

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 the 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: <ul style="list-style-type: none"> • 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).
<i>map_name</i>	Name assigned to the Layer 3 and Layer 4 class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

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

The ACE supports a system-wide maximum of 8192 class maps.

Examples

To create a Layer 3 and Layer 4 class map named L4VIP_CLASS to identify the network traffic that can pass through the ACE for server load balancing, enter:

```
host1/Admin(config)# class-map match-all L4VIP_CLASS
host1/Admin(config-cmap)#
```

Related Commands

(config) [policy-map](#)

(config-cmap) description

To provide a brief summary about a Layer 3 and Layer 4 class map, use the **description** command. Use the **no** form of the command to remove the Layer 3 and Layer 4 class map description from the class map.

description *text*

no description

Syntax Description

<i>text</i>	Description about a Layer 3 and Layer 4 class map. Enter a description as an unquoted text string with a maximum of 240 alphanumeric characters.
-------------	--

Command Modes

Class map configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

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

Examples

To add a description that the class map is to filter network traffic based on the source IP address, enter:

```
host1/Admin(config)# class-map L4_SOURCE_IP_CLASS
host1/Admin(config-cmap)# description match on source IP address of incoming traffic
```

Related Commands

This command has no related commands.

(config-cmap) match access-list

To configure the Layer 3 and Layer 4 class map to filter network traffic using a predefined access control list, use the **match access-list** command. When a packet matches an entry in an access list, and if it is a **permit** entry, the ACE allows the matching result. If it is a **deny** entry, the ACE blocks the matching result. Use the **no** form of the 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

<i>line_number</i>	(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 255 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
<i>name</i>	Previously created access list identifier. Enter an unquoted text string with a maximum of 64 characters.

Command Modes

Class map configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

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

A single class map can have multiple **match access-list** commands. You can combine multiple **match access-list**, **match source-address**, **match destination-address**, and **match port** commands in a class map.

See the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide* for details about the creating access control lists in the ACE.

Examples

To specify that the class map is to match on the access control list INBOUND, enter:

```
host1/Admin(config)# class-map match-any L4_FILTERTRAFFIC_CLASS
host1/Admin(config-cmap)# match access-list INBOUND
```

Related Commands

[\(config-cmap\) description](#)

(config-cmap) match any

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

```
[line_number] match any
```

```
no [line_number] match any
```

Syntax Description

<i>line_number</i>	(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 255 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
--------------------	--

Command Modes

Class map configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

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

You can include only one **match any** command within a class map, and you cannot combine the **match any** command with other types of **match** commands in a class map because the match criteria will be ignored.

Examples

To specify that the class map is to match on any network traffic, enter:

```
host1/Admin(config)# class-map match-any L4_MATCHANYTRAFFIC_CLASS
host1/Admin(config-cmap)# match any
```

Related Commands

[\(config-cmap\) description](#)

(config-cmap) match destination-address

To specify the destination IP address and subnet mask as the network traffic matching criteria, use the **match destination-address** command. Use the **no** form of the command to clear the destination IP address and subnet mask match criteria from the class map.

```
[line_number] match destination-address ip_address [mask]
```

```
no [line_number] match destination-address ip_address [mask]
```

Syntax Description

<i>line_number</i>	(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 255 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
<i>ip_address</i>	Destination IP address. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
<i>mask</i>	(Optional) Subnet mask entry in dotted-decimal notation (for example, 255.255.255.0).

Command Modes

Class map configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

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

A single class map can have multiple **match destination-address** commands. You can combine multiple **match destination-address**, **match access-list**, **match source-address**, and **match port** commands in a class map.

An entry of 0.0.0.0 0.0.0.0 indicates a wildcard match for any destination IP address and subnet mask.

