifies the system logging facility setup commands.
vip	Specifies commands for virtual IP addresses.

Command Modes

Role configuration mode.

Command History

Release	Modification
A1(7)	This command was introduced.
A3(2.2)	The **changeto** and **exec-commands** options were added to this command.

Usage Guidelines

This command has no usage guidelines.

Examples

To configure a rule that allows a role to create and configure real servers, enter:

```
host1/C1(config-role)# rule 1 permit create rserver
```

To remove the rule from a role, enter:

```
host1/C1(config-role)# no rule 1 permit create rserver
```

Related Commands

This command has no related commands.

Server Farm Host Configuration Mode Commands

Serverfarm host configuration mode commands allow you to create and configure host server farms and associate host real servers with the server farm. Host server farms are clusters of real servers that provide web content or services in a data center. You must configure a real server using the **(config) rserver** command in configuration mode before you can associate it with a server farm.

To create a host server farm and access serverfarm host configuration mode, use the **serverfarm** command. Note that host is the default server-farm type, so you do not need to enter the **host** option. The CLI prompt changes to (config-sfarm-host). For information about the commands in this mode, see the following commands.

Use the **no** form of this command to remove a server farm from the configuration.

serverfarm [**host**] *name*

no serverfarm *name*

Syntax Description

host	(Optional) Specifies a server farm of mirrored real servers that provide web content or services.
name	Unique identifier of the server farm. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the server-farm feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To create a host server farm named SFARM1, enter:

```
host1/Admin(config)# serverfarm SFARM1
host1/Admin(config-sfarm-host)#
```

To delete the server farm named SFARM1, enter:

```
host1/Admin(config)# no serverfarm SFARM1
```

Related Commands

show serverfarm
show running-config
(config) rserver

(config-sfarm-host) description

To configure the description of a server farm, use the **description** command. Use the **no** form of this command to delete the description of a server farm.

description *text*

no description

Syntax Description

text	Text description of a server farm. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Serverfarm host configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To configure a description of a server farm, enter:

```
host1/Admin(config-sfarm-host)# description CURRENT EVENTS ARCHIVE
```

To delete the description of a server farm, enter:

```
host1/Admin(config-sfarm-host)# no description
```

Related Commands

This command has no related commands.

(config-sfarm-host) failaction

To configure the action that the ACE takes if a real server in a server farm goes down, use the **failaction** command. Use the **no** form of this command to reset the ACE to its default of taking no action when a server fails.

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

no failaction

Syntax Description

purge	Specifies that the ACE remove the connections to a real server if that real server in the server farm fails after you configure this command. The appliance sends a reset (RST) both to the client and to the server that failed.
reassign	Specifies that the ACE reassigns existing server connections to the backup real server, if a backup real server is configured. If no backup real server is configured, this keyword has no effect.

Command Modes

Serverfarm host configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised (**reassign** keyword added).

Usage Guidelines

If you do not configure this command, the ACE takes the real server out of rotation for new connections and allows existing connections to complete. The ACE does not send the connections to a backup server in the server farm or to a backup server farm if all servers in the primary server farm fail. To clear connections to servers that have failed prior to entering the **failaction** command, use the clear conn command.

This feature is required for stateful firewall load balancing (FWLB). For details about FWLB, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*

The use of the **failaction reassign** command requires that you enable the **transparent** command (see (config-sfarm-host) transparent) to instruct the ACE not to use NAT to translate the ACE VIP address to the server IP address. The **failaction reassign** command is intended for use in FWLB where the destination IP address for the connection coming in to the ACE is for the end-point real server, and the ACE reassigns the connection so that it is transmitted through a different next hop.

Examples

To instruct the ACE to remove connections from a failed server in the server farm, enter:

```
host1/Admin(config-sfarm-host)# failaction purge
```

To specify that the ACE reassign the existing server connections to the backup real server, enter:

```
host1/Admin(config-sfarm-host)# failaction reassign
host1/Admin(config-sfarm-host)# transparent
```

To reset the ACE to its default of taking no action if a real server fails, enter:

```
host1/Admin(config-sfarm-host)# no failaction
```

Related Commands **(config-sfarm-host) transparent**

(config-sfarm-host) fail-on-all

To configure the real servers in a server farm to use AND logic with respect to multiple server farm probes, use the **fail-on-all** command in server farm host configuration mode. This command is applicable to all probe types. The syntax of this command is:

fail-on-all

no fail-on-all

Syntax Description

This command has no keywords or arguments.

Command Modes

Server farm host configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

By default, real servers that you configure in a server farm inherit the probes that you configure directly on that server farm. When you configure multiple probes on a server farm, the real servers in the server farm use an OR logic with respect to the probes. This means that if one of the probes configured on the server farm fails, all the real servers in that server farm fail and enter the PROBE-FAILED state.

With AND logic, if one server farm probe fails, the real servers in the server farm remain in the OPERATIONAL state. If all the probes associated with the server farm fail, then all the real servers in that server farm fail and enter the PROBE-FAILED state. You can also configure AND logic for probes that you configure directly on real servers in a server farm. For more information, see the command in server farm host real server configuration mode.

Examples

To configure the SERVER1 real server to remain in the OPERATIONAL state unless all associated probes fail, enter the following commands:

```
host1/Admin(config)# rserver SERVER1
host1/Admin(config-rserver-host)# ip address 192.168.12.15
host1/Admin(config-rserver-host)# probe HTTP_PROBE
host1/Admin(config-rserver-host)# probe ICMP_PROBE
host1/Admin(config-rserver-host)# fail-on-all
```

To remove the AND probe logic from the real server and return the behavior to the default of OR logic, enter the following command:

```
host1/Admin(config-rserver-host)# no fail-on-all
```

Related Commands

This command has no related commands.

(config-sfarm-host) partial-threshold

By default, if you configured a backup server farm and all real servers in the primary server farm go down, the primary server farm fails over to the backup server farm. Partial server farm failover allows you to specify a failover threshold. If the percentage of active real servers in a server farm falls below the specified threshold, the primary server farm fails over to the backup server farm (if configured).

To enable partial server farm failover, use the **partial-threshold** command in server farm host configuration mode. Use the **no** form of this command to disable partial server farm failover.

partial-threshold *percentage1* **back-inservice** *percentage2*

no partial-threshold

Syntax Description

percentage1	Minimum percentage of real servers in the primary server farm that must remain active for the server farm to stay up. If the percentage of active real servers falls below this threshold, the ACE takes the server farm out of service. Enter an integer from 0 to 99.
back-inservice *percentage2*	Specifies the percentage of real servers in the primary server farm that must be active again for the ACE to place the server farm back into service. Enter an integer from 0 to 99. The percentage configured with the **back-inservice** keyword must be greater than or equal to the *percentage1* value.

Command Modes

Server-farm host configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

Each time that a server is taken out of service (for example, by an administrator using the CLI, because of a probe failure, or because the retcode threshold is exceeded), the ACE is updated. If the percentage of active real servers in a server farm falls below the specified threshold, the primary server farm fails over to the backup server farm (if a backup server farm is configured).

With partial server farm failover configured, the ACE allows current connections on the remaining active servers in the failed primary server farm to complete. The ACE redirects any new connection requests to the backup server farm.

Examples

To configure partial server farm failover, enter:

```
host1/Admin(config-sfarm-host)# partial-threshold 40 back-inservice 60
```

To disable partial server farm failover, enter:

```
host1/Admin(config-sfarm-host)# no partial-threshold
```

Related Commands show serverfarm

(config-sfarm-host) predictor

To configure the load-balancing algorithm for the server farm, use the **predictor** command. Use the **no** form of this command to revert to the default load-balancing algorithm (the round-robin algorithm).

predictor {**hash** {**address** [**destination** | **source**] [*netmask*]} | {**content** [**offset** *number1*] [**length** *number2*] [**begin-pattern** *expression1*] [**end-pattern** *expression2*]} | {**cookie** [**secondary**] *name1*} | {**header** *name2*} | {**layer4-payload** [**offset** *number3*] [**length** *number4*] [**begin-pattern** *expression3*] [**end-pattern** *expression4*]} | {**url** [**begin-pattern** *expression5*] [**end-pattern** *expression6*]}} | {**least-bandwidth** [**samples** *number5*] [**assess-time** *seconds*]} | {**least-loaded probe** *name3* [**samples** *number6*]} | {**leastconns** [**slowstart** *seconds*]} | {**response** {**app-req-to-resp** | **syn-to-close** | **syn-to-synack**} [**samples** *number7*]} | {**roundrobin**}

no predictor

Syntax Description

hash address	Selects the server using a hash value based on the source and destination IP addresses. Use the **hash address source** and **hash address destination** methods for firewall load balancing (FWLB).
destination	(Optional) Selects the server using a hash value based on the destination IP address.
source	(Optional) Selects the server using a hash value based on the source IP address.
netmask	(Optional) Bits in the IP address to use for the hash. If not specified, the default is 255.255.255.255.
hash content	Selects the server using a hash value based on the specified content string of the HTTP packet body.
offset *number1*	(Optional) Specifies the portion of the content that the ACE uses to stick the client on a particular server by indicating the bytes to ignore starting with the first byte of the payload. Enter an integer from 0 to 999. The default is 0, which indicates that the ACE does not exclude any portion of the content.
length *number2*	(Optional) Specifies the length of the portion of the content (starting with the byte after the offset value) that the ACE uses for sticking the client to the server. Enter an integer from 1 to 1000. The default is the entire payload. The offset and length can vary from 0 to 1000 bytes. If the payload is longer than the offset but shorter than the offset plus the length of the payload, the ACE sticks the connection based on that portion of the payload starting with the byte after the offset value and ending with the byte specified by the offset plus the length. The total of the offset and the length cannot exceed 1000. Note: You cannot specify both the **length** and the **end-pattern** options in the same **hash content** command.

begin-pattern *expression1*	(Optional) Specifies the beginning pattern of the content string and the pattern string to match before hashing. If you do not specify a beginning pattern, the ACE starts parsing the HTTP body immediately following the offset byte. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters for each pattern that you configure. You can enter a text string with spaces if you enclose the entire string in quotation marks (“). The ACE supports the use of regular expressions for matching string expressions. When matching data strings, note that the period (.) and question mark (?) characters do not have a literal meaning in regular expressions. Use brackets ([]) to match these symbols (for example, enter www[.]xyz[.]com instead of www.xyz.com). You can also use a backslash (\) to escape a dot (.) or a question mark (?).
end-pattern *expression2*	(Optional) Specifies the pattern that marks the end of hashing. If you do not specify either a length or an end pattern, the ACE continues to parse the data until it reaches the end of the field or the end of the packet, or until it reaches the maximum body parse length. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters for each pattern that you configure. You can enter a text string with spaces if you enclose the entire string in quotation marks (“). The ACE supports the use of regular expressions for matching string expressions. Note: You cannot specify both the **length** and the **end-pattern** options in the same **hash content** command.
hash cookie	Selects the server using a hash value based on the cookie name or based on the name in the cookie name of the URL query string.
secondary	(Optional) Selects the server by using the hash value based on the specified name in the cookie name in the URL query string, not the cookie header. If you do not include this option, the ACE selects a real server using the hash value of the cookie name.
name1	Cookie name. Enter a cookie name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

hash header *name2*	Selects the server using a hash value based on the header name. Enter a header name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters, or enter one of the following standard headers: • **Accept** • **Accept-Charset** • **Accept-Encoding** • **Accept-Language** • **Authorization** • **Cache-Control** • **Connection** • **Content-MD5** • **Expect** • **From** • **Host** • **If-Match** • **Pragma** • **Referrer** • **Transfer-Encoding** • **User-Agent** • **Via**
hash layer4-payload	Specifies a Layer 4 generic protocol load-balancing method. Use this predictor to load balance packets from protocols that are not explicitly supported by the ACE.
offset *number3*	(Optional) Specifies the portion of the payload that the ACE uses to stick the client on a particular server by indicating the bytes to ignore starting with the first byte of the payload. Enter an integer from 0 to 999. The default is 0, which indicates that the ACE does not exclude any portion of the payload.
length *number4*	(Optional) Specifies the length of the portion of the payload (starting with the byte after the offset value) that the ACE uses for sticking the client to the server. Enter an integer from 1 to 1000. The default is the entire payload. The offset and length can vary from 0 to 1000 bytes. If the payload is longer than the offset but shorter than the offset plus the length of the payload, the ACE sticks the connection based on that portion of the payload starting with the byte after the offset value and ending with the byte specified by the offset plus the length. The total of the offset and the length cannot exceed 1000. Note: You cannot specify both the **length** and the **end-pattern** options in the same **hash layer4-payload** command.

begin-pattern *expression3*	(Optional) Specifies the beginning pattern of the Layer 4 payload and the pattern string to match before hashing. If you do not specify a beginning pattern, the ACE starts parsing the HTTP body immediately following the offset byte. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters for each pattern that you configure. You can enter a text string with spaces if you enclose the entire string in quotation marks (“). The ACE supports the use of regular expressions for matching string expressions. When matching data strings, note that the period (.) and question mark (?) characters do not have a literal meaning in regular expressions. Use brackets ([]) to match these symbols (for example, enter www[.]xyz[.]com instead of www.xyz.com). You can also use a backslash (\) to escape a dot (.) or a question mark (?).
end-pattern *expression4*	(Optional) Specifies the pattern that marks the end of hashing. If you do not specify either a length or an end pattern, the ACE continues to parse the data until it reaches the end of the field or the end of the packet, or until it reaches the maximum body parse length. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters for each pattern that you configure. You can enter a text string with spaces if you enclose the entire string in quotation marks (“). The ACE supports the use of regular expressions for matching string expressions. Note: You cannot specify both the **length** and the **end-pattern** options in the same **hash layer4-payload** command.
hash url	Selects the server using a hash value based on the requested URL. Use this predictor method to load balance cache servers. Cache servers perform better with the URL hash method because you can divide the contents of the caches evenly if the traffic is random enough. In a redundant configuration, the cache servers continue to work even if the active ACE switches over to the standby ACE. For information about configuring redundancy, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.
begin-pattern *expression5*	(Optional) Specifies the beginning pattern of the URL and the pattern string to match before hashing. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters for each pattern that you configure. If you want to match a URL that contains spaces, you must use **\x20** for each space character.

end-pattern *expression6*	(Optional) Specifies the pattern that marks the end of hashing. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters for each pattern that you configure. If you want to match a URL that contains spaces, you must use **\x20** for each space character.
least-bandwidth	Selects the server that processed the least amount of network traffic over a specified sampling period. Use this predictor for heavy traffic use, such as downloading a video clip. The ACE measures traffic statistics between itself and the real servers in the server farm in both directions and calculates the bandwidth over the sampling period. Then, it creates an ordered list of real servers based on the sampling results and selects the server that used the least amount of bandwidth during the sampling period.
samples *number5*	(Optional) Specifies the number of samples over which you want to weight and average the results of the probe query to calculate the final load value. Enter an integer from 1 to 16. Each value must be a power of 2, so the valid values are as follows: 1, 2, 4, 8, and 16. The default is 8.
assess-time *seconds*	(Optional) Specifies the sampling period over which the ACE measures traffic for all the servers in the server farm. Enter an integer from 1 to 10. The default is 2 seconds.
least-loaded	Selects the server with the lowest load based on information obtained from SNMP probes. To use this predictor, you must associate an SNMP probe with the server farm. The ACE queries one user-specified OID (for example, CPU utilization or memory utilization). The ACE uses the retrieved value directly to determine the server with the lowest load.
probe *name3*	Specifies the name of the SNMP probe that you want to query. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
samples *number6*	(Optional) Specifies the number of samples over which you want to weight and average the results of the probe query to calculate the final load value. Enter an integer from 1 to 16. Each value must be a power of 2, so the valid values are as follows: 1, 2, 4, 8, and 16. The default is 8.
leastconns	Selects the real server with the fewest number of active connections based on the server weight. Use this predictor for processing light user requests (for example, browsing simple static web pages). For information about setting real server weight, see the (config-sfarm-host-rs) weight section.
slowstart *seconds*	(Optional) Specifies that the connections to the real server be in a slow-start mode for the duration indicated by the *seconds* value. Use the slow-start mechanism to avoid sending a high rate of new connections to servers that you have recently put into service. Enter an integer from 1 to 65535, where 1 is the slowest ramp-up value. By default, **slowstart** is disabled.

response	Selects the server with the lowest response time for the requested response-time measurement. If you do not specify a response-time measurement method, the ACE uses the HTTP app-req-to-response method.
app-req-to-resp	(Default) Measures the response time from when the ACE sends an HTTP request to a server to the time that the ACE receives a response from the server for that request.
syn-to-close	Measures the response time from when the ACE sends a TCP SYN to a server to the time that the ACE receives a CLOSE from the server.
syn-to-synack	Measures the response time from when the ACE sends a TCP SYN to a server to the time that the ACE receives the SYN-ACK from the server.
samples *number7*	(Optional) Number of samples over which you want to average the results of the response time measurement. Enter an integer from 1 to 16 in powers of 2. Valid values are: 1, 2, 4, 8, and 16. The default is 8.
roundrobin	(Default) Selects the next server in the list of real servers based on server weight (weighted round-robin). For information about setting real server weight, see the (config-sfarm-host-rs) weight section.

Command Modes

Server-farm host configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised.
A3(2.2)	This **secondary** option for the **hash cookie** keywords was added.

Usage Guidelines

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

The weight assigned to the real servers is used only in the **roundrobin** and **leastconns** predictor methods. The **hash** and the **response** predictor methods do not recognize the weight for the real servers. For information about setting real server weight, see the (config-sfarm-host-rs) weight section.

If you configure the **leastconns** predictor, you can use a **slowstart** mechanism (ramp-up) to avoid sending a high rate of new connections to the servers that have just been put in service. The real server with the fewest number of active connections will get the next connection request for the server farm with the **leastconns** predictor. The ramp-up stops when the duration timer that you specify expires.

The only time that the sequence of servers starts over at the beginning (with the first server) is when there is a configuration or server state change (for example, a probe failure).

Server weights take effect only when there are open connections to the servers. When there are no sustained connections to any of the servers, the leastconns predictor method behaves like the roundrobin method.

Examples

To configure the ACE to select the real server with the lowest number of connections in the server farm, enter:

```
host1/Admin(config-sfarm-host)# predictor leastconns slowstart 300
```

To reset the load-balancing algorithm to the default of roundrobin, enter:

```
host1/Admin(config-sfarm-host)# no predictor
```

Related Commands

(config-sfarm-host-rs) weight

(config-sfarm-host) probe

Use probes to monitor the health of real servers in a server farm. To associate a probe with a server farm, use the **probe** command. Use the **no** form of this command to dissociate a probe from a server farm.

probe *probe-name*

no probe *probe-name*

Syntax Description

probe-name	Identifier of an existing probe that you want to associate with a server farm. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Serverfarm host configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The probe must already exist. (To create a probe, see the **(config) probe** command.) You can associate multiple probes of the same or different protocols with each server farm.

Examples

To associate a probe with a server farm, enter:

```
host1/Admin(config-sfarm-host)# probe TCP1
```

To dissociate a probe from a server farm, enter:

```
host1/Admin(config-sfarm-host)# no probe TCP1
```

Related Commands

(config) probe

(config-sfarm-host) retcode

To configure HTTP return-code checking (retcode map) for a server farm, use the **retcode** command. Use the **no** form of this command to dissociate a return code map. You can specify a single return code number or a range of return code numbers. For example, you can instruct the ACE to check for and count the number of occurrences of such return codes as HTTP/1.1 200 OK, HTTP/1.1 100 Continue, or HTTP/1.1 404 Not Found.

retcode *number1 number2* **check** {**count** | {**log** *threshold_number* **reset** *seconds1*
| {**remove** *threshold_number* **reset** *seconds1* [**resume-service** *seconds2*]}}

no retcode *number1 number2*

Syntax Description

number1	Minimum value for an HTTP return code. Enter an integer from 100 to 599. The minimum value must be less than or equal to the maximum value.
number2	Maximum value for an HTTP return code. Enter an integer from 100 to 599. The maximum value must be greater than or equal to the minimum value.
check	Checks for HTTP return codes associated with the server farm.
count	Tracks the total number of return codes received for each return code number that you specify.
log	Specifies a syslog error message when the number of events reaches the threshold specified by the *threshold_number* argument.
remove	Specifies a syslog error message when the number of events reaches the threshold specified by the *threshold_number* argument and the ACE removes the server from service.
threshold_number	Threshold for the number of events that the ACE receives before it performs the **log** or **remove** action. Enter an integer from 1 to 4294967295.
reset *seconds1*	Specifies the time interval in seconds over which the ACE checks for the return code for the **log** or **remove** action. Enter an integer from 1 to 4294967295.
resume-service *seconds2*	(Optional) Specifies the number of seconds that the ACE waits before it resumes service for the real server automatically after taking the real server out of service because the **remove** option is configured. Enter an integer from 30 to 3600. The default setting is 300.

