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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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 *Virtualization Guide, Cisco ACE Application Control Engine*.

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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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 *Virtualization Guide, Cisco ACE Application Control Engine*.

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. • For the ACE module, enter an integer from 1 to 255 as the line number. • For the ACE appliance, 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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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 *Virtualization Guide, Cisco ACE Application Control Engine*.

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 *Security Guide, Cisco ACE Application Control Engine* 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 IPv4 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. • For the ACE module, enter an integer from 1 to 255 as the line number. • For the ACE appliance, 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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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 *Virtualization Guide, Cisco ACE Application Control Engine*.

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 IPv4 network traffic, enter:

```
host1/Admin(config)# class-map match-any L4_MATCHANYTRAFFIC_CLASS_IPV4
host1/Admin(config-cmap)# match any
```

Related Commands

(config-cmap) description

(config-cmap) match anyv6

To instruct the ACE to perform a match on any IPv6 network traffic that passes through the device, use the **match anyv6** command. Use the **no** form of this command to remove the match any criteria from the class map.

[*line_number*] **match anyv6**

no [*line_number*] **match anyv6**

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. • For the ACE module, enter an integer from 1 to 255 as the line number. • For the ACE appliance, 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

ACE Module/Appliance Release	Modification
A5(1.0)	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 *Virtualization Guide, Cisco ACE Application Control Engine*.

You can include only one **match anyv6** command within a class map, and you cannot combine the **match anyv6** 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 IPv6 network traffic, enter:

```
host1/Admin(config)# class-map match-any L4_MATCHANYTRAFFIC_CLASS_IPV6
host1/Admin(config-cmap)# match anyv6
```

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** *ipv6_address* [*/prefix_length*] | *ip_address* [*mask*]

no [*line_number*] **match destination-address** *ipv6_address /prefix_length* | *ip_address* [*mask*]

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. • For the ACE module, enter an integer from 1 to 255 as the line number. • For the ACE appliance, 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.
ipv6_address	IPv6 address of the destination.
/prefix_length	(Optional) Specifies the length of the IPv6 prefix.
ip_address	Destination IPv4 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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.
A5(1.0)	Added IPv6 support.

ACE Appliance Release	Modification
A1(7)	This command was introduced.
A5(1.0)	Added IPv6 support.

Usage Guidelines

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

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 IPv4 address and subnet mask.

Examples

IPv6 Example

The following example specifies that the network traffic must match destination IPv6 address 2001:DB8:1::7/64:

```
host1/C1(config)# class-map match-any IP_CLASS
host1/C1(config-cmap)# match destination-address 2001:DB8:1::7/64
```

To remove the destination IPv6 address match criteria from the class map, enter:

```
host1/C1(config-cmap)# no match destination-address 2001:DB8:1::7/64
```

IPv4 Example

The following example specifies that the network traffic must match destination IP address 172.27.16.7:

```
host1/C1(config)# class-map match-any IP_CLASS
host1/C1(config-cmap)# match destination-address 172.27.16.7
```

To remove the destination IP address match criteria from the class map, enter:

```
host1/C1(config-cmap)# no match destination-address 172.27.16.7
```

Related Commands

(config-cmap) description

(config-cmap) match port

To specify a TCP or UDP port number or port range as the IPv4 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. • For the ACE module, enter an integer from 1 to 255 as the line number. • For the ACE appliance, 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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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 *Virtualization Guide, Cisco ACE Application Control Engine*.

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 a port to match, enter the following command:

```
switch/Admin(config)# class-map match-all TCP_ANY
switch/Admin(config-cmap)# match port tcp any
```

Related Commands

(config-cmap) description

(config-cmap) match port-v6

To specify a TCP or UDP port number or port range as the IPv6 network traffic matching criteria, use the **match port-v6** 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-v6** {**tcp** | **udp**} {**any** | **eq** {*port_number*} | **range** *port1 port2*}

no [*line_number*] **match port-v6** {**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. • For the ACE module, enter an integer from 1 to 255 as the line number. • For the ACE appliance, 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

ACE Module/Appliance Release	Modification
A5(1.0)	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 *Virtualization Guide, Cisco ACE Application Control Engine*.

A single class map can have multiple **match port-v6** commands. You can combine multiple **match port-v6**, **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-v6 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** *ipv6_address* [*/prefix_length*] | *ip_address mask*

no [*line_number*] **match source-address** *ipv6_address* [*/prefix_length*] | *ip_address mask*

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. • For the ACE module, enter an integer from 1 to 255 as the line number. • For the ACE appliance, 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.
ipv6_address	Source IPv6 address of the client.
/prefix_length	
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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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 *Virtualization Guide, Cisco ACE Application Control Engine*.

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* {{*/prefix_length* | [*netmask*]} *protocol_number* | **any** | {**tcp** | **udp** {**any** | **eq** *port_number* | **range** *port1 port2*}}}

no [*line_number*] **match virtual-address** *vip_address* {{*/prefix_length* | [*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. • For the ACE module, enter an integer from 1 to 255 as the line number. • For the ACE appliance, 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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.
A2(1.0)	This command was revised.

ACE Appliance 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 *Virtualization Guide, Cisco ACE Application Control Engine*.

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.