Command Modes

Server-farm host configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised.

Usage Guidelines

You can configure multiple return code maps on each server farm. You can view hitcounts for return code checking by using the **show serverfarm** command.

Examples

To check for and count the number of return code hits for all return codes from 200 to 500 inclusive, enter:

```
host1/Admin(config-sfarm-host)# retcode 200 500 check count
```

To remove the HTTP return-code map from the configuration, enter:

```
host1/Admin(config-sfarm-host)# no retcode 200 500
```

Related Commands

show serverfarm

(config-sfarm-host) rserver

To associate one or more existing host real servers with a server farm and access serverfarm host real server configuration mode, use the **rserver** command. The CLI prompt changes to (config-sfarm-host-rs). For information on commands in serverfarm host real server configuration mode, see the "Server Farm Host Real Server Configuration Mode Commands" section. Use the **no** form of this command to dissociate the real server from the server farm.

rserver *name* [*port*]

no rserver *name* [*port*]

Syntax Description

name	Unique identifier of the real server. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
port	(Optional) Port number used for the real server Port Address Translation (PAT). Enter an integer from 1 to 65535.

Command Modes

Serverfarm host configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The real server must already exist. To create a real server, see the **(config) rserver** command. You can associate a maximum of 16,384 real servers with a server farm.

If you choose not to assign a port number for the real server association with the server farm, the default behavior by the ACE is to automatically assign the same destination port that was used by the inbound connection to the outbound server connection. For example, if the incoming connection to the ACE is a secure client HTTPS connection, the connection is typically made on port 443. If you do not assign a port number to the real server, the ACE will automatically use port 443 to connect to the server, which results in the ACE making a clear-text HTTP connection over port 443. In this case, you would typically define an outbound destination port of 80, 81, or 8080 for the backend server connection.

Examples

To associate a real server with a server farm, enter:

```
host1/Admin(config-sfarm-host)# rserver server1 80
```

To dissociate a real server from a server farm, enter:

```
host1/Admin(config-sfarm-host)# no rserver server1 80
```

Related Commands

(config) rserver

(config-sfarm-host) transparent

To configure the ACE not to use Network Address Translation (NAT) to translate the ACE VIP address to the server IP address, use the **transparent** command. Use the **no** form of this command to reset the ACE to its default of using NAT to translate the VIP address to the server IP address.

transparent

no transparent

Syntax Description

This command has no keywords or arguments.

Command Modes

Serverfarm host configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Use this command in firewall load balancing (FWLB) when you configure the insecure and secure sides of the firewall as a server farm. For details about FWLB, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To prevent the ACE from using NAT to translate the ACE VIP address to the server IP address, enter:

```
host1/Admin(config-sfarm-host)# transparent
host1/Admin(config-sfarm-host)#
```

To reset the ACE to its default of using NAT to translate the VIP address to the server IP address, enter:

```
host1/Admin(config-sfarm-host)# no transparent
host1/Admin(config-sfarm-host)#
```

Related Commands

This command has no related commands.

Serverfarm Host Predictor Configuration Mode Commands

Serverfarm host predictor configuration mode commands allow you to configure additional parameters for some of the server farm predictor methods.

To configure these additional predictor parameters, use the **predictor least-loaded** or the **predictor response** command in serverfarm host configuration mode. The CLI prompt changes to (config-sfarm-host-predictor). For information about the commands in this mode, see the following commands. Use the **no** form of this command to remove the predictor from the server farm.

predictor {**least-loaded probe** *name*} | {**response** {**app-req-to-resp** | **syn-to-close** | **syn-to-synack**}[**samples** *number*]}}

no predictor

Syntax Description

least-loaded	Selects the server with the lowest load based on information obtained from SNMP probes. To use this predictor, you must associate an SNMP probe with the server farm. The ACE queries one user-specified OID (for example, CPU utilization or memory utilization). The ACE uses the retrieved value directly to determine the server with the lowest load.
probe *name*	Specifies the name of the SNMP probe that you want to query. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
response	Selects the server with the lowest response time for the requested response-time measurement. If you do not specify a response-time measurement method, the ACE uses the HTTP app-req-to-response method.
app-req-to-resp	(Default) Measures the response time from when the ACE sends an HTTP request to a server to the time that the ACE receives a response from the server for that request.
syn-to-close	Measures the response time from when the ACE sends a TCP SYN to a server to the time that the ACE receives a CLOSE from the server.

syn-to-synack	Measures the response time from when the ACE sends a TCP SYN to a server to the time that the ACE receives the SYN-ACK from the server.
samples *number*	(Optional) Number of samples over which you want to average the results of the response time measurement. Enter an integer from 1 to 16 in powers of 2. Valid values are: 1, 2, 4, 8, and 16. The default is 8.

Command Modes

Serverfarm host configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The commands in this mode require the server-farm feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To specify the least-loaded predictor method with a probe called SNMP_PROBE for the server farm, enter:

```
host1/Admin(config-sfarm-host)# predictor least-loaded probe SNNMP_PROBE
host1/Admin(config-sfarm-host-predictor)#
```

To remove the least-loaded predictor from the server farm, enter:

```
host1/Admin(config-sfarm-host)# no predictor
```

To specify the response predictor method that measures the response time from when the ACE sends an HTTP request to a server to the time that the ACE receives a response from the server for that request, enter:

```
host1/Admin(config-sfarm-host)# predictor response app-req-to-resp
host1/Admin(config-sfarm-host-predictor)#
```

To remove the response predictor from the server farm, enter:

```
host1/Admin(config-sfarm-host)# no predictor
```

Related Commands

show serverfarm detail
(config-sfarm-host) predictor
(config-sfarm-host-predictor) autoadjust
(config-sfarm-host-predictor) weight connection

(config-sfarm-host-predictor) autoadjust

After you specify the **predictor least-loaded** command, use the **autoadjust** command to apply the average load of the server farm to a real server whose load reaches zero. Use the **no** form of this command to return the ACE behavior to the default of assigning a maximum load value of 16000 to a server whose load has reached zero to prevent it from being flooded with new incoming connections.

autoadjust {**average** | **off**}

no autoadjust

Syntax Description

average	Instructs the ACE to apply the average load of the server farm to a real server whose load reaches zero. The average load is the running average of the load values across all real servers in the server farm.
off	Overrides the default behavior of the ACE of setting the load value for a server with a load of zero to 16000. When you configure this command, the ACE sends all new connections to the server that has a load of zero until the next load update arrives from the SNMP probe for this server.

Command Modes

Serverfarm host predictor configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

Whenever a server's load reaches zero, by default, the ACE uses the autoadjust feature to assign a maximum load value of 16000 to that server to prevent it from being flooded with new incoming connections. The ACE periodically adjusts this load value based on feedback from the server's SNMP probe and other configured options.

Using the least-loaded predictor with the configured server weight and the current connection count option enabled, the ACE calculates the final load of a real server as follows:

final load = *weighted load* × *static weight* × *current connection count*

where:

- *weighted load* is the load reported by the SNMP probe
- *static weight* is the configured weight of the real server
- *current connection count* is the total number of active connections to the real server

The ACE recalculates the final load whenever the connection count changes, provided that the **(config-sfarm-host-predictor) weight connection** command is configured. If the **(config-sfarm-host-predictor) weight connection** command is not configured, the ACE updates the final load when the next load update arrives from the SNMP probe.

If two servers have the same lowest load (either zero or nonzero), the ACE load balances the connections between the two servers in a round-robin manner.

Examples

To instruct the ACE to apply the average load of the server farm to a real server whose load reaches zero, enter:

```
host1/Admin(config-sfarm-host-predictor)# autoadjust average
```

To turn off the autoadjust feature for all servers in a server farm so that servers with a load of zero receive all new connections, enter:

```
host1/Admin(config-sfarm-host-predictor)# autoadjust off
```

To reset the behavior of the ACE to the default of applying the maximum load value of 16000 to a real server whose load is zero, enter:

```
host1/Admin(config-sfarm-host-predictor)# no autoadjust average
host1/Admin(config-sfarm-host-predictor)# no autoadjust off
```

Related Commands

show serverfarm detail
(config-sfarm-host) predictor
(config-sfarm-host-predictor) weight connection

(config-sfarm-host-predictor) weight connection

After you specify the **predictor least-loaded** or the **predictor response** command, use the **weight connection** command to instruct the ACE to use the current connection count in the final load calculation for each real server in the server farm. Use the **no** form of this command to reset the behavior of the ACE to the default of excluding the current connection count from the load calculation.

weight connection

no weight connection

Syntax Description

This command has no keywords or arguments.

Command Modes

Serverfarm host predictor configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

To see how the **weight connection** command affects the **(config-sfarm-host-predictor) autoadjust** command for the least-loaded predictor, see the Usage Guidelines section of the **(config-sfarm-host-predictor) autoadjust** command.

Examples

To instruct the ACE to use the current connection count in the final load calculation for each real server in the server farm, enter:

```
host1/Admin(config-sfarm-host-predictor)# weight connection
```

To reset the behavior of the ACE to the default of excluding the current connection count from the load calculation, enter:

```
host1/Admin(config-sfarm-host-predictor)# no weight connection
```

Related Commands

show serverfarm detail
(config-sfarm-host) predictor
(config-sfarm-host-predictor) autoadjust

Server Farm Host Real Server Configuration Mode Commands

Serverfarm host real server configuration mode commands allow you to associate a host real server with a host server farm and configure the real server attributes.

To associate one or more existing host real servers with a host server farm and access serverfarm host real server configuration mode, use the **rserver** command in serverfarm host configuration mode. The CLI prompt changes to (config-sfarm-host-rs). For information about the commands in this mode, see the following commands. Use the **no** form of this command to remove the real server from the server farm.

rserver *name* [*port*]

no rserver *name*

Syntax Description

name	Unique identifier of the real server. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
port	(Optional) Port number used for the real server Port Address Translation (PAT). Enter an integer from 1 to 65535.

Command Modes

Serverfarm host configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the server-farm feature in your user role unless otherwise specified. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The real server must already exist. To create a real server, see the **(config) rserver** command. You can associate a maximum of 16,384 real servers with a server farm.

Examples

To associate a real server with a server farm, enter:

```
host1/Admin(config-sfarm-host)# rserver SERVER1
```

To dissociate a real server from a server farm, enter:

```
host1/Admin(config-sfarm-host)# no rserver SERVER1
```

Related Commands

This command has no related commands.

(config-sfarm-host-rs) backup-rserver

To configure a backup real server for a real server in a server farm, use the **backup-rserver** command. If a real server associated with a server farm becomes unavailable, the ACE directs flows to the configured backup real server. Use the **no** form of this command to remove a backup real server from the configuration.

backup-rserver *name* [*port*]

no backup-rserver

Syntax Description

name	Unique identifier of an existing real server that you want to configure as a backup server in a server farm. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
port	(Optional) Port number used for the backup real server Port Address Translation (PAT). Enter an integer from 0 to 65535.

Command Modes

Serverfarm host real server configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(2.2)	This command now supports cyclic backup of real servers in a server farm.

Usage Guidelines

The real server used as a backup server must already exist. To create a real server, see the **(config) rserver** command.

Examples

To associate a backup real server with a server farm, enter:

```
host1/Admin(config-sfarm-host-rs)# backup-rserver BACKUP_SERVER1 3500
```

To dissociate a backup real server from a server farm, enter:

```
host1/Admin(config-sfarm-host-rs)# no backup-rserver
```

Related Commands

(config) rserver
(config-sfarm-host-rs) inservice

(config-sfarm-host-rs) conn-limit

To configure the maximum and minimum number of connections that you want to allow for a host real server in a server farm, use the **conn-limit** command. Use the **no** form of this command to reset the limits for the real server maximum connections and minimum connections to the default of4000000.

conn-limit max *maxconns* **min** *minconns*

no conn-limit

Syntax Description

max *maxconns*	Specifies the maximum number of connections allowed for this real server. Enter an integer from 2 to 4000000. The default is4000000.
min *minconns*	Specifies the connection threshold below which the real server will start accepting connections again after the number of connections exceeds the configured maximum number of connections. Enter an integer from 2 to4000000. The default is *minconns* equal to *maxconns*.

Command Modes

Serverfarm host real server configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Use this command to specify the maximum number of connections and the minimum connection threshold for a host real server in a server farm. The *minconns* value must be less than or equal to the *maxconns* value. The ACE uses the *minconns* value as a threshold to start accepting connections again after the *maxconns* limit is exceeded.

Examples

To configure the maximum number of connections and the minimum connection threshold for a host real server, enter:

```
host1/Admin(config-sfarm-host-rs)# conn-limit max 65535 min 40000
```

To reset the maximum number of connections and the minimum connection threshold for a host real server to the default of4000000, enter:

```
host1/Admin(config-sfarm-host-rs)# no conn-limit
```

Related Commands

(config-sfarm-host-rs) rate-limit

(config-sfarm-host-rs) cookie-string

To configure a cookie string value of the real server for HTTP cookie insertion when establishing a sticky connection, use the **cookie-string** command. Use the **no** form of this command to remove the user-defined cookie string value of the real server for cookie insertion and have the ACE generate the cookie string for the associated real server.

cookie-string *text_string*

no cookie-string

Syntax Description

text_string	Cookie string value for the real server. Enter a text string with a maximum of 32 alphanumeric characters. When you include spaces and special characters in a cookie string value, enter a quoted text string (for example, “test cookie string”). The quotes appear in the running-configuration file.

Command Modes

Serverfarm host real server configuration mode

Admin and user contexts

Command History

Release	Modification
A3(2.2)	This command was introduced.

Usage Guidelines

Use cookie insertion when you want to use a session cookie for persistence if the server is not currently setting the appropriate cookie. When you configure a cookie string value, the ACE inserts the cookie in the Set-Cookie header of the response from the server to the client.

If you do not configure a cookie string value, when you enable cookie insertion for a sticky group, the ACE generates the cookie string for each real server after sending a connection to it. The ACE-generated cookie string appears as “Rxxxxxxx” (for example, R2148819051).

When configuring a cookie string value, consider the following:

- You can configure one cookie string for each real server.
- The ACE automatically uses the user-defined cookie string for cookie insertion for a sticky group instead of the ACE-generated cookie string.
- Ensure that there are no duplicate strings configured for real servers. If there are duplicate cookie strings, the old entry will be removed and sticky database will use the latest configured cookie string for the real server.

If you remove the user-defined cookie string from a real server, the ACE generates the cookie string for the associated real server after sending a connection.

Examples

To configure a cookie string value of the real server for HTTP cookie insertion, enter:

```
host1/Admin(config-sfarm-host-rs)# cookie-string ABC123
```

To remove the configured cookie string value, enter:

```
host1/Admin(config-sfarm-host-rs)# no cookie-string
```

Related Commands **show sticky database** **strict**

(config-sfarm-host-rs) fail-on-all

To configure a real server in a server farm to remain in the OPERATIONAL state unless all probes associated with it fail (AND logic), use the **fail-on-all** command in server farm host real server configuration mode. This command is applicable to all probe types. The syntax of this command is:

fail-on-all

no fail-on-all

Syntax Description

This command has no keywords or arguments.

Command Modes

Server farm host real server configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

By default, multiple probes that you configure directly on a real server in a server farm have an OR logic associated with them. This means that, if one of the real server probes fails, then the real server fails and enters the PROBE-FAILED state.

You can selectively configure this command on only certain real servers in the server farm to give those server ADN logic. Any real server that you do not configure with the **fail-on-all** command, maintains its default OR logic with respect to probes.

Examples

For example, to configure the SERVER1 real server in SFARM1 to remain in the OPERATIONAL state unless all associated probes fail, enter the following commands:

```
host1/Admin(config)# serverfarm SFARM1
host1/Admin(config-sfarm-host)# rserver SERVER1
host1/Admin(config-sfarm-host-rs)# inservice
host1/Admin(config-sfarm-host-rs)# probe HTTP_PROBE
host1/Admin(config-sfarm-host-rs)# probe ICMP_PROBE
host1/Admin(config-sfarm-host-rs)# fail-on-all
```

If either HTTP_PROBE or ICMP_PROBE fails, the SERVER1 real server remains in the OPERATIONAL state. If both probes fail, the real server fails and enters the PROBE-FAILED state.

To remove the AND probe logic from the real server in a server farm and return the behavior to the default of OR logic, enter the following command:

```
host1/Admin(config-rserver-host)# no fail-on-all
```

Related Commands

This command has no related commands.

(config-sfarm-host-rs) inservice

To place a real server associated with a server farm in service, use the **inservice** command. Use the **no** form of this command to take a real server out of service.

inservice [**standby**]

no inservice

Syntax Description

standby	(Optional) Used with backup real servers, specifies that a backup real server remain inactive unless the primary real server fails. If the primary fails, the backup server becomes active and starts accepting connections.

Command Modes

Serverfarm host real server configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the real-inservice feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To start load balancing connections to a real server in a server farm, you must place the real server in service by using the **inservice** command.

You can modify the attributes of a real server in a server farm without taking the server out of service.

In addition to putting a backup real server in service standby, another use of the **inservice standby** command is to provide the graceful shutdown of primary real servers. Use this command to gracefully shut down servers with sticky connections. When you enter this command for a primary real server, the ACE does the following:

- Tears down existing non-TCP connections to the server
- Allows current TCP connections to complete
- Allows new sticky connections for existing server connections that match entries in the sticky database
- Load balances all new connections (other than the matching sticky connections mentioned above) to the other servers in the server farm
- Eventually takes the server out of service

Examples

To place a real server in service, enter:

```
host1/Admin(config-sfarm-host-rs)# inservice
```

To take a real server out of service, enter:

```
host1/Admin(config-sfarm-host-rs)# no inservice
```

To perform a graceful shutdown on a primary real server with sticky connections in a server farm, enter:

```
host1/Admin(config-sfarm-host-rs)# inservice standby
```

Related Commands

This command has no related commands.

(config-sfarm-host-rs) probe

To configure a probe to monitor the health of a host real server in a host server farm, use the **probe** command. Use the **no** form of this command to remove the probe from the real server.

probe *probe-name*

no probe *probe-name*

Syntax Description

probe-name	Identifier of an existing probe that you want to assign to a real server to monitor its health. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Serverfarm host real server configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You can associate multiple probes with each real server.

The ACE periodically sends the probes to the real servers. If the ACE receives the appropriate responses from the servers, the ACE includes the servers in load-balancing decisions. If not, the ACE marks the servers as out of service, depending on the configured number of retries.

Examples

To configure a probe for a host real server, enter:

```
host1/Admin(config-sfarm-host-rs)# probe SERVER1_PROBE
```

To remove a probe from a host real server, enter:

```
host1/Admin(config-sfarm-host-rs)# no probe SERVER1_PROBE
```

Related Commands

This command has no related commands.

(config-sfarm-host-rs) rate-limit

To configure a limit for the connection rate and the bandwidth rate of a real server in a host server farm, use the **rate-limit** command. The connection rate is the number of connections per second received by the ACE and destined to a particular real server. The bandwidth rate is the number of bytes per second received by the ACE and destined for a particular real server. Use the **no** form of this command to revert to the ACE default of not limiting the connection rate or bandwidth rate of real servers in a server farm.

rate-limit {**connection** *number1* | **bandwidth** *number2*}

no rate-limit {**connection** | **bandwidth**}

Syntax Description

connection *number1*	Specifies the real server connection-rate limit in connections per second. Enter an integer from 2 to 350000. There is no default value.
bandwidth *number2*	Specifies the real server bandwidth-rate limit in bytes per second. Enter an integer from 2 to 300000000. There is no default value.

Command Modes

Serverfarm host real server configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

If the connection rate or the bandwidth rate of incoming traffic destined for a particular real server exceeds the configured rate for the server, the ACE blocks any further traffic destined to that real server until the connection rate or bandwidth rate drops below the configured limit. Also, the ACE removes the blocked real server from future load-balancing decisions. By default, the ACE does not limit the connection rate or the bandwidth rate of real servers in a server farm.

Examples

To limit the connection rate of a real server to 100,000 connections per second, enter:

```
host1/Admin(config-sfarm-host-rs)# rate-limit connection 100000
```

To revert to the ACE default of not limiting the real-server connection rate, enter:

```
host1/Admin(config-sfarm-host-rs)# no rate-limit connection
```

To limit the real-server bandwidth rate to 5,000,000 bytes per second, enter:

```
host1/Admin(config-sfarm-host-rs)# rate-limit bandwidth 5000000
```

To revert to the ACE default of not limiting real-server bandwidth, enter:

```
host1/Admin(config-sfarm-host-rs)# no rate-limit bandwidth
```

Related Commands

(config-sfarm-host-rs) conn-limit

(config-sfarm-host-rs) weight

To configure the capacity of a real server in relation to other servers in a server farm, use the **weight** command. The weight value that you specify for a server is used in the weighted round-robin and least-connections predictor load-balancing methods. Use the **no** form of this command to reset the real server weight to the default.

weight *number*

no weight

Syntax Description

number	Weight value assigned to a real server in a server farm. This value is used in the weighted round-robin and least-connections predictor load-balancing algorithms. Enter an integer from 1 to 100. The default is 8.

Command Modes

Serverfarm host real server configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Servers with higher weight values receive a proportionally higher number of connections than servers with lower weight values. If you do not specify a weight in serverfarm host real server configuration mode, the ACE uses the weight that you configured for the global real server in real server host configuration mode.

To specify different weight values for a host real server in a server farm, you can assign multiple IP addresses to the server. You can also use the same IP address of a real server with different port numbers.

Server weights take effect only when there are open connections to the servers. When there are no sustained connections to any of the servers, the leastconns predictor method behaves like the roundrobin method.

Examples

To configure a weight value for a real server, enter:

```
host1/Admin(config-sfarm-host-rs)# weight 50
```

To reset the weight of a real server to the default of 8, enter:

```
host1/Admin(config-sfarm-host-rs)# no weight
```

Related Commands

(config-rserver-host) weight

(config-sfarm-host) predictor

Server Farm Redirect Configuration Mode Commands

Serverfarm redirect configuration mode commands allow you to create and configure redirect server farms and associate redirect real servers with the server farm. Redirect server farms are clusters of real servers that redirect users to alternative URLs where content has been moved, either temporarily or permanently. The server farm consists only of real servers that redirect client requests to alternative locations specified by the relocation string or port number in the real server configuration. You must configure a redirect real server using the **(config) rserver redirect** command in configuration mode before you can associate it with a server farm.

To create a redirect server farm and access serverfarm redirect configuration mode, use the **serverfarm redirect** command. The CLI prompt changes to (config-sfarm-redirect). For information about the commands in this mode, see the following commands.

Use the **no** form of this command to remove a server farm from the configuration.

serverfarm redirect *name*

no serverfarm redirect *name*

Syntax Description

name	Unique identifier of the server farm. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the server-farm feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To create a redirect server farm named SFARM2, enter:

```
host1/Admin(config)# serverfarm redirect SFARM2
host1/Admin(config-sfarm-redirect)#
```

To delete the redirect server farm named SFARM2, enter:

```
host1/Admin(config)# no serverfarm redirect SFARM2
```

Related Commands

show serverfarm
show running-config
(config) rserver

(config-sfarm-redirect) description

To configure the text description of a server farm, use the **description** command. Use the **no** form of this command to delete the description of a server farm.

description *text*

no description

Syntax Description

text	Text description of a server farm. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

Command Modes

Serverfarm redirect configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To configure a description of a server farm, enter:

```
host1/Admin(config-sfarm-redirect)# description REDIRECT_NEW_SITE
```

To delete the description of a server farm, enter:

```
host1/Admin(config-sfarm-redirect)# no description
```

Related Commands

This command has no related commands.

(config-sfarm-redirect) failaction

To configure the action that the ACE takes if a real server in a server farm goes down, use the **failaction** command. Use the **no** form of this command to reset the ACE to its default of taking no action when a server fails.

failaction {**purge** | **reassign** [**across-interface**]}

no failaction

Syntax Description

purge	Specifies that the ACE removes the connections to a real server in the server farm if that real server fails. The ACE sends a reset (RST) both to the client and to the server that failed.
reassign	Specifies that the ACE reassigns existing server connections to the backup real server if a backup real server is configured. If no backup real server is configured, this keyword has no effect.

Command Modes

Serverfarm redirect configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised (**reassign** keyword added).

Usage Guidelines

If you do not configure this command, the ACE takes the real server out of rotation for new connections and allows existing connections to complete. The ACE does not send the connections to a backup server in the server farm or to a backup server farm if all servers in the primary server farm fail.

This feature is required for stateful firewall load balancing (FWLB). For details about FWLB, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To instruct the ACE to remove connections from a failed server in the server farm, enter:

```
host1/Admin(config-sfarm-redirect)# failaction purge
```

To reset the ACE to its default of taking no action if a real server fails, enter:

```
host1/Admin(config-sfarm-redirect)# no failaction
```

Related Commands

This command has no related commands.

(config-sfarm-redirect) predictor

To configure the load-balancing algorithm for the server farm, use the **predictor** command. Use the **no** form of this command to revert to the default load-balancing algorithm (the round-robin algorithm).

predictor {**hash** {**address** [**destination** | **source**] [*netmask*]} | {**content** [**offset** *number1*] [**length** *number2*] [**begin-pattern** *expression1*] [**end-pattern** *expression2*]} | {**cookie** *name1*} | {**header** *name2*} | {**layer4-payload** [**offset** *number3*] [**length** *number4*] [**begin-pattern** *expression3*] [**end-pattern** *expression4*]} | {**url** [**begin-pattern** *expression5*] [**end-pattern** *expression6*]}} | {**least-bandwidth** [**samples** *number5*] [**assess-time** *seconds*]} | {**least-loaded probe** *name3* [**samples** *number6*]} | {**leastconns** [**slowstart** *seconds*]} | {**response** {**app-req-to-resp** | **syn-to-close** | **syn-to-synack**} [**samples** *number7*] [**threshold** *milliseconds* [**resume-timer** *seconds*]]} | {**roundrobin**}

no predictor

Syntax Description

hash address	Selects the server using a hash value based on the source and destination IP addresses. Use the **hash address source** and **hash address destination** methods for firewall load balancing (FWLB).
destination	(Optional) Selects the server using a hash value based on the destination IP address.
source	(Optional) Selects the server using a hash value based on the source IP address.
netmask	(Optional) Bits in the IP address to use for the hash. If not specified, the default is 255.255.255.255.
hash content	Selects the server using a hash value based on the specified content string of the HTTP packet body.
offset *number1*	(Optional) Specifies the portion of the content that the ACE uses to stick the client on a particular server by indicating the bytes to ignore starting with the first byte of the payload. Enter an integer from 0 to 999. The default is 0, which indicates that the ACE does not exclude any portion of the content.
length *number2*	(Optional) Specifies the length of the portion of the content (starting with the byte after the offset value) that the ACE uses for sticking the client to the server. Enter an integer from 1 to 1000. The default is the entire payload. The offset and length can vary from 0 to 1000 bytes. If the payload is longer than the offset but shorter than the offset plus the length of the payload, the ACE sticks the connection based on that portion of the payload starting with the byte after the offset value and ending with the byte specified by the offset plus the length. The total of the offset and the length cannot exceed 1000. You cannot specify both the **length** and the **end-pattern** options in the same **hash content** command.

begin-pattern *expression1*	(Optional) Specifies the beginning pattern of the content string and the pattern string to match before hashing. If you do not specify a beginning pattern, the ACE starts parsing the HTTP body immediately following the offset byte. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters for each pattern that you configure. You can enter a text string with spaces if you enclose the entire string in quotation marks (“). The ACE supports the use of regular expressions for matching string expressions. When matching data strings, note that the period (.) and question mark (?) characters do not have a literal meaning in regular expressions. Use brackets ([]) to match these symbols (for example, enter www[.]xyz[.]com instead of www.xyz.com). You can also use a backslash (\) to escape a dot (.) or a question mark (?).
end-pattern *expression2*	(Optional) Specifies the pattern that marks the end of hashing. If you do not specify either a length or an end pattern, the ACE continues to parse the data until it reaches the end of the field or the end of the packet, or until it reaches the maximum body parse length. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters for each pattern that you configure. You can enter a text string with spaces if you enclose the entire string in quotation marks (“). The ACE supports the use of regular expressions for matching string expressions. You cannot specify both the **length** and the **end-pattern** options in the same **hash content** command.
hash cookie *name1*	Selects the server using a hash value based on the cookie name. Enter a cookie name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

hash header *name2*	Selects the server using a hash value based on the header name. Enter a header name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters, or enter one of the following standard headers: • **Accept** • **Accept-Charset** • **Accept-Encoding** • **Accept-Language** • **Authorization** • **Cache-Control** • **Connection** • **Content-MD5** • **Expect** • **From** • **Host** • **If-Match** • **Pragma** • **Referrer** • **Transfer-Encoding** • **User-Agent** • **Via**
hash layer4-payload	Specifies a Layer 4 generic protocol load-balancing method. Use this predictor to load balance packets from protocols that are not explicitly supported by the ACE.
offset *number3*	(Optional) Specifies the portion of the payload that the ACE uses to stick the client on a particular server by indicating the bytes to ignore starting with the first byte of the payload. Enter an integer from 0 to 999. The default is 0, which indicates that the ACE does not exclude any portion of the payload.
length *number4*	(Optional) Specifies the length of the portion of the payload (starting with the byte after the offset value) that the ACE uses for sticking the client to the server. Enter an integer from 1 to 1000. The default is the entire payload. The offset and length can vary from 0 to 1000 bytes. If the payload is longer than the offset but shorter than the offset plus the length of the payload, the ACE sticks the connection based on that portion of the payload starting with the byte after the offset value and ending with the byte specified by the offset plus the length. The total of the offset and the length cannot exceed 1000. You cannot specify both the **length** and the **end-pattern** options in the same **hash layer4-payload** command.

begin-pattern *expression3*	(Optional) Specifies the beginning pattern of the Layer 4 payload and the pattern string to match before hashing. If you do not specify a beginning pattern, the ACE starts parsing the HTTP body immediately following the offset byte. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters for each pattern that you configure. You can enter a text string with spaces if you enclose the entire string in quotation marks (“). The ACE supports the use of regular expressions for matching string expressions. When matching data strings, note that the period (.) and question mark (?) characters do not have a literal meaning in regular expressions. Use brackets ([]) to match these symbols (for example, enter www[.]xyz[.]com instead of www.xyz.com). You can also use a backslash (\) to escape a dot (.) or a question mark (?).
end-pattern *expression4*	(Optional) Specifies the pattern that marks the end of hashing. If you do not specify either a length or an end pattern, the ACE continues to parse the data until it reaches the end of the field or the end of the packet, or until it reaches the maximum body parse length. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters for each pattern that you configure. You can enter a text string with spaces if you enclose the entire string in quotation marks (“). The ACE supports the use of regular expressions for matching string expressions. Note: You cannot specify both the **length** and the **end-pattern** options in the same **hash layer4-payload** command.
hash url	Selects the server using a hash value based on the requested URL. Use this predictor method to load balance cache servers. Cache servers perform better with the URL hash method because you can divide the contents of the caches evenly if the traffic is random enough. In a redundant configuration, the cache servers continue to work even if the active ACE switches over to the standby ACE. For information about configuring redundancy, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*.
begin-pattern *expression5*	(Optional) Specifies the beginning pattern of the URL and the pattern string to match before hashing. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters for each pattern that you configure. If you want to match a URL that contains spaces, you must use **\x20** for each space character.

end-pattern *expression6*	(Optional) Specifies the pattern that marks the end of hashing. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters for each pattern that you configure. If you want to match a URL that contains spaces, you must use **\x20** for each space character.
least-bandwidth	Selects the server that processed the least amount of network traffic over a specified sampling period. Use this predictor for heavy traffic use, such as downloading a video clip. The ACE measures traffic statistics between itself and the real servers in the server farm in both directions and calculates the bandwidth over the sampling period. Then, it creates an ordered list of real servers based on the sampling results and selects the server that used the least amount of bandwidth during the sampling period.
samples *number5*	(Optional) Specifies the number of samples over which you want to weight and average the results of the probe query to calculate the final load value. Enter an integer from 1 to 16. Each value must be a power of 2, so the valid values are as follows: 1, 2, 4, 8, and 16. The default is 8.
assess-time *seconds*	(Optional) Specifies the sampling period over which the ACE measures traffic for all the servers in the server farm. Enter an integer from 1 to 10. The default is 4 seconds.
least-loaded	Selects the server with the lowest load based on information obtained from SNMP probes. To use this predictor, you must associate an SNMP probe with the server farm. The ACE queries one user-specified OID (for example, CPU utilization or memory utilization). The ACE uses the retrieved value directly to determine the server with the lowest load.
probe *name3*	Specifies the name of the SNMP probe that you want to query. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
samples *number6*	(Optional) Specifies the number of samples over which you want to weight and average the results of the probe query to calculate the final load value. Enter an integer from 1 to 16. Each value must be a power of 2, so the valid values are as follows: 1, 2, 4, 8, and 16. The default is 8.
leastconns	Selects the real server with the fewest number of active connections based on the server weight. Use this predictor for processing light user requests (for example, browsing simple static web pages). For information about setting real server weight, see the (config-sfarm-redirect-rs) weight section.
slowstart *seconds*	(Optional) Specifies that the connections to the real server be in a slow-start mode for the duration indicated by the *seconds* value. Use the slow-start mechanism to avoid sending a high rate of new connections to servers that you have recently put into service. Enter an integer from 1 to 65535, where 1 is the slowest ramp-up value. By default, **slowstart** is disabled.

response	Selects the server with the lowest response time for the requested response-time measurement. If you do not specify a response-time measurement method, the ACE uses the HTTP app-req-to-response method.
app-req-to-resp	(Default) Measures the response time from when the ACE sends an HTTP request to a server to the time that the ACE receives a response from the server for that request.
syn-to-close	Measures the response time from when the ACE sends a TCP SYN to a server to the time that the ACE receives a CLOSE from the server.
syn-to-synack	Measures the response time from when the ACE sends a TCP SYN to a server to the time that the ACE receives the SYN-ACK from the server.
samples *number7*	(Optional) Specifies the number of samples that you want to average from the results of the response time measurement. Enter an integer from 1 to 16 in powers of 2. Valid values are 1, 2, 4, 8, and 16. The default is 8.
threshold *milliseconds*	(Optional) Specifies the required minimum average response time for a server. If the server response time is greater than the specified threshold value, the ACE removes the server from the load-balancing decision process (takes the server out of service). Enter an integer from 1 to 300000 milliseconds (5 minutes). The default is no threshold (servers are not taken out of service).
resume-timer *seconds*	(Optional) Specifies the number of seconds after which the ACE sends traffic again to a server that was taken out of the load-balancing decision process. The ACE monitors the server's response time. If that response time is less than or equal to the value set with the **threshold** keyword, the ACE places the server back in service. Enter an integer from 30 to 3600 seconds (1 hour). The default value is 300 seconds (5 minutes) if you configure a threshold without specifying the resume timer.
roundrobin	(Default) Selects the next server in the list of real servers based on server weight (weighted round-robin). For information about setting the real server weight, see the (config-sfarm-redirect-rs) weight section.

Command Modes

Server-farm redirect configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised (**reassign** keyword added).

Usage Guidelines

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

The weight assigned to the real servers is used only in the **roundrobin** and **leastconns** predictor methods. The **hash** and the **response** predictor methods do not recognize the weight for the real servers. For information about setting the real server weight, see the (config-sfarm-redirect-rs) weight section.

If you configure the **leastconns** predictor, you can use a **slowstart** mechanism (ramp-up) to avoid sending a high rate of new connections to the servers that have just been put in service. The real server with the fewest number of active connections will get the next connection request for the server farm with the **leastconns** predictor. The ramp-up stops when the duration timer that you specify expires.

The only time that the sequence of servers starts over at the beginning (with the first server) is when there is a configuration or server state change (for example, a probe failure).

Examples

To configure the ACE to select the real server with the lowest number of connections in the server farm, enter:

```
host1/Admin(config-sfarm-redirect)# predictor leastconns slowstart 300
```

To reset the load-balancing algorithm to the default round-robin algorithm, enter:

```
host1/Admin(config-sfarm-redirect)# no predictor
```

Related Commands

(config-sfarm-redirect-rs) weight

(config-sfarm-redirect) rserver

To associate one or more existing redirect real servers with a server farm and access serverfarm redirect real server configuration mode, use the **rserver** command. The CLI prompt changes to (config-sfarm-redirect-rs). For information on commands in serverfarm redirect real server configuration mode, see the "Server Farm Redirect Real Server Configuration Mode Commands" section. Use the **no** form of this command to dissociate the real server from the server farm.

rserver *name* [*port*]

no rserver *name* [*port*]

Syntax Description

name	Unique identifier of the real server. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
port	(Optional) Port number used for the real server Port Address Translation (PAT). Enter an integer from 1 to 65535.

Command Modes

Serverfarm redirect configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines The real server must already exist. To create a real server, see the **(config) rserver** command. You can associate a maximum of 16,384 real servers with a server farm.

Examples To associate a real server with a server farm, enter:

```
host1/Admin(config-sfarm-redirect)# rserver server1 4000
host1/Admin(config-sfarm-redirect-rs)#
```

To dissociate a real server from a server farm, enter:

```
host1/Admin(config-sfarm-redirect)# no rserver server1
host1/Admin(config-sfarm-redirect)#
```

Related Commands **(config) rserver**

Serverfarm Redirect Predictor Configuration Mode Commands

Serverfarm redirect predictor configuration mode commands allow you to configure additional parameters for some of the server farm predictor methods.

To configure these additional predictor parameters, use the **predictor least-loaded** or the **predictor response** command in serverfarm host configuration mode. The CLI prompt changes to (config-sfarm-host-predictor). For information about the commands in this mode, see the following commands. Use the **no** form of this command to remove the predictor from the server farm.

predictor {**least-loaded probe** *name*} | {**response** {**app-req-to-resp** | **syn-to-close** | **syn-to-synack**}[**samples** *number*]}}

no predictor

Syntax Description

least-loaded	Selects the server with the lowest load based on information obtained from SNMP probes. To use this predictor, you must associate an SNMP probe with the server farm. The ACE queries one user-specified OID (for example, CPU utilization or memory utilization). The ACE uses the retrieved value directly to determine the server with the lowest load.
probe *name*	Specifies the name of the SNMP probe that you want to query. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
response	Selects the server with the lowest response time for the requested response-time measurement. If you do not specify a response-time measurement method, the ACE uses the HTTP app-req-to-response method.
app-req-to-resp	(Default) Measures the response time from when the ACE sends an HTTP request to a server to the time that the ACE receives a response from the server for that request.
syn-to-close	Measures the response time from when the ACE sends a TCP SYN to a server to the time that the ACE receives a CLOSE from the server.

syn-to-synack	Measures the response time from when the ACE sends a TCP SYN to a server to the time that the ACE receives the SYN-ACK from the server.
samples *number*	(Optional) Number of samples over which you want to average the results of the response time measurement. Enter an integer from 1 to 16 in powers of 2. Valid values are: 1, 2, 4, 8, and 16. The default is 8.

Command Modes

Serverfarm redirect configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The commands in this mode require the server-farm feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To specify the least-loaded predictor method with a probe called SNMP_PROBE for the server farm, enter:

```
host1/Admin(config-sfarm-redirect)# predictor least-loaded probe SNNMP_PROBE
host1/Admin(config-sfarm-redirect-predictor)#
```

To remove the least-loaded predictor from the server farm, enter:

```
host1/Admin(config-sfarm-redirect)# no predictor
```

To specify the response predictor method that measures the response time from when the ACE sends an HTTP request to a server to the time that the ACE receives a response from the server for that request, enter:

```
host1/Admin(config-sfarm-redirect)# predictor response app-req-to-resp
host1/Admin(config-sfarm-redirect-predictor)#
```

To remove the response predictor from the server farm, enter:

```
host1/Admin(config-sfarm-redirect)# no predictor
```

Related Commands

show serverfarm detail
(config-sfarm-redirect) predictor
(config-sfarm-redirect-predictor) autoadjust
(config-sfarm-redirect-predictor) weight connection

(config-sfarm-redirect-predictor) autoadjust

After you specify the **predictor least-loaded** command, use the **autoadjust** command to apply the average load of the server farm to a real server whose load reaches zero. Use the **no** form of this command to return the ACE behavior to the default of assigning a maximum load value of 16000 to a server whose load has reached zero to prevent it from being flooded with new incoming connections.

autoadjust {**average** | **off**}

no autoadjust

Syntax Description

average	Instructs the ACE to apply the average load of the server farm to a real server whose load reaches zero. The average load is the running average of the load values across all real servers in the server farm.
off	Overrides the default behavior of the ACE of setting the load value for a server with a load of zero to 16000. When you configure this command, the ACE sends all new connections to the server that has a load of zero until the next load update arrives from the SNMP probe for this server.