The ACE does not allow you to configure a class-map VIP address that overlaps with an ACE interface IP address. If you do, the ACE displays the following warning:

```
Error: Entered VIP address is not the first address in the VIP range
```

See the *Server Load-Balancing Guide, Cisco ACE Application Control Engine* 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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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 *Virtualization Guide, Cisco ACE Application Control Engine*.

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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.
A2(1.0)	This command was revised.

ACE Appliance 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

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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 the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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 any priority for the match statements.
name	Name of an existing Layer 7 generic class map.

Command Modes

Class map generic configuration mode

Admin and user contexts

Command History

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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 the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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 any priority for the match statements.
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 2-9.

Command Modes

Class map generic configuration mode

Admin and user contexts

Command History

ACE Module Release	Modification
A2(1.0)	This command was introduced.
A2(2.1)	This command supports the “\xST” metacharacter.

ACE Appliance 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 2-9 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.
\xST	(ACE module only) Stop metacharacter.

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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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 any 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 generic configuration mode

Admin and user contexts

Command History

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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 *Virtualization Guide, Cisco ACE Application Control Engine*.

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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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. • For the ACE module, enter a range of 1 to 1024 alphanumeric characters. • For the ACE appliance, enter a range of 2 to 1024 alphanumeric characters. For a list of the supported characters that you can use in regular expressions, see Table 2-9.
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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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 2-9 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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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 2-9 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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 and Gnutella. For the ACE appliance, the GoToMyPC application is included.
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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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**. (ACE module only) The ACE also supports the inspection of the following HTTP request extension methods: **notify**, **poll**, **subscribe,** **unsubscribe**, and **x-ms-emumatts**.
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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.
A2(1.0)	This command was revised.

ACE Appliance 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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 2-9.

Command Modes

Class map HTTP inspection configuration mode

Admin and user contexts

Command History

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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 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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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 *Virtualization Guide, Cisco ACE Application Control Engine*.

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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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 *Server Load-Balancing Guide, Cisco ACE Application Control Engine* 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

(ACE appliance only) 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 policy. 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

ACE Appliance 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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	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 2-9.
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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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 2-9.

Command Modes

Class map HTTP load balancing configuration mode

Admin and user contexts

Command History

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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 2-10.
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 2-9.

Command Modes

Class map HTTP load balancing configuration mode

Admin and user contexts

Command History

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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 2-9.

Table 2-10 lists the standard HTTP header fields that you can use in an HTTP load-balancing class map.

Table 2-10 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.
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.

Table 2-10 Standard HTTP Header Fields (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 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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 2-9.
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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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 2-9.

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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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 *Virtualization Guide, Cisco ACE Application Control Engine*.

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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.

ACE Appliance 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** | **icmpv6** | **kalap-udp** | **snmp** | **ssh** | **telnet** | **xml-https**} {**any** | **anyv6** | **source-address** {*ipv6_address/prefix_length* | *ipv4_address mask*}

no [*line_number*] **match protocol** {**http** | **https** | **icmp** | **icmpv6** | **kalap-udp** | **snmp** | **ssh** | **telnet** | **xml-https**} {**any** | **anyv6** | **source-address** {*ipv6_address/prefix_length* | *ipv4_address mask*}

Syntax Description

line_number	(Optional) Line number that allows you to edit or delete individual **match** commands. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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.
http	Specifies the Hypertext Transfer Protocol (HTTP).
https	Specifies the secure (SSL) Hypertext Transfer Protocol (HTTP). (ACE appliance only) 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).
icmpv6	Specifies the Internet Control Message Protocol Version 6 messages to the ACE.
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	(ACE appliance only) 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 IPv4 address for the management traffic classification.
anyv6	Specifies any client source IPv6 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.
ipv6_address	Source IPv6 address of the client.
/prefix_length	Prefix length of the client entry (for example, /64).
ipv4_address	Source IPv4 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

ACE Module Release	Modification
3.0(0)A1(2)	This command was introduced.
A2(1.0)	This command was revised.
A5(1.0)	Added the **anyv6** and **icmpv6** keywords.

ACE Appliance Release	Modification
A1(7)	This command was introduced.
A3(1.0)	This command was revised.
	Added the **anyv6** and **icmpv6** keywords.

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

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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 the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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 any priority for the match statements.
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 2-9.

Command Modes

Class map RADIUS load balancing configuration mode

Admin and user contexts

Command History

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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 the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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 any priority for the match statements.
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

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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 the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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 any priority for the match statements.
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 2-10 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 2-9.

Command Modes

Class map RTSP load balancing configuration mode

Admin and user contexts

Command History

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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 the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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 any priority for the match statements.
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 2-9.
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

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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 2-9 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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 2-9 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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 2-9 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

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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 2-9 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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 2-9 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

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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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 2-9 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. • For the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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 the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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 any priority for the match statements.
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

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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 the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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 any priority for the match statements.

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 2-11. Because SIP is similar to HTTP/1.1, you can use any HTTP header listed in Table 2-10 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 2-9.

Command Modes

Class map SIP load balancing configuration mode

Admin and user contexts

Command History

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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 2-11 lists the standard SIP header fields.

Table 2-11 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.

Table 2-11 Standard SIP Header Fields (continued)

Field Name	Description
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 the ACE module, enter an integer from 1 to 1024 as the line number. • For the ACE appliance, 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 any 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 SIP load balancing configuration mode

Admin and user contexts

Command History

ACE Module Release	Modification
A2(1.0)	This command was introduced.

ACE Appliance 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