Command Modes

Serverfarm redirect predictor configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

Whenever a server's load reaches zero, by default, the ACE uses the autoadjust feature to assign a maximum load value of 16000 to that server to prevent it from being flooded with new incoming connections. The ACE periodically adjusts this load value based on feedback from the server's SNMP probe and other configured options.

Using the least-loaded predictor with the configured server weight and the current connection count option enabled, the ACE calculates the final load of a real server as follows:

final load = *weighted load* × *static weight* × *current connection count*

where:

- *weighted load* is the load reported by the SNMP probe
- *static weight* is the configured weight of the real server
- *current connection count* is the total number of active connections to the real server

The ACE recalculates the final load whenever the connection count changes, provided that the **(config-sfarm-redirect-predictor) weight connection** command is configured. If the **(config-sfarm-redirect-predictor) weight connection** command is not configured, the ACE updates the final load when the next load update arrives from the SNMP probe.

If two servers have the same lowest load (either zero or nonzero), the ACE load balances the connections between the two servers in a round-robin manner.

Examples

To instruct the ACE to apply the average load of the server farm to a real server whose load reaches zero, enter:

```
host1/Admin(config-sfarm-redirect-predictor)# autoadjust average
```

To turn off the autoadjust feature for all servers in a server farm so that servers with a load of zero receive all new connections, enter:

```
host1/Admin(config-sfarm-redirect-predictor)# autoadjust off
```

To reset the behavior of the ACE to the default of applying the maximum load value of 16000 to a real server whose load is zero, enter:

```
host1/Admin(config-sfarm-redirect-predictor)# no autoadjust average
host1/Admin(config-sfarm-redirect-predictor)# no autoadjust off
```

Related Commands

show serverfarm detail
(config-sfarm-redirect) predictor
(config-sfarm-redirect-predictor) weight connection

(config-sfarm-redirect-predictor) weight connection

After you specify the **predictor least-loaded** or the **predictor response** command, use the **weight connection** command to instruct the ACE to use the current connection count in the final load calculation for each real server in the server farm. Use the **no** form of this command to reset the behavior of the ACE to the default of excluding the current connection count from the load calculation.

weight connection

no weight connection

Syntax Description

This command has no keywords or arguments.

Command Modes

Serverfarm redirect predictor configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

To see how the **weight connection** command affects the **(config-sfarm-redirect-predictor) autoadjust** command for the least-loaded predictor, see the Usage Guidelines section of the **(config-sfarm-redirect-predictor) autoadjust** command.

Examples

To instruct the ACE to use the current connection count in the final load calculation for each real server in the server farm, enter:

```
host1/Admin(config-sfarm-redirect-predictor)# weight connection
```

To reset the behavior of the ACE to the default of excluding the current connection count from the load calculation, enter:

```
host1/Admin(config-sfarm-redirect-predictor)# no weight connection
```

Related Commands

show serverfarm detail
(config-sfarm-redirect) predictor
(config-sfarm-redirect-predictor) autoadjust

Server Farm Redirect Real Server Configuration Mode Commands

Serverfarm redirect real server configuration mode commands allow you to associate a redirect real server with a redirect server farm and configure the real server attributes.

To associate one or more existing redirect real servers with a redirect server farm and access serverfarm redirect real server configuration mode, use the **rserver** command in serverfarm redirect configuration mode. The CLI prompt changes to (config-sfarm-redirect-rs). For information about the commands in this mode, see the following commands. Use the **no** form of this command to remove the real server from the server farm.

rserver *name*

no rserver *name*

Syntax Description

name	Unique identifier of the real server. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Serverfarm redirect configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the server-farm feature in your user role unless otherwise specified. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

The redirect real server must already exist. To create a real server, see the **(config) rserver redirect** command. You can associate a maximum of 16,384 real servers with a server farm.

Examples

To associate a real server with a server farm, enter:

```
host1/Admin(config-sfarm-redirect)# rserver server1
```

To dissociate a real server from a server farm, enter:

```
host1/Admin(config-sfarm-redirect)# no rserver server1
```

Related Commands

This command has no related commands.

(config-sfarm-redirect-rs) backup-rserver

To configure a backup real server for a real server in a server farm, use the **backup-rserver** command. If a real server associated with a server farm becomes unavailable, the ACE directs flows to the configured backup real server. Use the **no** form of this command to remove a backup real server from the configuration.

backup-rserver *name*

no backup-rserver

Syntax Description

name	Unique identifier of an existing real server that you want to configure as a backup server in a server farm. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Serverfarm redirect real server configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The real server used as a backup server must already exist. To create a redirect real server, see the **(config) rserver redirect** command.

Examples

To associate a backup real server with a server farm, enter:

```
host1/Admin(config-sfarm-redirect-rs)# backup-rserver BACKUP_SERVER1
```

To dissociate a backup real server from a server farm, enter:

```
host1/Admin(config-sfarm-redirect-rs)# no backup-rserver
```

Related Commands

(config) rserver

(config-sfarm-redirect-rs) conn-limit

To configure the maximum and minimum number of connections that you want to allow for a redirect real server in a server farm, use the **conn-limit** command. Use the **no** form of this command to reset the real server maximum connections and minimum connections threshold to the default of4000000.

conn-limit max *maxconns* **min** *minconns*

no conn-limit

Syntax Description

max *maxconns*	Specifies the maximum number of connections allowed for this real server. Enter an integer from 2 to 4000000. The default is4000000.
min *minconns*	Specifies the connection threshold below which the real server will start accepting connections again after the number of connections exceeds the configured maximum number of connections. Enter an integer from 2 to4000000. The default is *minconns* equal to *maxconns*.

Command Modes

Serverfarm redirect real server configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Use this command to specify the maximum number of connections and the minimum connection threshold for a redirect real server in a server farm. The *minconns* value must be less than or equal to the *maxconns* value. The ACE uses the *minconns* value as a threshold to start accepting connections again after the *maxconns* limit is exceeded.

Examples

To configure the maximum number of connections and the minimum connection threshold for a redirect real server, enter:

```
host1/Admin(config-sfarm-redirect-rs)# conn-limit max 65535 min 40000
```

To reset the maximum number of connections and the minimum connection threshold for a redirect real server to the default of4000000, enter:

```
host1/Admin(config-sfarm-redirect-rs)# no conn-limit
```

Related Commands

(config-sfarm-redirect-rs) rate-limit

(config-sfarm-redirect-rs) inservice

To place a real server associated with a server farm in service, use the **inservice** command. Use the **no** form of this command to take a real server out of service.

inservice [**standby**]

no inservice

Syntax Description

standby	(Optional) Used with backup real servers, specifies that a backup real server remain inactive unless the primary real server fails. If the primary fails, the backup server becomes active and starts accepting connections.

Command Modes

Serverfarm redirect real server configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command requires the real-inservice feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

To start load-balancing connections to a real server in a server farm, you must place the real server in service by using the **inservice** command.

You can modify the attributes of a real server in a server farm without taking the server out of service.

In addition to putting a backup real server in service standby, another use of the **inservice standby** command is to provide the graceful shutdown of primary real servers. Use this command to gracefully shut down servers with sticky connections. When you enter this command for a primary real server, the ACE does the following:

- Tears down existing non-TCP connections to the server
- Allows current TCP connections to complete
- Allows new sticky connections for existing server connections that match entries in the sticky database
- Load balances all new connections (other than the matching sticky connections mentioned above) to the other servers in the server farm
- Eventually takes the server out of service

Examples

To place a real server in service, enter:

```
host1/Admin(config-sfarm-redirect-rs)# inservice
```

To perform a graceful shutdown on a primary real server with sticky connections in a server farm, enter:

```
host1/Admin(config-sfarm-host-rs)# inservice standby
```

To take a real server out of service, enter:

```
host1/Admin(config-sfarm-redirect-rs)# no inservice
```

Related Commands This command has no related commands.

(config-sfarm-redirect-rs) rate-limit

To configure a limit for the connection rate and the bandwidth rate of a real server in a redirect server farm, use the **rate-limit** command. The connection rate is the number of connections per second received by the ACE and destined to a particular redirect real server. The bandwidth rate is the number of bytes per second received by the ACE and destined for a particular redirect real server. Use the **no** form of this command to revert to the ACE default of not limiting the connection rate or bandwidth rate of real servers in a server farm.

rate-limit {**connection** *number1* | **bandwidth** *number2*}

no rate-limit {**connection** | **bandwidth**}

Syntax Description

connection *number1*	Specifies the real server connection-rate limit in connections per second. Enter an integer from 2 to 350000. There is no default value.
bandwidth *number2*	Specifies the real server bandwidth-rate limit in bytes per second. Enter an integer from 2 to 300000000. There is no default value.

Command Modes Serverfarm redirect real server configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines If the connection rate or the bandwidth rate of incoming traffic destined for a particular real server exceeds the configured rate for the server, the ACE blocks any further traffic destined to that real server until the connection rate or bandwidth rate drops below the configured limit. Also, the ACE removes the blocked real server from future load-balancing decisions. By default, the ACE does not limit the connection rate or the bandwidth rate of real servers in a server farm.

Examples To limit the connection rate of a real server to 100,000 connections per second, enter:

```
host1/Admin(config-sfarm-redir-rs)# rate-limit connection 100000
```

To revert to the ACE default of not limiting the real-server connection rate, enter:

```
host1/Admin(config-sfarm-redir-rs)# no rate-limit connection
```

To limit the real-server bandwidth rate to 5,000,000 bytes per second, enter:

```
host1/Admin(config-sfarm-redir-rs)# rate-limit bandwidth 5000000
```

To revert to the ACE default of not limiting real-server bandwidth, enter:

```
host1/Admin(config-sfarm-redir-rs)# no rate-limit bandwidth
```

Related Commands (config-sfarm-redirect-rs) conn-limit

(config-sfarm-redirect-rs) weight

To configure the capacity of a real server in relation to other servers in a server farm, use the **weight** command. The weight value that you specify for a server is used in the weighted round-robin and least-connections predictor load-balancing methods. Use the **no** form of this command to reset the real server weight to the default.

weight *number*

no weight

Syntax Description

number	Weight value assigned to a real server in a server farm. This value is used in the weighted round-robin and least-connections predictor load-balancing algorithms. Enter an integer from 1 to 100. The default is 8.

Command Modes

Serverfarm redirect real server configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Servers with higher weight values receive a proportionally higher number of connections than servers with lower weight values.

To specify different weight values for a redirect real server in a server farm, you can assign multiple IP addresses to the server.

Examples

To configure a weight value for a real server, enter:

```
host1/Admin(config-sfarm-redirect-rs)# weight 50
```

To reset the weight of a real server to the default of 8, enter:

```
host1/Admin(config-sfarm-redirect-rs)# no weight
```

Related Commands (config-sfarm-redirect) predictor

SSL Proxy Configuration Mode Commands

SSL proxy configuration mode commands allow you to define the Secure Sockets Layer (SSL) parameters that the ACE SSL proxy service uses in either SSL termination (proxy server service) or SSL initiation (proxy client service) during the SSL handshake.

To create a new proxy service (or edit an existing proxy service) and access SSL proxy configuration mode, use the **ssl-proxy service** command in configuration mode. The CLI prompt changes to (config-ssl-proxy). Use the **no** form of this command to delete an existing SSL proxy service.

ssl-proxy service *pservice_name*

no ssl-proxy service *pservice_name*

Syntax Description

pservice_name	Name of the SSL proxy service. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the SSL feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

When you create a SSL proxy service, the CLI changes to the SSL proxy configuration mode, where you define the following SSL proxy service attributes:

- Client authentication group—See the **(config-ssl-proxy) authgroup** command.
- Certificate—See the **(config-ssl-proxy) cert** command.
- Client authentication using CRLs—See the **(config-ssl-proxy) crl** command
- Chain group—See the **(config-ssl-proxy) chaingroup** command.
- Key pair—See the **(config-ssl-proxy) key** command.
- Parameter map—See the **(config-ssl-proxy) ssl advanced-options** command.

Examples

To create the SSL proxy service PSERVICE_SERVER, enter:

```
host1/Admin(config)# ssl-proxy service PSERVICE_SERVER
host1/Admin(config-ssl-proxy)#
```

To delete an existing SSL proxy service, enter:

```
host1/Admin(config)# no ssl-proxy PSERVICE_SERVER
```

Related Commands

(config-ssl-proxy) authgroup
(config-ssl-proxy) cert
(config-ssl-proxy) chaingroup
(config-ssl-proxy) key
(config-ssl-proxy) ssl advanced-options

(config-ssl-proxy) authgroup

To specify the certificate authentication group that the ACE uses during the Secure Sockets Layer (SSL) handshake and enable client authentication on this SSL-proxy service, use the **authgroup** command. Use the **no** form of this command to delete a certificate authentication group from the SSL proxy service.

authgroup *group_name*

no authgroup *group_name*

Syntax Description

group_name	Name of an existing certificate authentication group.

Command Modes

SSL proxy configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

When you enable client authentication, a significant performance decrease may occur in the ACE appliance.

Examples

To specify the certificate authentication group AUTH-CERT1, enter:

```
host1/Admin(config-ssl-proxy)# authgroup AUTH-CERT1
```

To delete the certificate authentication group AUTH-CERT1 from the SSL proxy service, enter:

```
host1/Admin(config-ssl-proxy)# no authgroup AUTH-CERT1
```

Related Commands

(config) crypto chaingroup
(config-ssl-proxy) cert
(config-ssl-proxy) key
(config-ssl-proxy) ssl advanced-options

(config-ssl-proxy) cert

To specify the certificate that the ACE uses during the Secure Sockets Layer (SSL) handshake to prove its identity, use the **cert** command. Use the **no** form of this command to delete a certificate file from the SSL proxy service.

cert *cert_filename*

no cert *cert_filename*

Syntax Description

name	Name of an existing certificate file loaded on the ACE. Enter an unquoted text string with no spaces and a maximum of 40 alphanumeric characters. To display a list of available certificate files, use the **do show crypto files** command.

Command Modes

SSL proxy configuration mode

Command HistoryA

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The public key embedded in the certificate that you select must match the public key in the key pair file that you select. To verify that the public keys in the two files match, use the **crypto verify** command in the Exec mode.

Examples

To specify the certificate in the certificate file MYCERT.PEM, enter:

```
host1/Admin(config-ssl-proxy)# cert MYCERT.PEM
```

To delete the certificate in the certificate file MYCERT.PEM from the SSL proxy service, enter:

```
host1/Admin(config-ssl-proxy)# no cert MYCERT.PEM
```

Related Commands

crypto verify
(config) crypto chaingroup
(config-ssl-proxy) authgroup
(config-ssl-proxy) chaingroup
(config-ssl-proxy) key
(config-ssl-proxy) ssl advanced-options

(config-ssl-proxy) chaingroup

To specify the certificate chain group that the ACE sends to its peer during the Secure Sockets Layer (SSL) handshake, use the **chaingroup** command. Use the **no** form of this command to delete a certificate chain group from the SSL proxy service.

chaingroup *group_name*

no chaingroup *group_name*

Syntax Description

group_name	Name of an existing certificate chain group.

Command Modes

SSL proxy configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The ACE includes the certificate chain with the certificate that you specified for the SSL proxy service.

When a change occurs in a chain-group certificate, the change takes effect when you read the associated chain group through the **chaingroup** command.

Examples

To configure the ACE SSL proxy service to send the certificate chain group MYCHAINGROUP to its peer during the SSL handshake, enter:

```
host1/Admin(config-ssl-proxy)# chaingroup MYCHAINGROUP
```

To delete the certificate chain group MYCHAINGROUP from the SSL proxy service, enter:

```
host1/Admin(config-ssl-proxy)# no chaingroup MYCHAINGROUP
```

Related Commands

(config) crypto chaingroup
(config-ssl-proxy) authgroup
(config-ssl-proxy) cert
(config-ssl-proxy) key
(config-ssl-proxy) ssl advanced-options

(config-ssl-proxy) crl

To determine which certificate revocation lists (CRLs) to use for clientauthentication, use the **crl** command. Use the **no** form of this command to disable the use of CRL certificates during authentication.

crl *crl_name* | **best- effort**

no crl *crl_name* | **best-effort**

Syntax Description

crl_name	Name that you assigned to the CRL when you downloaded it using the configuration mode **crypto crl** command. See (config) crypto crl for more information.
best-effort	Specifies that the ACE scans each certificate to determine if it contains a CDP pointing to a CRL in the certificate extension and then retrieves the CRLs from that location, if the CDP is valid.

Command Modes

SSL proxy configuration mode

Command HistoryA

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

By default, the ACE does not use CRLs during client authentication. You can configure the SSL proxy service to use a CRL by either of the following methods:

- The ACE can scan each certificate for the service to determine if it contains a CRL Distribution Point (CDP) pointing to a CRL in the certificate extension and then retrieve the CRL from that location if the CDP is valid. If the CDP has an http:// based URL, it uses the URL to download the CRL to the ACE appliance.
- You can manually configure the download location for the CRL from which the ACE retrieves it.

By default, the ACE does not reject certificates when the CRL in use has passed its update date. To configure the ACE to reject certificates when the CRL is expired, use the **expired-crl reject** command in parameter map SSL configuration mode.

Examples

To enable the CRL1 CRL for authentication on an SSL proxy service, enter:

```
host1/Admin(config-ssl-proxy)# crl CRL1
```

To scan the client certificate for CRL information, enter:

```
host1/Admin(config-ssl-proxy)# crl best-effort
```

To disable the use of a downloaded CRL during authentication, enter:

```
host1/Admin(config-ssl-proxy)# no crl CRL1
```

To disable the use of CRL client certificates during authentication, enter:

```
host1/Admin(config-ssl-proxy)# no crl best-effort
```

Related Commands

crypto crlparams
(config) crypto crl
(config-parammap-ssl) expired-crl reject
(config-ssl-proxy) authgroup
(config-ssl-proxy) cert
(config-ssl-proxy) chaingroup
(config-ssl-proxy) key
(config-ssl-proxy) ssl advanced-options

(config-ssl-proxy) key

To specify the key pair that the ACE uses during the Secure Sockets Layer (SSL) handshake for data encryption, use the **key** command. Use the **no** form of this command to delete a private key from the SSL proxy service.

key *key_filename*

no key *key_filename*

Syntax Description

key_filename	Name of an existing key pair file loaded on the ACE. Enter an unquoted text string with no spaces and a maximum of 40 alphanumeric characters.

Command Modes

SSL proxy configuration mode

Command HistoryA

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The public key in the key pair file that you select must match the public key embedded in the certificate that you select. To verify that the public keys in the two files match, use the **crypto verify** command in the Exec mode.

Examples

To specify the private key in the key pair file MYKEY.PEM for the SSL proxy service, enter:

```
host1/Admin(config-ssl-proxy)# key MYKEY.PEM
```

To delete the private key in the key pair file MYKEY.PEM from the SSL proxy service, enter:

```
host1/Admin(config-ssl-proxy)# no key MYKEY.PEM
```

Related Commands

crypto verify
(config-ssl-proxy) authgroup
(config-ssl-proxy) cert
(config-ssl-proxy) chaingroup
(config-ssl-proxy) ssl advanced-options

(config-ssl-proxy) ssl advanced-options

To associate a context Secure Sockets Layer (SSL) parameter map with the SSL proxy server service, use the **ssl advanced-options** command. Use the **no** form of this command to remove the association of an SSL parameter map with the SSL proxy service.

ssl advanced-options *parammap_name*

no ssl advanced-options *parammap_name*

Syntax Description

parammap_name	Name of an existing SSL parameter map.

Command Modes

SSL proxy configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To associate the parameter map PARAMMAP_SSL with the SSL proxy service, enter:

```
host1/Admin(config-ssl-proxy)# ssl advanced-options PARAMMAP_SSL
```

To remove the association of an SSL parameter map PARAMMAP_SSL with the SSL proxy service, enter:

```
host1/Admin(config-ssl-proxy)# no ssl advanced-options PARAMMAP_SSL
```

Related Commands

(config) parameter-map type
(config-ssl-proxy) authgroup
(config-ssl-proxy) cert
(config-ssl-proxy) chaingroup
(config-ssl-proxy) key

Sticky HTTP Cookie Configuration Mode Commands

Sticky cookie configuration mode commands allow you to configure the ACE to learn a cookie from either the HTTP header of a client request or the Set-Cookie message sent by the server to a client. The ACE then uses the learned cookie to provide stickiness between a client and a server for the duration of a transaction. To configure the ACE to use HTTP cookies for stickiness, use the **sticky http-cookie** command in configuration mode. This command creates a sticky cookie group and allows you to access sticky cookie configuration mode. The prompt changes to (config-sticky-cookie). To remove the sticky cookie group from the configuration, use the **no** form of this command.

sticky http-cookie *name1 name2*

no sticky http-cookie *name1 name2*

Syntax Description

name1	Cookie value from the HTTP header of the client request or from the Set-Cookie message from the server. Enter a unique identifier for the cookie with a maximum of 64 alphanumeric characters.
name2	Unique identifier of the sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the sticky feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can create a maximum of 4096 sticky groups in the ACE.

By default, the maximum number of bytes that the ACE parses to check for a cookie, HTTP header, or URL is 2048. If a cookie, HTTP header, or URL exceeds the default value, the ACE drops the packet and sends a RST (reset) to the client browser. You can increase the number of bytes that the ACE parses using the **(config-parammap-http) set header-maxparse-length** command in HTTP parameter-map configuration mode.

You can also change the default behavior of the ACE when a cookie, header, or URL exceeds the maximum parse length using the **(config-parammap-http) length-exceed** command in HTTP parameter-map configuration mode.

Examples

To create a sticky group for cookie stickiness, enter:

```
host1/Admin(config)# sticky http-cookie cisco.com GROUP3
host1/Admin(config-sticky-cookie)#
```

To remove the sticky group from the configuration, enter:

```
host1/Admin(config)# no sticky http-cookie cisco.com GROUP3
```

Related Commands

show running-config
show sticky database
(config) sticky http-header
(config) sticky ip-netmask

(config-sticky-cookie) cookie insert

To enable cookie insertion, use the **cookie insert** command. Use cookie insertion when you want to use a session cookie for persistence if the server is not currently setting the appropriate cookie. Use the **no** form of this command to disable cookie insertion.

cookie insert [**browser-expire**]

no cookie insert [**browser-expire**]

Syntax Description

browser-expire	(Optional) Allows the client's browser to expire a cookie when the session ends.

Command Modes

Sticky cookie configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

With cookie insertion enabled, the ACE inserts the cookie in the Set-Cookie header of the response from the server to the client. The ACE selects a cookie value that identifies the original server from which the client received a response. For subsequent connections of the same transaction, the client uses the cookie to stick to the same server.

With either TCP server reuse or persistence rebalance enabled, the ACE inserts a cookie in every client request. See the **(config-parammap-http) server-conn reuse** or **(config-parammap-http) persistence-rebalance** commands.

Examples

To enable cookie insertion, enter:

```
host1/Admin(config-sticky-cookie)# cookie insert
```

To disable cookie insertion, enter:

```
host1/Admin(config-sticky-cookie)# no cookie insert
```

Related Commands (config) sticky http-cookie

(config-sticky-cookie) cookie

To configure the cookie offset and length, use the **cookie** command. Use the **no** form of this command to remove the cookie offset and length from the configuration.

cookie offset *number1* [**length** *number2*]

no cookie offset *number1* [**length** *number2*]

Syntax Description

offset *number1*	Specifies the portion of the cookie that the ACE uses to stick the client on a particular server by indicating the bytes to ignore starting with the first byte of the cookie. Enter an integer from 0 to 999. The default is 0, which indicates that the ACE does not exclude any portion of the cookie.
length *number2*	(Optional) Specifies the length of the portion of the cookie (starting with the byte after the offset value) that the ACE uses for sticking the client to the server. Enter an integer from 1 to 1000. The default is 1000.

Command Modes

Sticky cookie configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

An HTTP cookie value may change over time with only a portion remaining constant throughout a transaction between the client and a server. You can configure the ACE to use the constant portion of a cookie to make persistent connections to a specific server. The ACE stores cookie offset and length values in the sticky table.

The offset and length can vary from 0 to 1000 bytes. If the content string is longer than the offset but shorter than the offset plus the length of the string, the ACE sticks the connection based on that portion of the content starting with the byte after the offset value and ending with the byte specified by the offset plus the length. The total of the offset and the length cannot exceed 1000.

Examples

To configure the cookie offset and length, enter:

```
host1/Admin(config-sticky-cookie)# cookie offset 300 length 900
```

To remove the cookie offset and length from the configuration, enter:

```
host1/Admin(config-sticky-cookie)# no cookie offset 300 length 900
```

Related Commands **(config) sticky http-cookie**

(config-sticky-cookie) cookie secondary

To configure a secondary cookie, use the **cookie secondary** command. Use the **no** form of this command to remove a secondary cookie from the configuration.

cookie secondary *name*

no cookie secondary

Syntax Description

name	Name of the secondary cookie. Enter a cookie name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Sticky cookie configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You can configure an alternative cookie name that appears in the URL string of the web page on the server. The ACE uses this cookie to maintain a sticky connection between a client and a server and adds a secondary entry in the sticky table.

Examples

To configure a secondary cookie, enter:

```
host1/Admin(config-sticky-cookie)# cookie secondary mysite.com
```

To remove a secondary cookie from the configuration, enter:

```
host1/Admin(config-sticky-cookie)# no cookie secondary
```

Related Commands **(config) sticky http-cookie**

(config-sticky-cookie) replicate sticky

To instruct the ACE to replicate HTTP cookie sticky table entries on the standby ACE, use the **replicate sticky** command. Use the **no** form of this command to restore the ACE to its default of not replicating HTTP cookie sticky table entries.

replicate sticky

no replicate sticky

Command Modes

Sticky cookie configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

If you are using redundancy, you can configure the ACE to replicate HTTP cookie sticky table entries on the standby ACE so if a switchover occurs, the new active ACE can maintain existing sticky connections.

The timer of a sticky table entry on the standby ACE is reset every time the entry is synchronized with the active ACE entry. Thus, the standby sticky entry may have a lifetime up to twice as long as the active entry. However, if the entry expires on the active ACE or a new real server is selected and a new entry is created, the old entry on the standby ACE is replaced.

Examples

To instruct the ACE to replicate HTTP cookie sticky table entries on the standby ACE, enter:

```
host1/Admin(config-sticky-cookie)# replicate sticky
```

To restore the ACE to its default of not replicating HTTP cookie sticky table entries, enter:

```
host1/Admin(config-sticky-cookie)# no replicate sticky
```

Related Commands

(config) sticky http-cookie

(config-sticky-cookie) serverfarm

To complete a sticky group configuration, you must configure a server farm entry for the group. To configure a server farm entry for a sticky group, use the **serverfarm** command. Use the **no** form of this command to dissociate a server farm from a sticky group.

serverfarm *name1* [**backup** *name2* [**sticky**] [**aggregate-state**]]

no serverfarm

Syntax Description

name1	Identifier of an existing server farm that you want to associate with the sticky group. You can associate one server farm with each sticky group. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
backup *name2*	(Optional) Specifies the identifier of an existing server farm that you want the ACE to use as a backup server farm. If the primary server farm is unavailable, the ACE uses the configured backup server farm. The backup server farm becomes sticky when you enter the **sticky** keyword. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
sticky	(Optional) Specifies that the backup server farm is sticky.
aggregate-state	(Optional) Specifies that the state of the primary server farm is tied to the state of all the real servers in that server farm and in the backup server farm if configured. The ACE declares the primary server farm down if all real servers in the primary server farm and all real servers in the backup server farm are down.

Command Modes

Sticky cookie configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

If all the servers in the primary server farm fail, the ACE sends all connections to the backup server farm. When the primary server farm comes back up (at least one server becomes active):

- If the **sticky** option is enabled, then:
  - All new sticky connections that match existing sticky table entries for the real servers in the backup server farm are stuck to the same real servers in the backup server farm.
  - All new non-sticky connections and those sticky connections that do not have an entry in the sticky table are load balanced to the real servers in the primary server farm.
- If the **sticky** option is not enabled, then the ACE load balances all new connections to the real servers in the primary server farm.
- Existing non-sticky connections to the servers in the backup server farm are allowed to complete in the backup server farm.

You can fine-tune the conditions under which the primary server farm fails over and returns to service by configuring a partial server farm failover. For details about partial server farm failover, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To associate a server farm with a sticky group and specify a sticky backup server farm, enter:

```
host1/Admin(config-sticky-cookie)# serverfarm SFARM1 backup BKUP_SFARM2 sticky
aggregate-state
```

To dissociate a server farm from a sticky group, enter:

```
host1/Admin(config-sticky-cookie)# no serverfarm
```

Related Commands

(config) sticky http-cookie

(config-sticky-cookie) static cookie-value

To configure a static cookie, use the **static cookie-value** command. Use the **no** form of this command to remove a static cookie from the configuration.

static cookie-value *value* **rserver** *name* [*number*]

no static cookie-value *value* **rserver** *name* [*number*]

Syntax Description

value	Cookie string value. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters. Alternatively, you can enter a text string with spaces provided that you enclose the string in quotation marks (“).
rserver *name*	Specifies the hostname of an existing real server. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
number	(Optional) Port number of the real server. Enter an integer from 1 to 65535.

Command Modes

Sticky cookie configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You can configure the ACE to use static cookies from entries based on cookie values and, optionally, real server names and ports. Static cookie values remain constant over time.

You can configure multiple static cookie entries, but only one unique real-server name can exist for a given static cookie value. When you configure a static entry, the ACE enters it into the sticky table immediately. You can create a maximum of 4096 static sticky entries in the ACE.

Examples

To configure a static cookie, enter:

```
host1/Admin(config-sticky-cookie)# static cookie-value CORVETTE rserver SERVER1 4000
```

To remove a static cookie form the configuration, enter:

```
host1/Admin(config-sticky-cookie)# no static cookie-value CORVETTE rserver SERVER1 4000
```

Related Commands **(config) sticky http-cookie**

(config-sticky-cookie) timeout

To configure an HTTP cookie sticky timeout, use the **timeout** *minutes* command. Use the **no** form of this command to reset the sticky timeout to the default of 1440 minutes.

timeout {*minutes* | **activeconns**}

no timeout {*minutes* | **activeconns**}

Syntax Description

minutes	Length of time in minutes that the ACE appliance remembers the last real server to which a client made a sticky connection. Enter an integer from 0 to 65535. The default timeout value is 1440 minutes (24 hours).
activeconns	Specifies that a sticky entry is timed out when the timer expires even if there are active connections associated with the sticky entry.

Command Modes

Sticky cookie configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The sticky timeout specifies the period of time that the ACE keeps the HTTP cookie sticky information for a client connection in the sticky table after the latest client connection terminates. The ACE resets the sticky timer for a specific sticky-table entry each time that the appliance opens a new connection matching that entry.

By default, the ACE times out a sticky table entry when the timeout for that entry expires and no active connections matching that entry exist. To specify that the ACE time out HTTP cookie sticky table entries even if active connections exist after the sticky timer expires, use the **timeout activeconns** command.

Examples

To set the duration for sticky connections between a client and a real server to 720 minutes, enter:

```
host1/Admin(config-sticky-cookie)# timeout 720
```

To configure the ACE to time out HTTP cookie sticky entries even if active connections exist for those entries, enter:

```
host1/Admin(config-sticky-cookie)# timeout activeconns
```

To restore the ACE to its default of not timing out HTTP cookie sticky entries if active connections exist for those entries, enter:

```
host1/Admin(config-sticky-cookie)# no timeout activeconns
```

Related Commands **(config) sticky http-cookie**

Sticky HTTP Content Configuration Mode Commands

Sticky HTTP content configuration mode commands allow you to configure the ACE to stick client connections to the same real server based on a string in the data portion of the HTTP packet. To create an HTTP content sticky group and access sticky HTTP content configuration mode, use the **sticky http-content** command. The prompt changes to (config-sticky-content). Use the **no** form of this command to remove the sticky group from the configuration.

sticky http-content *name*

no sticky http-content *name*

Syntax Description

name	Unique identifier of the sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The commands in this mode require the sticky feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can create a maximum of 4096 sticky groups on the ACE.

Examples

To create a sticky group for HTTP packet content stickiness, enter:

```
host1/Admin(config)# sticky http-content HTTP_CONTENT_GROUP
host1/Admin(config-sticky-content)#
```

To remove the sticky group from the configuration, enter:

```
host1/Admin(config)# no sticky http-content HTTP_CONTENT_GROUP
```

Related Commands

show running-config
show sticky database

(config-sticky-content) content

To define the portion of the HTTP packet contents that you want the ACE to match, use the **content** command. Using this command, you can specify offset and length values and a beginning and ending pattern based on a regular expression. The ACE stores these values in the sticky table and uses them to stick a client to a particular server. Use the **no** form of this command to remove the HTTP content specification from the sticky table.

content [**offset** *number1*] [**length** *number2*] [**begin-pattern** *expression1*] [**end-pattern** *expression2*]

no content [**offset** *number1*] [**length** *number2*] [**begin-pattern** *expression1*] [**end-pattern** *expression2*]

Syntax Description

offset *number1*	(Optional) Specifies the portion of the content that the ACE uses to stick the client on a particular server by indicating the bytes to ignore starting with the first byte of the content. Enter an integer from 0 to 999. The default is 0, which indicates that the ACE does not exclude any portion of the content.
length *number2*	(Optional) Specifies the length of the portion of the content (starting with the byte after the offset value) that the ACE uses for sticking the client to the server. Enter an integer from 1 to 1000. The default is the entire content. The offset and length can vary from 0 to 1000 bytes. If the content string is longer than the offset but shorter than the offset plus the length of the string, the ACE sticks the connection based on that portion of the content starting with the byte after the offset value and ending with the byte specified by the offset plus the length. The total of the offset and the length cannot exceed 1000. You cannot specify both the **length** and the **end-pattern** options in the same **content** command.

begin-pattern *expression1*	(Optional) Specifies the beginning pattern of the HTTP packet content payload and the pattern string to match before hashing. If you do not specify a beginning pattern, the ACE starts parsing immediately following the offset byte. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters for each pattern that you configure. You can enter a text string with spaces if you enclose the entire string in quotation marks (“). The ACE supports the use of regular expressions for matching string expressions. When matching data strings, the period (.) and question mark (?) characters do not have a literal meaning in regular expressions. Use brackets ([]) to match these symbols (for example, enter www[.]xyz[.]com instead of www.xyz.com). You can also use a backslash (\) to escape a dot (.) or a question mark (?).
end-pattern *expression2*	(Optional) Specifies the pattern that marks the end of hashing. If you do not specify either a length or an ending pattern, the ACE continues to parse the data until it reaches the end of the field or the end of the packet, or until it reaches the maximum body parse length. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters for each pattern that you configure. You can enter a text string with spaces if you enclose the entire string in quotation marks (“). The ACE supports the use of regular expressions for matching string expressions. You cannot specify both the **length** and the **end-pattern** options in the same **content** command.

Command Modes

Sticky HTTP content configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The contents of an HTTP packet may change over time with only a portion remaining constant throughout a transaction between the client and a server. You can configure the ACE to use the constant portion of the HTTP packet content to make persistent connections to a specific server. To define the portion of the packet content that you want the ACE to use, you specify offset and length values and a beginning and ending pattern. The ACE stores these values in the sticky table.

Examples

To create an HTTP packet content specification that the ACE will use to stick traffic to a server, enter:

```
host1/Admin(config-sticky-content)# content offset 250 length 750 begin-pattern abc123.*
```

To remove the HTTP packet content specification from the configuration, enter:

```
host1/Admin(config-sticky-content)# no content
```

Related Commands (config) sticky http-content

(config-sticky-content) replicate sticky

To instruct the ACE to replicate HTTP content sticky table entries on the standby ACE, use the **replicate sticky** command. Use the **no** form of this command to restore the ACE to its default of not replicating HTTP content sticky table entries.

replicate sticky

no replicate sticky

Syntax Description This command has no keywords or arguments.

Command Modes Sticky HTTP content configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines If you are using redundancy, you can configure the ACE to replicate HTTP content sticky table entries on the standby ACE so if a switchover occurs, the new active ACE can maintain existing sticky connections.

The timer of a sticky table entry on the standby ACE is reset every time the entry is synchronized with the active ACE entry. Thus, the standby sticky entry may have a lifetime up to twice as long as the active entry. However, if the entry expires on the active ACE or a new real server is selected and a new entry is created, the old entry on the standby ACE is replaced.

Examples To instruct the ACE to replicate HTTP content sticky table entries on the standby ACE, enter:

```
host1/Admin(config-sticky-content)# replicate sticky
```

To restore the ACE default of not replicating HTTP content sticky table entries, enter:

```
host1/Admin(config-sticky-content)# no replicate sticky
```

Related Commands (config) sticky http-content

(config-sticky-content) serverfarm

To complete a sticky group configuration, you must configure a server farm entry for the group. To configure a server farm entry for a sticky group, use the **serverfarm** command. Use the **no** form of this command to dissociate a server farm from a sticky group.

serverfarm *name1* [**backup** *name2* [**sticky**] [**aggregate-state**]]

no serverfarm

Syntax Description

name1	Identifier of an existing server farm that you want to associate with the sticky group. You can associate one server farm with each sticky group. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
backup *name2*	(Optional) Specifies the identifier of an existing server farm that you want the ACE to use as a backup server farm. If the primary server farm is unavailable, the ACE uses the configured backup server farm. The backup server farm becomes sticky when you enter the **sticky** keyword. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
sticky	(Optional) Specifies that the backup server farm is sticky.
aggregate-state	(Optional) Specifies that the state of the primary server farm is tied to the state of all the real servers in that server farm and in the backup server farm, if configured. The ACE declares the primary server farm down if all real servers in the primary server farm and all real servers in the backup server farm are down.

Command Modes

Sticky HTTP content configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

If all the servers in the primary server farm fail, the ACE sends all connections to the backup server farm. When the primary server farm comes back up (at least one server becomes active):

- If the **sticky** option is enabled, then:
  - All new sticky connections that match existing sticky table entries for the real servers in the backup server farm are stuck to the same real servers in the backup server farm.
  - All new non-sticky connections and those sticky connections that do not have an entry in the sticky table are load balanced to the real servers in the primary server farm.

- If the **sticky** option is not enabled, then the ACE load balances all new connections to the real servers in the primary server farm.
- Existing non-sticky connections to the servers in the backup server farm are allowed to complete in the backup server farm.

You can fine-tune the conditions under which the primary server farm fails over and returns to service by configuring a partial server farm failover. For details about partial server farm failover, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To associate a server farm with an HTTP content sticky group and specify a sticky backup server farm, enter:

```
host1/Admin(config-sticky-content)# serverfarm SFARM1 backup BKUP_SFARM2 sticky
aggregate-state
```

To dissociate a server farm from an HTTP content sticky group, enter:

```
host1/Admin(config-sticky-content)# no serverfarm
```

Related Commands

(config) sticky http-content

(config-sticky-content) static content

To configure a static HTTP content sticky table entry, use the **static content** command. Use the **no** form of this command to remove the static entry from the sticky table.

static content *value* **rserver** *name* [*number*]

no static content *value* **rserver** *name* [*number*]

Syntax Description

value	Content string value. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters. You can enter a text string with spaces provided that you enclose the entire string in quotation marks (“).
rserver *name*	Specifies that the static entry is based on the real server name. Enter the name of an existing real server as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
number	(Optional) Port number of the real server. Enter an integer from 1 to 65535.

Command Modes

Sticky HTTP content configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

You can configure the ACE to use static sticky table entries based on the HTTP content and optionally, the real server name and port. Static sticky HTTP content entries remain constant over time. You can configure multiple static content entries, but only one unique real-server name can exist for a given static content string. When you configure a static entry, the ACE enters it into the sticky table immediately. You can configure a maximum of 4096 static sticky entries in the ACE.

Examples

To configure a static sticky entry based on the HTTP content and the server name and port number, enter:

```
host1/Admin(config-sticky-content)# static content STINGRAY rserver SERVER1 4000
```

To remove the static HTTP content entry from the sticky table, enter:

```
host1/Admin(config-sticky-content)# no static content STINGRAY rserver SERVER1 4000
```

Related Commands

(config) sticky http-content

(config-sticky-content) timeout

To configure an HTTP content sticky timeout, use the **timeout** *minutes* command. Use the **no** form of this command to reset the sticky timeout to the default of 1440 minutes (24 hours).

timeout {*minutes* | **activeconns**}

no timeout {*minutes* | **activeconns**}

Syntax Description

minutes	Number of minutes that the ACE remembers the last real server to which a client made a sticky connection. Enter an integer from 1 to 65535. The default timeout value is 1440 minutes (24 hours).
activeconns	Specifies that sticky entries are timed out when the sticky timer expires even if there are active connections.

Command Modes

Sticky HTTP content configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The sticky timeout specifies the period of time that the ACE keeps the HTTP content sticky information for a client connection in the sticky table after the latest client connection terminates. The ACE resets the sticky timer for a specific sticky-table entry each time that the appliance opens a new connection matching that entry.

By default, the ACE times out a sticky table entry when the timeout for that entry expires and no active connections matching that entry exist. To specify that the ACE time out HTTP content sticky table entries even if active connections exist after the sticky timer expires, use the **timeout activeconns** command.

Examples

To specify a timeout value of 720 minutes, enter:

```
host1/Admin(config-sticky-content)# timeout 720
```

To reset the timeout to the default value of 1440 minutes (24 hours), enter:

```
host1/Admin(config-sticky-content)# no timeout 720
```

To specify that the ACE time out HTTP content sticky table entries even if active connections exist after the sticky timer expires, enter:

```
host1/Admin(config-sticky-content)# timeout activeconns
```

To restore the ACE to its default of not timing out HTTP content sticky entries if active connections exist for those entries, enter:

```
host1/Admin(config-sticky-content)# no timeout activeconns
```

Related Commands

(config) sticky http-content

Sticky HTTP Header Configuration Mode Commands

Sticky HTTP header configuration mode commands allow you to create an HTTP header sticky group to enable the ACE to stick client connections to the same real server based on HTTP headers. To access sticky HTTP header configuration mode, use the **sticky http-header** command. The prompt changes to (config-sticky-header). Use the **no** form of this command to remove the sticky group from the configuration.

sticky http-header *name1 name2*

no sticky http-header *name1 name2*

Syntax Description

name1	HTTP header name. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. Alternatively, you can enter one of the standard HTTP headers described in Table 2-18.
name2	Unique identifier of the sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the sticky feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can create a maximum of 4096 sticky groups in the ACE.

By default, the maximum number of bytes that the ACE parses to check for a cookie, HTTP header, or URL is 2048. If a cookie, HTTP header, or URL exceeds the default value, the ACE drops the packet and sends a RST (reset) to the client browser. You can increase the number of bytes that the ACE parses using the **(config-parammap-http) set header-maxparse-length** command in HTTP parameter-map configuration mode.

You can also change the default behavior of the ACE when a cookie, header, or URL exceeds the maximum parse length using the **(config-parammap-http) length-exceed** command in HTTP parameter-map configuration mode.

Table 2-18 lists and describes the standard HTTP header names.

Table 2-18 HTTP Header Names

Field Name	Description
Accept	Semicolon-separated list of representation schemes (content type metainformation values) that will be accepted in the response to the request.
Accept-Charset	Character sets that are acceptable for the response. This field allows clients that can understand more comprehensive or special-purpose character sets to signal that capability to a server that can represent documents in those character sets.
Accept-Encoding	Restricts the content encoding that a user will accept from the server.
Accept-Language	ISO code for the language in which the document is written. The language code is an ISO 3316 language code with an optional ISO 639 country code to specify a national variant.
Authorization	Specifies that the user agent wants to authenticate itself with a server, usually after receiving a 401 response.
Cache-Control	Directives that must be obeyed by all caching mechanisms on the request/response chain. The directives specify behavior intended to prevent caches from adversely interfering with the request or response.
Connection	Allows the sender to specify connection options.
Content-MD5	MD5 digest of the entity body that provides an end-to-end integrity check. Only a client or an origin server can generate this header field.
Expect	Used by a client to inform the server about the behaviors that the client requires.
From	E-mail address of the person who controls the requesting user agent.
Host	Internet host and port number of the resource being requested, as obtained from the original URI given by the user or referring resource. The Host field value must represent the naming authority of the origin server or gateway given by the original URL.
If-Match	Used with a method to make it conditional. A client that has one or more entities previously obtained from the resource can verify that one of those entities is current by including a list of their associated entity tags in the If-Match header field. This feature allows efficient updates of cached information with a minimum amount of transaction overhead. It is also used, on updating requests, to prevent inadvertent modification of the wrong version of a resource. As a special case, the asterisk (*) value matches any current entity of the resource.
Pragma	Pragma directives that are understood by servers to which the directives are relevant. The syntax is the same as for other multiple-value fields in HTTP. For example, the **accept** field is a comma-separated list of entries for which the optional parameters are separated by semicolons.
Referer	Address (URI) of the resource from which the URI in the request was obtained.
Transfer-Encoding	What (if any) type of transformation has been applied to the message body in order to safely transfer it between the sender and the recipient.

Table 2-18 HTTP Header Names (continued)

Field Name	Description
User-Agent	Information about the user agent (for example, a software program originating the request). This information is for statistical purposes, the tracing of protocol violations, and automated recognition of user agents for tailoring responses to avoid user agent limitations.
Via	Used by gateways and proxies to indicate the intermediate protocols and recipients between the user agent and the server on requests and between the origin server and the client on responses.

Examples

To create a group for HTTP header stickiness, enter:

```
host1/Admin(config-sticky-header)# sticky http-header Host GROUP4
```

To remove the sticky group from the configuration, enter:

```
host1/Admin(config-sticky-header)# no sticky http-header Host GROUP4
```

Related Commands

show running-config
show sticky database
(config) sticky http-cookie
(config) sticky ip-netmask

(config-sticky-header) header

To configure the HTTP header offset and length, use the **header** command. Use the **no** form of this command to remove the HTTP header offset and length values from the configuration.

header offset *number1* [**length** *number2*]

no header offset *number1* [**length** *number2*]

Syntax Description

offset *number1*	Specifies the portion of the HTTP header that the ACE uses to stick the client on a particular server by indicating the bytes to ignore starting with the first byte of the HTTP header. Enter an integer from 0 to 999. The default is 0, which indicates that the ACE does not exclude any portion of the header.
length *number2*	(Optional) Specifies the length of the portion of the HTTP header (starting with the byte after the offset value) that the ACE uses for sticking the client to the server. Enter an integer from 1 to 1000. The default is 1000.

Command Modes

Sticky HTTP header configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The ACE stores header offset and length values in the sticky table.

You can configure the ACE to use a portion of an HTTP header to make persistent connections to a specific server. To define the portion of the HTTP header that you want the ACE to use, you specify HTTP header offset and length values. The offset and length can vary from 0 to 1000 bytes. The ACE sticks the connection based on that portion of the HTTP header that starts with the byte after the offset value and ends with the byte specified by the offset plus the length. The total bytes represented by the header offset and length cannot exceed 1000.

Examples

To configure the header offset and length, enter:

```
host1/Admin(config-sticky-header)# header offset 300 length 900
```

To remove the HTTP header offset and length values from the configuration, enter:

```
host1/Admin(config-sticky-header)# no header offset 300 length 900
```

Related Commands

(config) sticky http-header

(config-sticky-header) replicate sticky

To instruct the ACE to replicate HTTP header sticky table entries on the standby ACE, use the **replicate sticky** command. Use the **no** form of this command to restore the ACE to its default of not replicating HTTP header sticky table entries.

replicate sticky

no replicate sticky

Syntax Description

This command has no keywords or arguments.

Command Modes

Sticky HTTP header configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

If you are using redundancy, you can configure the ACE to replicate HTTP header sticky table entries on the standby ACE so if a switchover occurs, the new active ACE can maintain existing sticky connections.

The timer of a sticky table entry on the standby ACE is reset every time the entry is synchronized with the active ACE entry. Thus, the standby sticky entry may have a lifetime up to twice as long as the active entry. However, if the entry expires on the active ACE or a new real server is selected and a new entry is created, the old entry on the standby ACE is replaced.

Examples

To instruct the ACE to replicate HTTP header sticky table entries on the standby ACE, enter:

```
host1/Admin(config-sticky-header)# replicate sticky
```

To restore the ACE to its default of not replicating HTTP header sticky table entries, enter:

```
host1/Admin(config-sticky-header)# no replicate sticky
```

Related Commands

(config) sticky http-header

(config-sticky-header) serverfarm

To complete a sticky group configuration, you must configure a server farm entry for the group. To configure a server farm entry for a sticky group, use the **serverfarm** command. Use the **no** form of this command to dissociate a server farm from a sticky group.

serverfarm *name1* [**backup** *name2* [**sticky**] [**aggregate-state**]]

no serverfarm

Syntax Description

name1	Identifier of an existing server farm that you want to associate with the sticky group. You can associate one server farm with each sticky group. Enter a name as an unquoted text string with no spaces and a maximum of 64 characters.
backup *name2*	(Optional) Specifies the identifier of an existing server farm that you want the ACE to use as a backup server farm. If the primary server farm is unavailable, the ACE uses the configured backup server farm. The backup server farm becomes sticky when you enter the **sticky** keyword. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
sticky	(Optional) Specifies that the backup server farm is sticky.
aggregate-state	(Optional) Specifies that the state of the primary server farm is tied to the state of all the real servers in that server farm and in the backup server farm, if configured. The ACE declares the primary server farm down if all real servers in the primary server farm and all real servers in the backup server farm are down.

Command Modes

Sticky HTTP header configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

If all the servers in the primary server farm fail, the ACE sends all connections to the backup server farm. When the primary server farm comes back up (at least one server becomes active):

- If the **sticky** option is enabled, then:
  - All new sticky connections that match existing sticky table entries for the real servers in the backup server farm are stuck to the same real servers in the backup server farm.
  - All new non-sticky connections and those sticky connections that do not have an entry in the sticky table are load balanced to the real servers in the primary server farm.
- If the **sticky** option is not enabled, then the ACE load balances all new connections to the real servers in the primary server farm.
- Existing non-sticky connections to the servers in the backup server farm are allowed to complete in the backup server farm.

You can fine-tune the conditions under which the primary server farm fails over and returns to service by configuring a partial server farm failover. For details about partial server farm failover, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To associate a server farm with a sticky group and specify a sticky backup server farm, enter:

```
host1/Admin(config-sticky-header)# serverfarm SFARM1 backup BKUP_SFARM2 sticky
aggregate-state
```

To dissociate a server farm from a sticky group, enter:

```
host1/Admin(config-sticky-header)# no serverfarm
```

Related Commands

(config) serverfarm
(config) sticky http-header

(config-sticky-header) static header-value

To configure a static header, use the **static header-value** command. Use the **no** form of this command to remove a static header from the configuration.

static header-value *value* **rserver** *name* [*number*]

no static header-value *value* **rserver** *name* [*number*]

Syntax Description

value	Header string value. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters. Alterrnatively, you can enter a text string with spaces provided that you enclose the entire string in quotation marks (“).
rserver *name*	Specifies the hostname of an existing real server. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
number	(Optional) Port number of the real server. Enter an integer from 1 to 65535.

Command Modes

Sticky HTTP header configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You can configure the ACE to use static header sticky entries based on HTTP header values and optionally, real server names and ports. Static sticky header values remain constant over time. You can configure multiple static header entries, but only one unique real-server name can exist for a given static header sticky value.

When you configure a static entry, the ACE enters it into the sticky table immediately. You can create a maximum of 4096 static sticky entries in the ACE.

Examples

To configure a static header, enter:

```
host1/Admin(config-sticky-header)# static header-value CORVETTE rserver SERVER1 4000
```

To remove a static header from the configuration, enter:

```
host1/Admin(config-sticky-header)# no static header-value CORVETTE rserver SERVER1 4000
```

Related Commands

(config) sticky http-header

(config-sticky-header) timeout

To configure an HTTP header sticky timeout, use the **timeout** *minutes* command. Use the **no** form of this command to reset the sticky timeout to the default of 1440 minutes.

timeout {*minutes* | **activeconns**}

no timeout {*minutes* | **activeconns**}

Syntax Description

minutes	Length of time in minutes that the ACE appliance remembers the last real server to which a client made a sticky connection. Enter an integer from 1 to 65535. The default timeout value is 1440 minutes (24 hours).
activeconns	Specifies that sticky entries are timed out when the timer expires even if there are active connections.

Command Modes

Sticky HTTP header configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The sticky timeout specifies the period of time that the ACE keeps the HTTP header sticky information for a client connection in the sticky table after the latest client connection terminates. The ACE resets the sticky timer for a specific sticky-table entry each time that the appliance opens a new connection matching that entry.

By default, the ACE times out a sticky table entry when the timeout for that entry expires and no active connections matching that entry exist. To specify that the ACE time out HTTP header sticky table entries even if active connections exist after the sticky timer expires, use the **timeout activeconns** command.

Examples

To specify a timeout value of 720 minutes, enter:

```
host1/Admin(config-sticky-header)# timeout 720
```

To reset the timeout to the default value of 1440 minutes (24 hours), enter:

```
host1/Admin(config-sticky-header)# no timeout 720
```

To specify that the ACE time out HTTP header sticky table entries even if active connections exist after the sticky timer expires, enter:

```
host1/Admin(config-sticky-content)# timeout activeconns
```

To restore the ACE to its default of not timing out HTTP header sticky entries if active connections exist for those entries, enter:

```
host1/Admin(config-sticky-header)# no timeout activeconns
```

Related Commands

(config) sticky http-header

Sticky IP Configuration Mode Commands

Sticky IP configuration mode commands allow you to create a sticky group for IP address stickiness. To create a sticky group and access sticky IP configuration mode, use the **sticky ip-netmask** command. The prompt changes to (config-sticky-ip). Use the **no** form of this command to remove the sticky group from the configuration.

sticky ip-netmask *netmask* **address** {**source** | **destination** | **both**} *name*

no sticky ip-netmask *netmask* **address** {**source** | **destination** | **both**} *name*

Syntax Description

netmask	Network mask that the ACE applies to the IP address. Enter a network mask in dotted-decimal notation (for example, 255.255.255.0).
address {**source** | **destination** | **both**}	Specifies the IP address used for stickiness. Enter one of the following keywords: • **source**—Specifies that the ACE use the client source IP address to stick the client to a server. You use this keyword in web application environments. • **destination**—Specifies that the ACE use the destination address specified in the client request to stick the client to a server. You use this keyword in caching environments. • **both**—Specifies that the ACE use both the source IP address and the destination IP address to stick the client to a server.
name	Unique identifier of the sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the sticky feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can create a maximum of 4096 sticky groups on the ACE.

Examples

To create a sticky group that uses IP address stickiness based on both the source IP address and the destination IP address, enter:

```
host1/Admin(config)# sticky ip-netmask 255.255.255.0 address both GROUP1
host1/Admin(config-sticky-ip)#
```

To remove the sticky group from the configuration, enter:

```
host1/Admin(config)# no sticky ip-netmask 255.255.255.0 address both GROUP1
```

Related Commands

show running-config
show sticky database
(config) sticky http-cookie
(config) sticky http-header

(config-sticky-ip) replicate sticky

To instruct the ACE to replicate IP address sticky table entries on the standby ACE, use the **replicate sticky** command. Use the **no** form of this command to restore the ACE to its default of not replicating IP address sticky table entries.

replicate sticky

no replicate sticky

Syntax Description

This command has no keywords or arguments.

Command Modes

Sticky IP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

If you are using redundancy, you can configure the ACE to replicate IP address sticky table entries on the standby ACE so that, if a switchover occurs, the new active ACE can maintain existing sticky connections.

The timer of a sticky table entry on the standby ACE is reset every time the entry is synchronized with the active ACE entry. Thus, the standby sticky entry may have a lifetime up to twice as long as the active entry. However, if the entry expires on the active ACE or a new real server is selected and a new entry is created, the old entry on the standby ACE is replaced.

Examples

To instruct the ACE to replicate IP address sticky table entries on the standby ACE, enter:

```
host1/Admin(config-sticky-ip)# replicate sticky
```

To restore the ACE default of not replicating IP address sticky table entries, enter:

```
host1/Admin(config-sticky-ip)# no replicate sticky
```

Related Commands (config) sticky ip-netmask

(config-sticky-ip) serverfarm

To complete a sticky group configuration, you must configure a server farm entry for the group. To configure a server farm entry for a sticky group, use the **serverfarm** command. Use the **no** form of this command to dissociate a server farm from a sticky group.

serverfarm *name1* [**backup** *name2* [**sticky**] [**aggregate-state**]]

no serverfarm

Syntax Description

name1	Identifier of an existing server farm that you want to associate with the sticky group. You can associate one server farm with each sticky group. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
backup *name2*	(Optional) Specifies the identifier of an existing server farm that you want the ACE to use as a backup server farm. If the primary server farm is unavailable, the ACE uses the configured backup server farm. The backup server farm becomes sticky when you enter the **sticky** keyword. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
sticky	(Optional) Specifies that the backup server farm is sticky.
aggregate-state	(Optional) Specifies that the state of the primary server farm is tied to the state of all the real servers in that server farm and in the backup server farm, if configured. The ACE declares the primary server farm down if all real servers in the primary server farm and all real servers in the backup server farm are down.

Command Modes

Sticky IP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

If all the servers in the primary server farm fail, the ACE sends all connections to the backup server farm. When the primary server farm comes back up (at least one server becomes active):

- If the **sticky** option is enabled, then:

  - All new sticky connections that match existing sticky table entries for the real servers in the backup server farm are stuck to the same real servers in the backup server farm.
  - All new non-sticky connections and those sticky connections that do not have an entry in the sticky table are load balanced to the real servers in the primary server farm.
- If the **sticky** option is not enabled, then the ACE load balances all new connections to the real servers in the primary server farm.
- Existing non-sticky connections to the servers in the backup server farm are allowed to complete in the backup server farm.

You can fine-tune the conditions under which the primary server farm fails over and returns to service by configuring a partial server farm failover. For details about partial server farm failover, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To associate a server farm with a sticky group and specify a sticky backup server farm, enter:

```
host1/Admin(config-sticky-ip)# serverfarm SFARM1 backup BKUP_SFARM2 sticky aggregate-state
```

To dissociate a server farm from a sticky group, enter:

```
host1/Admin(config-sticky-ip)# no serverfarm
```

Related Commands

(config) sticky ip-netmask

(config-sticky-ip) static client source

To configure static sticky-IP table entries, use the **static client** command. Use the **no** form of this command to remove the static entry from the sticky table.

The syntax of this command varies according to the **address** option that you chose when you created the sticky group using the **(config) sticky ip-netmask** command. If you configured the sticky group with the **source** option, the syntax of this command is as follows:

static client source *ip_address* **rserver** *name* [*number*]

no static client source *ip_address* **rserver** *name* [*number*]

If you configured the sticky group with the **destination** option, the syntax of this command is as follows:

static client destination *ip_address* **rserver** *name* [*number*]

no static client destination *ip_address* **rserver** *name* [*number*]

If you configured the sticky group with the **both** option, the syntax of this command is as follows:

static client source *ip_address* **destination** *ip_address* **rserver** *name* [*number*]

no static client source *ip_address* **destination** *ip_address* **rserver** *name* [*number*]

Syntax Description

source *ip-address*	Specifies that the static entry is based on the source IP address. Enter an IP address in dotted-decimal notation (for example, 192.168.12.15).
rserver *name*	Specifies that the static entry is based on the real server name. Enter the name of an existing real server as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
number	(Optional) Port number of the real server. Enter an integer from 1 to 65535.
destination *ip-address*	Specifies that the static entry is based on the destination IP address. Enter an IP address in dotted-decimal notation (for example, 172.16.27.3).

Command Modes

Sticky IP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You can configure static sticky table entries based on the source IP address, the destination IP address, or the real server name and port. Static sticky-IP values remain constant over time and you can configure multiple static entries. When you configure a static entry, the ACE enters it into the sticky table immediately. You can configure a maximum of 4096 static sticky entries in the ACE.

Examples

To configure a static sticky entry based on the source IP address, the destination IP address, and the server name and port number, enter:

```
host1/Admin(config-sticky-ip)# static client source 192.168.12.15 destination 172.16.27.3
rserver SERVER1 2000
```

To remove the static entry from the sticky table, enter:

```
host1/Admin(config-sticky-ip)# no static client source 192.168.12.15 destination
172.16.27.3 rserver SERVER1 2000
```

Related Commands

(config) sticky ip-netmask

(config-sticky-ip) timeout

To configure an IP address sticky timeout, use the **timeout** *minutes* command. Use the **no** form of this command to reset the sticky timeout to the default of 1440 minutes (24 hours).

timeout {*minutes* | **activeconns**}

no timeout {*minutes* | **activeconns**}

Syntax Description

minutes	Number of minutes that the ACE remembers the last real server to which a client made a sticky connection. Enter an integer from 1 to 65535. The default timeout value is 1440 minutes (24 hours).
activeconns	Specifies that sticky entries are timed out when the timer expires even if there are active connections.

Command Modes

Sticky IP configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The sticky timeout specifies the period of time that the ACE keeps (if possible) the IP address sticky information for a client connection in the sticky table after the latest client connection terminates. The ACE resets the sticky timer for a specific sticky-table entry each time that the appliance opens a new connection or receives a new HTTP GET on an existing connection matching that entry. High connection rates may cause the sticky table entries to age out prematurely.

By default, the ACE times out a sticky table entry when the timeout for that entry expires and no active connections matching that entry exist. To specify that the ACE time out IP address sticky table entries even if active connections exist after the sticky timer expires, use the **timeout activeconns** command.

Examples

To specify a timeout value of 720 minutes, enter:

```
host1/Admin(config-sticky-ip)# timeout 720
```

To specify that the ACE time out IP address sticky table entries even if active connections exist after the sticky timer expires, enter:

```
host1/Admin(config-sticky-ip)# timeout activeconns
```

To restore the ACE to its default of not timing out IP address sticky entries if active connections exist, enter:

```
host1/Admin(config-sticky-ip)# no timeout activeconns
```

Related Commands

(config) sticky ip-netmask

Sticky Layer 4 Payload Configuration Mode Commands

Sticky Layer 4 payload configuration mode commands allow you to configure the ACE to stick client connections to the same real server based on a string in the payload portion of the Layer 4 protocol packet. To create a Layer 4 payload sticky group and access sticky Layer 4 payload configuration mode, use the **sticky layer4-payload** command. The prompt changes to (config-sticky-l4payloa). Use the **no** form of this command to remove the sticky group from the configuration.

sticky layer4-payload *name*

no sticky layer4-payload *name*

Syntax Description

name	Unique identifier of the sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The commands in this mode require the sticky feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can create a maximum of 4096 sticky groups on the ACE.

Examples

To create a sticky group that uses Layer 4 payload stickiness, enter:

```
host1/Admin(config)# sticky layer4-payload L4_PAYLOAD_GROUP
host1/Admin(config-sticky-l4payloa)#
```

To remove the sticky group from the configuration, enter:

```
host1/Admin(config)# no sticky layer4-payload L4_PAYLOAD_GROUP
```

Related Commands

show running-config
show sticky database

(config-sticky-l4payloa) layer4-payload

To define the portion of the payload that you want the ACE to match, use the **layer4-payload** command. Using this command, you can specify payload offset and length values and a beginning and ending pattern based on a regular expression. The ACE stores these values in the sticky table and uses them to stick a client to a particular server. Use the **no** form of this command to remove the Layer 4 payload specification from the sticky table.

layer4-payload [**offset** *number1*] [**length** *number2*] [**begin-pattern** *expression1*] [**end-pattern** *expression2*]

no layer4-payload [**offset** *number1*] [**length** *number2*] [**begin-pattern** *expression1*] [**end-pattern** *expression2*]

Syntax Description

offset *number1*	(Optional) Specifies the portion of the payload that the ACE uses to stick the client on a particular server by indicating the bytes to ignore starting with the first byte of the payload. Enter an integer from 0 to 999. The default is 0, which indicates that the ACE does not exclude any portion of the payload.
length *number2*	(Optional) Specifies the length of the portion of the payload (starting with the byte after the offset value) that the ACE uses for sticking the client to the server. Enter an integer from 1 to 1000. The default is the entire payload. The offset and length can vary from 0 to 1000 bytes. If the payload is longer than the offset but shorter than the offset plus the length of the payload, the ACE sticks the connection based on that portion of the payload starting with the byte after the offset value and ending with the byte specified by the offset plus the length. The total of the offset and the length cannot exceed 1000. You cannot specify both the **length** and the **end-pattern** options in the same **layer4-payload** command.
begin-pattern *expression1*	(Optional) Specifies the beginning pattern of the Layer 4 payload and the pattern string to match before hashing. If you do not specify a beginning pattern, the ACE starts parsing immediately following the offset byte. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters for each pattern that you configure. You can enter a text string with spaces if you enclose the entire string in quotation marks (“). The ACE supports the use of regular expressions for matching string expressions. When matching data strings, the period (.) and question mark (?) characters do not have a literal meaning in regular expressions. Use brackets ([]) to match these symbols (for example, enter www[.]xyz[.]com instead of www.xyz.com). You can also use a backslash (\) to escape a dot (.) or a question mark (?).

end-pattern *expression2*	(Optional) Specifies the pattern that marks the end of hashing. If you do not specify either a length or an ending pattern, the ACE continues to parse the data until it reaches the end of the field or the end of the packet, or until it reaches the maximum body parse length. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters for each pattern that you configure. You can enter a text string with spaces if you enclose the entire string in quotation marks (“). The ACE supports the use of regular expressions for matching string expressions. You cannot specify both the **length** and the **end-pattern** options in the same **layer4-payload** command.

Command Modes

Sticky Layer 4 payload configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

A Layer 4 payload may change over time with only a portion remaining constant throughout a transaction between the client and a server. You configure the ACE to use either a specific portion or the constant portion of a Layer 4 payload to make persistent connections to a specific server. To define the portion of the payload that you want the ACE to use, you specify payload offset and length values and a beginning and ending pattern. The ACE stores these values in the sticky table.

Examples

To create a Layer 4 payload specification that the ACE will use to stick traffic to a server, enter:

```
host1/Admin(config-sticky-l4payloa)# layer4-payload offset 250 length 750 begin-pattern
abc123.*
```

To remove the Layer 4 payload specification from the configuration, enter:

```
host1/Admin(config-sticky-l4payloa)# no layer4-payload
```

Related Commands

(config) sticky layer4-payload

(config-sticky-l4payloa) replicate sticky

To instruct the ACE to replicate Layer 4 payload sticky table entries on the standby ACE, use the **replicate sticky** command. Use the **no** form of this command to restore the ACE to its default of not replicating Layer 4 payload sticky table entries.

replicate sticky

no replicate sticky

Syntax Description

This command has no keywords or arguments.

Command Modes

Sticky Layer 4 payload configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

If you are using redundancy, you can configure the ACE to replicate Layer 4 payload sticky table entries on the standby ACE so if a switchover occurs, the new active ACE can maintain existing sticky connections.

The timer of a sticky table entry on the standby ACE is reset every time the entry is synchronized with the active ACE entry. Thus, the standby sticky entry may have a lifetime up to twice as long as the active entry. However, if the entry expires on the active ACE or a new real server is selected and a new entry is created, the old entry on the standby ACE is replaced.

Examples

To instruct the ACE to replicate Layer 4 payload sticky table entries on the standby ACE, enter:

```
host1/Admin(config-sticky-l4payloa)# replicate sticky
```

To restore the ACE default of not replicating Layer 4 payload sticky table entries, enter:

```
host1/Admin(config-sticky-l4payloa)# no replicate sticky
```

Related Commands

(config) sticky layer4-payload

(config-sticky-l4payloa) response sticky

To instruct the ACE to parse the response bytes from a server and perform sticky learning, use the **response sticky** command. Use the **no** form of this command to restore the ACE to its default of not parsing the response from a server.

response sticky

no response sticky

Syntax Description

This command has no keywords or arguments.

Command Modes

Sticky Layer 4 payload configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

Use this command when you want the ACE to parse both the request from the client and the response from the server. Sticky learning allows the ACE to populate the sticky database with a hash of the response bytes from a server. The next time a client request arrives with those same bytes, then the ACE sticks the client to the same server.

Examples

To instruct the ACE to perform sticky learning on responses from a server, enter:

```
host1/Admin(config-sticky-l4payloa)# response sticky
```

To restore the ACE default of not performing sticky learning on responses from a server, enter:

```
host1/Admin(config-sticky-l4payloa)# no response sticky
```

Related Commands

(config) sticky layer4-payload

(config-sticky-l4payloa) serverfarm

To complete a sticky group configuration, you must configure a server farm entry for the group. To configure a server farm entry for a sticky group, use the **serverfarm** command. Use the **no** form of this command to dissociate a server farm from a sticky group.

serverfarm *name1* [**backup** *name2* [**sticky**] [**aggregate-state**]]

no serverfarm

Syntax Description

name1	Identifier of an existing server farm that you want to associate with the sticky group. You can associate one server farm with each sticky group. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
backup *name2*	(Optional) Specifies the identifier of an existing server farm that you want the ACE to use as a backup server farm. If the primary server farm is unavailable, the ACE uses the configured backup server farm. The backup server farm becomes sticky when you enter the **sticky** keyword. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
sticky	(Optional) Specifies that the backup server farm is sticky.
aggregate-state	(Optional) Specifies that the state of the primary server farm is tied to the state of all the real servers in that server farm and in the backup server farm, if configured. The ACE declares the primary server farm down if all real servers in the primary server farm and all real servers in the backup server farm are down.

Command Modes

Sticky Layer 4 payload configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

If all the servers in the primary server farm fail, the ACE sends all connections to the backup server farm. When the primary server farm comes back up (at least one server becomes active):

- If the **sticky** option is enabled, then:
  - All new sticky connections that match existing sticky table entries for the real servers in the backup server farm are stuck to the same real servers in the backup server farm.
  - All new non-sticky connections and those sticky connections that do not have an entry in the sticky table are load balanced to the real servers in the primary server farm.
- If the **sticky** option is not enabled, then the ACE load balances all new connections to the real servers in the primary server farm.
- Existing non-sticky connections to the servers in the backup server farm are allowed to complete in the backup server farm.

You can fine-tune the conditions under which the primary server farm fails over and returns to service by configuring a partial server farm failover. For details about partial server farm failover, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To associate a server farm with a Layer 4 payload sticky group and specify a sticky backup server farm, enter:

```
host1/Admin(config-sticky-l4payloa)# serverfarm SFARM1 backup BKUP_SFARM2 sticky
aggregate-state
```

To dissociate a server farm from a Layer 4 payload sticky group, enter:

```
host1/Admin(config-sticky-l4payloa)# no serverfarm
```

Related Commands

(config) sticky layer4-payload

(config-sticky-l4payloa) static layer4-payload

To configure static Layer 4 payload sticky table entries, use the **static layer4-payload** command. Use the **no** form of this command to remove the static entry from the sticky table.

static layer4-payload *value* **rserver** *name* [*number*]

no static layer4-payload *value* **rserver** *name* [*number*]

Syntax Description

value	Payload string value. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters. You can enter a text string with spaces if you enclose the entire string in quotation marks (“).
rserver *name*	Specifies that the static entry is based on the real server name. Enter the name of an existing real server as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
number	(Optional) Port number of the real server. Enter an integer from 1 to 65535.

Command Modes

Sticky Layer 4 payload configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines You can configure static sticky table entries based on the Layer 4 payload and optionally, the real server name and port. Static sticky Layer 4 payload values remain constant over time. You can configure multiple static payload entries, but only one unique real-server name can exist for a given static payload value. When you configure a static entry, the ACE enters it into the sticky table immediately. You can configure a maximum of 4096 static sticky entries in the ACE.

Examples To configure a static sticky entry based on the Layer 4 payload and the server name and port number, enter:

```
host1/Admin(config-sticky-l4payloa)# static layer4-payload STINGRAY rserver SERVER1 4000
```

To remove the static Layer 4 payload entry from the sticky table, enter:

```
host1/Admin(config-sticky-l4payloa)# no static layer4-payload STINGRAY rserver SERVER1
4000
```

Related Commands **(config) sticky layer4-payload**

(config-sticky-l4payloa) timeout

To configure a Layer 4 payload sticky timeout, use the **timeout** *minutes* command. Use the **no** form of this command to reset the sticky timeout to the default of 1440 minutes (24 hours).

timeout {*minutes* | **activeconns**}

no timeout {*minutes* | **activeconns**}

Syntax Description

minutes	Number of minutes that the ACE remembers the last real server to which a client made a sticky connection. Enter an integer from 1 to 65535. The default timeout value is 1440 minutes (24 hours).
activeconns	Specifies that sticky entries are timed out when the sticky timer expires even if there are active connections.

Command Modes Sticky Layer 4 payload configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines The sticky timeout specifies the period of time that the ACE keeps the Layer 4 payload sticky information for a client connection in the sticky table after the latest client connection terminates. The ACE resets the sticky timer for a specific sticky-table entry each time that the appliance opens a new connection matching that entry.

By default, the ACE times out a sticky table entry when the timeout for that entry expires and no active connections matching that entry exist. To specify that the ACE time out Layer 4 payload sticky table entries even if active connections exist after the sticky timer expires, use the **timeout activeconns** command.

Examples

To specify a timeout value of 720 minutes, enter:

```
host1/Admin(config-sticky-l4payloa)# timeout 720
```

To specify that the ACE time out Layer 4 payload sticky table entries even if active connections exist after the sticky timer expires, enter:

```
host1/Admin(config-sticky-l4payloa)# timeout activeconns
```

To restore the ACE to its default of not timing out Layer 4 payload sticky entries if active connections exist, enter:

```
host1/Admin(config-sticky-l4payloa)# no timeout activeconns
```

Related Commands

(config) sticky layer4-payload

Sticky RADIUS Configuration Mode Commands

Sticky RADIUS configuration mode commands allow you to configure the ACE to stick client connections to the same real server based on a RADIUS attribute. To create a RADIUS attribute sticky group and access sticky RADIUS configuration mode, use the **sticky radius framed-ip** command. The prompt changes to (config-sticky-radius). Use the **no** form of this command to remove the sticky group from the configuration.

sticky radius framed-ip [**calling-station-id** | **username**] *name*

no sticky radius framed-ip [**calling-station-id** | **username**] *name*

Syntax Description

calling-station-id	(Optional) Specifies stickiness based on the RADIUS framed IP attribute and the calling station ID attribute.
username	(Optional) Specifies stickiness based on the RADIUS framed IP attribute and the username attribute.
name	Unique identifier of the RADIUS sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The commands in this mode require the sticky feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can create a maximum of 4096 sticky groups on the ACE.

Examples

To create a sticky group that uses RADIUS attribute stickiness, enter:

```
host1/Admin(config)# sticky radius framed-ip calling-station-id RADIUS_GROUP
host1/Admin(config-sticky-radius)#
```

To remove the sticky group from the configuration, enter:

```
host1/Admin(config)# no sticky radius framed-ip calling-station-id RADIUS_GROUP
```

Related Commands

show running-config
show sticky database

(config-sticky-radius) replicate sticky

To instruct the ACE to replicate RADIUS attribute sticky table entries on the standby ACE, use the **replicate sticky** command. Use the **no** form of this command to restore the ACE to its default of not replicating RADIUS sticky group table entries.

replicate sticky

no replicate sticky

Syntax Description

This command has no keywords or arguments.

Command Modes

Sticky RADIUS configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

If you are using redundancy, you can configure the ACE to replicate RADIUS attribute sticky table entries on the standby ACE so if a switchover occurs, the new active ACE can maintain existing sticky connections.

The timer of a sticky table entry on the standby ACE is reset every time the entry is synchronized with the active ACE entry. Thus, the standby sticky entry may have a lifetime up to twice as long as the active entry. However, if the entry expires on the active ACE or a new real server is selected and a new entry is created, the old entry on the standby ACE is replaced.

Examples

To instruct the ACE to replicate RADIUS attribute sticky table entries on the standby ACE, enter:

```
host1/Admin(config-sticky-radius)# replicate sticky
```

To restore the ACE default of not replicating RADIUS attribute sticky table entries, enter:

```
host1/Admin(config-sticky-radius)# no replicate sticky
```

Related Commands

(config) sticky radius framed-ip

(config-sticky-radius) serverfarm

To complete a RADIUS attribute sticky group configuration, you must configure a server farm entry for the group. To configure a server farm entry for a sticky group, use the **serverfarm** command. Use the **no** form of this command to dissociate a server farm from a sticky group.

serverfarm *name1* [**backup** *name2* [**sticky**] [**aggregate-state**]]

no serverfarm

Syntax Description

name1	Identifier of an existing server farm that you want to associate with the sticky group. You can associate one server farm with each sticky group. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
backup *name2*	(Optional) Specifies the identifier of an existing server farm that you want the ACE to use as a backup server farm. If the primary server farm is unavailable, the ACE uses the configured backup server farm. The backup server farm becomes sticky when you enter the **sticky** keyword. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
sticky	(Optional) Specifies that the backup server farm is sticky.
aggregate-state	(Optional) Specifies that the state of the primary server farm is tied to the state of all the real servers in that server farm and in the backup server farm, if configured. The ACE declares the primary server farm down if all real servers in the primary server farm and all real servers in the backup server farm are down.

Command Modes

Sticky RADIUS configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

If all the servers in the primary server farm fail, the ACE sends all connections to the backup server farm. When the primary server farm comes back up (at least one server becomes active):

- If the **sticky** option is enabled, then:
  - All new sticky connections that match existing sticky table entries for the real servers in the backup server farm are stuck to the same real servers in the backup server farm.
  - All new non-sticky connections and those sticky connections that do not have an entry in the sticky table are load balanced to the real servers in the primary server farm.
- If the **sticky** option is not enabled, then the ACE load balances all new connections to the real servers in the primary server farm.
- Existing non-sticky connections to the servers in the backup server farm are allowed to complete in the backup server farm.

You can fine-tune the conditions under which the primary server farm fails over and returns to service by configuring a partial server farm failover. For details about partial server farm failover, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To associate a server farm with a RADIUS attribute sticky group and specify a sticky backup server farm, enter:

```
host1/Admin(config-sticky-radius)# serverfarm SFARM1 backup BKUP_SFARM2 sticky
aggregate-state
```

To dissociate a server farm from a RADIUS attribute sticky group, enter:

```
host1/Admin(config-sticky-radius)# no serverfarm
```

Related Commands

(config) sticky radius framed-ip

(config-sticky-radius) timeout

To configure a RADIUS sticky timeout, use the **timeout** *minutes* command. Use the **no** form of this command to reset the sticky timeout to the default of 1440 minutes (24 hours).

timeout {*minutes* | **activeconns**}

no timeout {*minutes* | **activeconns**}

Syntax Description

minutes	Number of minutes that the ACE remembers the last real server to which a client made a sticky connection. Enter an integer from 1 to 65535. The default timeout value is 1440 minutes (24 hours).
activeconns	Specifies that sticky entries are timed out when the sticky timer expires even if there are active connections.

Command Modes

Sticky RADIUS configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The sticky timeout specifies the period of time that the ACE keeps the RADIUS attribute sticky group information for a client connection in the sticky table after the latest client connection terminates. The ACE resets the sticky timer for a specific sticky-table entry each time that the appliance opens a new connection matching that entry.

By default, the ACE times out a sticky table entry when the timeout for that entry expires and no active connections matching that entry exist. To specify that the ACE time out RADIUS sticky group table entries even if active connections exist after the sticky timer expires, use the **timeout activeconns** command.

Examples

To specify a timeout value of 720 minutes, enter:

```
host1/Admin(config-sticky-radius)# timeout 720
```

To specify that the ACE time out RADIUS sticky group table entries even if active connections exist after the sticky timer expires, enter:

```
host1/Admin(config-sticky-radius)# timeout activeconns
```

To restore the ACE to its default of not timing out RADIUS sticky group entries if active connections exist, enter:

```
host1/Admin(config-sticky-radius)# no timeout activeconns
```

Related Commands

(config) sticky radius framed-ip

Sticky RTSP Header Configuration Mode Commands

Sticky RTSP header configuration mode commands allow you to create an RTSP header sticky group to enable the ACE to stick client connections to the same real server based on the RTSP Session header field. To access sticky RTSP header configuration mode, use the **sticky rtsp-header** command. The prompt changes to (config-sticky-header). Use the **no** form of this command to remove the sticky group from the configuration.

sticky rtsp-header Session *name1*

no sticky rtsp-header Session *name1*

Syntax Description

Session	RTSP Session header field. The ACE supports only the RTSP Session header field for stickiness.
name1	Unique identifier of the RTSP sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The commands in this mode require the sticky feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can create a maximum of 4096 sticky groups in the ACE.

Examples

To create a group for RTSP header stickiness, enter:

```
host1/Admin(config)# sticky rtsp-header Session RTSP_GROUP
host1/Admin(config-sticky-header)#
```

To remove the sticky group from the configuration, enter:

```
host1/Admin(config)# no sticky rtsp-header Session RTSP_GROUP
```

Related Commands

show running-config
show sticky database

(config-sticky-header) header

To configure the RTSP Session header offset and length, use the **header** command. Use the **no** form of this command to remove the RTSP Session header offset and length values from the configuration.

header offset *number1* [**length** *number2*]

no header offset *number1* [**length** *number2*]

Syntax Description

offset *number1*	Specifies the portion of the RTSP Session header that the ACE uses to stick the client on a particular server by indicating the bytes to ignore starting with the first byte of the RTSP header. Enter an integer from 0 to 999. The default is 0, which indicates that the ACE does not exclude any portion of the header.
length *number2*	(Optional) Specifies the length of the portion of the RTSP header (starting with the byte after the offset value) that the ACE uses for sticking the client to the server. Enter an integer from 1 to 1000. The default is 1000.

Command Modes

Sticky RTSP header configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The ACE stores header offset and length values in the sticky table.

You can configure the ACE to use a portion of the RTSP header to make persistent connections to a specific server. To define the portion of the RTSP header that you want the ACE to use, you specify RTSP header offset and length values. The offset and length can vary from 0 to 1000 bytes. The ACE sticks the connection based on that portion of the RTSP header that starts with the byte after the offset value and ends with the byte specified by the offset plus the length. The total bytes represented by the header offset and length cannot exceed 1000.

Examples

To configure the header offset and length, enter:

```
host1/Admin(config-sticky-header)# header offset 300 length 900
```

To remove the RTSP header offset and length values from the configuration, enter:

```
host1/Admin(config-sticky-header)# no header offset 300 length 900
```

Related Commands

(config) sticky http-header

(config-sticky-header) replicate sticky

To instruct the ACE to replicate RTSP header sticky table entries on the standby ACE, use the **replicate sticky** command. Use the **no** form of this command to restore the ACE to its default of not replicating RTSP header sticky table entries.

replicate sticky

no replicate sticky

Syntax Description

This command has no keywords or arguments.

Command Modes

Sticky RTSP header configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

If you are using redundancy, you can configure the ACE to replicate RTSP header sticky table entries on the standby ACE so if a switchover occurs, the new active ACE can maintain existing sticky connections.

The timer of a sticky table entry on the standby ACE is reset every time the entry is synchronized with the active ACE entry. Thus, the standby sticky entry may have a lifetime up to twice as long as the active entry. However, if the entry expires on the active ACE or a new real server is selected and a new entry is created, the old entry on the standby ACE is replaced.

Examples

To instruct the ACE to replicate RTSP header sticky table entries on the standby ACE, enter:

```
host1/Admin(config-sticky-header)# replicate sticky
```

To restore the ACE to its default of not replicating RTSP header sticky table entries, enter:

```
host1/Admin(config-sticky-header)# no replicate sticky
```

Related Commands

(config) sticky rtsp-header

(config-sticky-header) serverfarm

To complete an RTSP header sticky group configuration, you must configure a server farm entry for the group. To configure a server farm entry for a sticky group, use the **serverfarm** command. Use the **no** form of this command to dissociate a server farm from a sticky group.

serverfarm *name1* [**backup** *name2* [**sticky**] [**aggregate-state**]]

no serverfarm

Syntax Description

name1	Identifier of an existing server farm that you want to associate with the sticky group. You can associate one server farm with each sticky group. Enter a name as an unquoted text string with no spaces and a maximum of 64 characters.
backup *name2*	(Optional) Specifies the identifier of an existing server farm that you want the ACE to use as a backup server farm. If the primary server farm is unavailable, the ACE uses the configured backup server farm. The backup server farm becomes sticky when you enter the **sticky** keyword. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
sticky	(Optional) Specifies that the backup server farm is sticky.
aggregate-state	(Optional) Specifies that the state of the primary server farm is tied to the state of all the real servers in that server farm and in the backup server farm, if configured. The ACE declares the primary server farm down if all real servers in the primary server farm and all real servers in the backup server farm are down.

Command Modes

Sticky RTSP header configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

If all the servers in the primary server farm fail, the ACE sends all connections to the backup server farm. When the primary server farm comes back up (at least one server becomes active):

- If the **sticky** option is enabled, then:
  - All new sticky connections that match existing sticky table entries for the real servers in the backup server farm are stuck to the same real servers in the backup server farm.
  - All new non-sticky connections and those sticky connections that do not have an entry in the sticky table are load balanced to the real servers in the primary server farm.
- If the **sticky** option is not enabled, then the ACE load balances all new connections to the real servers in the primary server farm.
- Existing non-sticky connections to the servers in the backup server farm are allowed to complete in the backup server farm.

You can fine-tune the conditions under which the primary server farm fails over and returns to service by configuring a partial server farm failover. For details about partial server farm failover, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To associate a server farm with a sticky group and specify a sticky backup server farm, enter:

```
host1/Admin(config-sticky-header)# serverfarm SFARM1 backup BKUP_SFARM2 sticky
aggregate-state
```

To dissociate a server farm from a sticky group, enter:

```
host1/Admin(config-sticky-header)# no serverfarm
```

Related Commands

(config) serverfarm
(config) sticky rtsp-header

(config-sticky-header) static header-value

To configure a static header, use the **static header-value** command. Use the **no** form of this command to remove a static header from the configuration.

static header-value *value* **rserver** *name* [*number*]

no static header-value *value* **rserver** *name* [*number*]

Syntax Description

value	Header value. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters. You can enter a text string with spaces provided that you enclose the entire string in quotation marks (“).
rserver *name*	Specifies the hostname of an existing real server. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
number	(Optional) Port number of the real server. Enter an integer from 1 to 65535.

Command Modes

Sticky RTSP header configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

You can configure the ACE to use static header sticky entries based on the value of the RTSP Session header field and optionally, real server names and ports. Static sticky header values remain constant over time. You can configure multiple static header entries, but only one unique real-server name can exist for a given static header sticky value.

When you configure a static entry, the ACE enters it into the sticky table immediately. You can create a maximum of 4096 static sticky entries in the ACE.

Examples

To configure a static RTSP header sticky entry, enter:

```
host1/Admin(config-sticky-header)# static header-value 12345678 rserver SERVER1 3000
```

To remove the static RTSP header entry from the sticky table, enter:

```
host1/Admin(config-sticky-header)# no static header-value 12345678 rserver SERVER1 3000
```

Related Commands

(config) sticky rtsp-header

(config-sticky-header) timeout

To configure an RTSP header sticky timeout, use the **timeout** *minutes* command. Use the **no** form of this command to reset the sticky timeout to the default of 1440 minutes.

timeout {*minutes* | **activeconns**}

no timeout {*minutes* | **activeconns**}

Syntax Description

minutes	Number of minutes that the ACE remembers the last real server to which a client made a sticky connection. Enter an integer from 1 to 65535. The default timeout value is 1440 minutes (24 hours).
activeconns	Specifies that sticky entries are timed out when the timer expires even if there are active connections.

Command Modes

Sticky RTSP header configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The sticky timeout specifies the period of time that the ACE keeps the RTSP header sticky information for a client connection in the sticky table after the latest client connection terminates. The ACE resets the sticky timer for a specific sticky-table entry each time that the appliance opens a new connection matching that entry.

By default, the ACE times out a sticky table entry when the timeout for that entry expires and no active connections matching that entry exist. To specify that the ACE time out RTSP header sticky table entries even if active connections exist after the sticky timer expires, use the **timeout activeconns** command.

Examples

To specify a timeout value of 720 minutes, enter:

```
host1/Admin(config-sticky-header)# timeout 720
```

To reset the timeout to the default value of 1440 minutes (24 hours), enter:

```
host1/Admin(config-sticky-header)# no timeout 720
```

To specify that the ACE time out RTSP header sticky table entries even if active connections exist after the sticky timer expires, enter:

```
host1/Admin(config-sticky-content)# timeout activeconns
```

To restore the ACE to its default of not timing out RTSP header sticky entries if active connections exist for those entries, enter:

```
host1/Admin(config-sticky-header)# no timeout activeconns
```

Related Commands

(config) sticky rtsp-header

Sticky SIP Header Configuration Mode Commands

Sticky SIP header configuration mode commands allow you to create a SIP header sticky group to enable the ACE to stick client connections to the same real server based on the SIP Call-ID header field. To access sticky SIP header configuration mode, use the **sticky sip-header** command. The prompt changes to (config-sticky-header). Use the **no** form of this command to remove the sticky group from the configuration.

sticky sip-header *name1 name2*

no sticky sip-header *name1 name2*

Syntax Description

name1	SIP header field. The ACE supports only the SIP Call-ID header field for stickiness. Enter **Call-ID**.
name2	Unique identifier of the SIP sticky group. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The commands in this mode require the sticky feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

You can create a maximum of 4096 sticky groups in the ACE.

Examples

To create a group for SIP header stickiness, enter:

```
host1/Admin(config)# sticky sip-header Call-ID SIP_GROUP
host1/Admin(config-sticky-header)#
```

To remove the sticky group from the configuration, enter:

```
host1/Admin(config)# no sticky sip-header Call-ID SIP_GROUP
```

Related Commands

show running-config
show sticky database

(config-sticky-header) replicate sticky

To instruct the ACE to replicate SIP header sticky table entries on the standby ACE, use the **replicate sticky** command. Use the **no** form of this command to restore the ACE to its default of not replicating SIP header sticky table entries.

replicate sticky

no replicate sticky

Syntax Description

This command has no keywords or arguments.

Command Modes

Sticky SIP header configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

If you are using redundancy, you can configure the ACE to replicate SIP header sticky table entries on the standby ACE so if a switchover occurs, the new active ACE can maintain existing sticky connections.

The timer of a sticky table entry on the standby ACE is reset every time the entry is synchronized with the active ACE entry. Thus, the standby sticky entry may have a lifetime up to twice as long as the active entry. However, if the entry expires on the active ACE or a new real server is selected and a new entry is created, the old entry on the standby ACE is replaced.

Examples

To instruct the ACE to replicate SIP header sticky table entries on the standby ACE, enter:

```
host1/Admin(config-sticky-header)# replicate sticky
```

To restore the ACE to its default of not replicating SIP header sticky table entries, enter:

```
host1/Admin(config-sticky-header)# no replicate sticky
```

Related Commands

(config) sticky sip-header

(config-sticky-header) serverfarm

To complete a SIP header sticky group configuration, you must configure a server farm entry for the group. To configure a server farm entry for a sticky group, use the **serverfarm** command. Use the **no** form of this command to dissociate a server farm from a sticky group.

serverfarm *name1* [**backup** *name2* [**sticky**] [**aggregate-state**]]

no serverfarm

Syntax Description

name1	Identifier of an existing server farm that you want to associate with the sticky group. You can associate one server farm with each sticky group. Enter a name as an unquoted text string with no spaces and a maximum of 64 characters.
backup *name2*	(Optional) Specifies the identifier of an existing server farm that you want the ACE to use as a backup server farm. If the primary server farm is unavailable, the ACE uses the configured backup server farm. The backup server farm becomes sticky when you enter the **sticky** keyword. Enter a name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
sticky	(Optional) Specifies that the backup server farm is sticky.
aggregate-state	(Optional) Specifies that the state of the primary server farm is tied to the state of all the real servers in that server farm and in the backup server farm, if configured. The ACE declares the primary server farm down if all real servers in the primary server farm and all real servers in the backup server farm are down.

Command Modes

Sticky SIP header configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

If all the servers in the primary server farm fail, the ACE sends all connections to the backup server farm. When the primary server farm comes back up (at least one server becomes active):

- If the **sticky** option is enabled, then:
  - All new sticky connections that match existing sticky table entries for the real servers in the backup server farm are stuck to the same real servers in the backup server farm.
  - All new non-sticky connections and those sticky connections that do not have an entry in the sticky table are load balanced to the real servers in the primary server farm.
- If the **sticky** option is not enabled, then the ACE load balances all new connections to the real servers in the primary server farm.
- Existing non-sticky connections to the servers in the backup server farm are allowed to complete in the backup server farm.

You can fine-tune the conditions under which the primary server farm fails over and returns to service by configuring a partial server farm failover. For details about partial server farm failover, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Examples

To associate a server farm with a sticky group and specify a sticky backup server farm, enter:

```
host1/Admin(config-sticky-header)# serverfarm SFARM1 backup BKUP_SFARM2 sticky
aggregate-state
```

To dissociate a server farm from a sticky group, enter:

```
host1/Admin(config-sticky-header)# no serverfarm
```

Related Commands

(config) serverfarm
(config) sticky sip-header

(config-sticky-header) static header-value

To configure a static header, use the **static header-value** command. Use the **no** form of this command to remove a static header from the configuration.

static header-value *value* **rserver** *name* [*number*]

no static header-value *value* **rserver** *name* [*number*]

Syntax Description

value	SIP header value. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters. You can enter a text string with spaces provided that you enclose the entire string in quotation marks (“).
rserver *name*	Specifies the hostname of an existing real server. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
number	(Optional) Port number of the real server. Enter an integer from 1 to 65535.

Command Modes

Sticky SIP header configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

You can configure the ACE to use static header sticky entries based on the value of the SIP Call-ID header field and optionally, real server names and ports. Static sticky header values remain constant over time. You can configure multiple static SIP header entries, but only one unique real-server name can exist for a given static SIP header sticky value.

When you configure a static entry, the ACE enters it into the sticky table immediately. You can create a maximum of 4096 static sticky entries in the ACE.

Examples

To configure a static SIP header sticky entry, enter:

```
host1/Admin(config-sticky-header)# static header-value 12345678 rserver SERVER1 3000
```

To remove the static SIP header entry from the sticky table, enter:

```
host1/Admin(config-sticky-header)# no static header-value 12345678 rserver SERVER1 3000
```

Related Commands

(config) sticky sip-header

(config-sticky-header) timeout

To configure a SIP header sticky timeout, use the **timeout** *minutes* command. Use the **no** form of this command to reset the sticky timeout to the default of 1440 minutes.

timeout {*minutes* | **activeconns**}

no timeout {*minutes* | **activeconns**}

Syntax Description

minutes	Number of minutes that the ACE remembers the last real server to which a client made a sticky connection. Enter an integer from 1 to 65535. The default timeout value is 1440 minutes (24 hours).
activeconns	Specifies that sticky entries are timed out when the timer expires even if there are active connections.

Command Modes

Sticky SIP header configuration mode

Admin and user contexts

Command History

Release	Modification
A3(1.0)	This command was introduced.

Usage Guidelines

The sticky timeout specifies the period of time that the ACE keeps the SIP header sticky information for a client connection in the sticky table after the latest client connection terminates. The ACE resets the sticky timer for a specific sticky-table entry each time that the appliance opens a new connection matching that entry.

By default, the ACE times out a sticky table entry when the timeout for that entry expires and no active connections matching that entry exist. To specify that the ACE time out SIP header sticky table entries even if active connections exist after the sticky timer expires, use the **timeout activeconns** command.

Examples

To specify a timeout value of 720 minutes, enter:

```
host1/Admin(config-sticky-header)# timeout 720
```

To reset the timeout to the default value of 1440 minutes (24 hours), enter:

```
host1/Admin(config-sticky-header)# no timeout 720
```

To specify that the ACE time out SIP header sticky table entries even if active connections exist after the sticky timer expires, enter:

```
host1/Admin(config-sticky-content)# timeout activeconns
```

To restore the ACE to its default of not timing out SIP header sticky entries if active connections exist for those entries, enter:

```
host1/Admin(config-sticky-header)# no timeout activeconns
```

Related Commands

(config) sticky sip-header

TACACS+ Configuration Mode Commands

TACACS+ configuration mode commands allow you to configure multiple Terminal Access Controller Access Control System Plus (TACACS+) servers as a named AAA server group. You can specify the IP address of one or more previously configured TACACS+ servers that you want added to or removed from a AAA server group, with a dead-time interval for the TACACS+ server group.

For details about creating a TACACS+ server group, see the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

To create a TACACS+ server group and access TACACS+ server configuration mode, enter the **aaa group server tacacs+** command in configuration mode. The CLI prompt changes to (config-tacacs+). Use the **no** form of this command to remove a TACACS+ server group.

aaa group server tacacs+ *group_name*

no aaa group server tacacs+ *group_name*

Syntax Description

group_name	Name assigned to the group of TACACS+ servers. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

A server group is a list of server hosts. The ACE allows you to configure multiple AAA servers as a named server group. You group the different AAA server hosts into distinct lists. The ACE searches for the server hosts in the order in which you specify them within a group. You can configure a maximum of 10 server groups for each context in the ACE.

You can configure server groups at any time, but you must enter the **aaa authentication login** or the **aaa accounting default** commands to apply the groups to the AAA service.

Examples

To create a TACACS+ server group, enter:

```
host1/Admin(config) aaa group server tacacs+ TACACS+_Server_Group1
host1/Admin(config-tacacs+)# server 172.16.56.76
host1/Admin(config-tacacs+)# server 172.16.56.79
host1/Admin(config-tacacs+)# server 172.16.56.82
```

Related Commands (config) aaa accounting default
(config) aaa authentication login

(config-tacacs+) deadtime

To specify a dead-time interval for the TACACS+ server group, use the **deadtime** command. Use the **no** form of this command to reset the TACACS+ server group dead-time request to the default of 0.

deadtime *minutes*

no deadtime *minutes*

Syntax Description

minutes	Length of time that the ACE skips a nonresponsive TACACS+ server for transaction requests. Valid entries are from 0 to 1440 (24 hours). The default is 0.

Command Modes

TACACS+ configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

During the dead-time interval, the ACE sends probe access-request packets to verify that the TACACS+ server is available and can receive authentication requests. The dead-time interval starts when the server does not respond to an authentication request transmission. When the server responds to a probe access-request packet, the ACE retransmits the authentication request to the server.

Use of the **deadtime** command causes the ACE to mark as dead any TACACS+ servers that fail to respond to authentication requests. Using this command prevents the wait for the request to time out before trying the next configured server. The ACE skips a TACACS+ server that is marked as dead by additional requests for the duration of minutes.

Examples

To globally configure a 15-minute dead-time for TACACS+ servers that fail to respond to authentication requests, enter:

```
host1/Admin(config-tacacs+)# deadtime 15
```

To reset the TACACS+ server dead-time request to the default of 0, enter:

```
host1/Admin(config-tacacs+)# no deadtime 15
```

Related Commands (config) aaa group server

(config-tacacs+) server

To specify the IP address of one or more previously configured TACACS+ servers that you want added to or removed from a AAA server group, use the **server** command. Use the **no** form of this command to remove the TACACS+ server from the AAA server group.

server *ip_address*

no server *ip_address*

Syntax Description

ip_address	IP address of the TACACS+ server. Enter the address in dotted-decimal IP notation (for example, 192.168.11.1).

Command Modes

TACACS+ configuration mode

Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You can add multiple TACACS+ servers to the AAA server group by entering multiple **server** commands in this mode. The same server can belong to multiple server groups.

Examples

To add servers to a TACACS+ server group, enter:

```
host1/Admin(config-tacacs+)# server 172.16.56.76
host1/Admin(config-tacacs+)# server 172.16.56.79
host1/Admin(config-tacacs+)# server 172.16.56.82
```

To remove a server from a TACACS+ server group, enter:

```
host1/Admin(config-tacacs+)# no server 172.16.56.76
```

Related Commands

(config) aaa group server

CLI COMMAND SUMMARY BY MODE

Level1IX