Examples

To specify that the class map is to match on the destination IP address 172.16.20.1 255.255.0.0, enter:

```
host1/Admin(config)# class-map L4_DEST_IP_CLASS
host1/Admin(config-cmap)# match destination-address 172.16.20.1 255.255.0.0
```

Related Commands

[\(config-cmap\) description](#)

(config-cmap) match port

To specify a TCP or UDP port number or port range as the network traffic matching criteria, use the **match port** command. Use the **no** form of the 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

<i>line_number</i>	(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 255 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence 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: <ul style="list-style-type: none"> • TCP port—Specify one of the following names or well-known port numbers: <ul style="list-style-type: none"> – 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) – smtp—Specifies the Simple Mail Transfer Protocol (25) – telnet—Specifies the Telnet protocol (23) – www—Specifies the World Wide Web (80) • UDP port—Specify one of the following protocols: <ul style="list-style-type: none"> – domain—Specifies the Domain Name Service (53) – 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 <i>port1</i>	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 <i>port1</i> and <i>port2</i>) instructs the ACE to match all ports.
<i>port2</i>	

Command Modes

Class map configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

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

A single class map can have multiple **match port** commands. You can combine multiple **match port**, **match access-list**, **match source-address**, and **match destination-address** commands in a class map.

Examples

To specify that the class map is to match on TCP port number 23 (Telnet client), enter:

```
host1/Admin(config)# class-map L4_TCPPORT_CLASS
host1/Admin(config-cmap)# match port tcp eq 23
```

Related Commands

[\(config-cmap\) description](#)

(config-cmap) match source-address

To specify a client source host IP address and subnet mask from which the ACE accepts traffic as the network traffic matching criteria, use the **match source-address** command. You configure the associated policy map to permit or restrict management traffic to the ACE from the specified source network or host. Use the **no** form of the command to clear the source IP address and subnet mask match criteria from the class map.

```
[line_number] match source-address ip_address mask
```

```
no [line_number] match source-address ip_address mask
```

Syntax Description

<i>line_number</i>	(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 255 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
<i>ip_address</i>	Source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
<i>mask</i>	Subnet mask of the client entry in dotted-decimal notation (for example, 255.255.255.0).

Command Modes

Class map configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

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

A single class map can have multiple **match source-address** commands. You can combine multiple **match source-address**, **match access-list**, **match destination-address**, and **match port** commands in a class map.

An entry of 0.0.0.0 0.0.0.0 indicates a wildcard match for any source IP address and subnet mask.

Examples

To specify that the class map match on the source IP address 192.168.11.2 255.255.255.0, enter:

```
host1/Admin(config)# class-map http type 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 the command to remove the VIP match statement from the class map.

```
[line_number] match virtual-address vip_address {[netmask] protocol_number | any | {tcp | udp
{any | eq port_number | range port1 port2}}}
```

```
no [line_number] match virtual-address vip_address {[netmask] protocol_number | any | {tcp |
udp {any | eq port_number | range port1 port2}}}
```

Syntax Description	
<i>line_number</i>	(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 255 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
<i>vip_address</i>	VIP server IP address of the ACE, specified in dotted-decimal format (for example, 192.168.1.2).
<i>netmask</i>	(Optional) Subnet mask for the VIP address, specified in dotted-decimal format (for example, 255.255.255.0).
<i>protocol_number</i>	(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 <i>port_number</i>	<p>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:</p> <ul style="list-style-type: none"> • TCP port—Specify one of the following names or well-known port numbers: <ul style="list-style-type: none"> – 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) – smtp—Specifies the Simple Mail Transfer Protocol (25) – telnet—Specifies the Telnet protocol (23) – www—Specifies the World Wide Web (80) • UDP port—Specify one of the following protocols: <ul style="list-style-type: none"> – domain—Specifies the Domain Name Service (53) – 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 <i>port1 port2</i>	<p>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 <i>port1</i> and <i>port2</i>) instructs the ACE to match all ports.</p>

Command Modes

Class map configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

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

You can specify multiple **match virtual-address** commands within a class map.

The **match virtual-address** command cannot be combined with other types of **match** commands.

See the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide* for details about configuring the ACE to perform server load balancing.

Examples

To specify that the class map L4VIPCLASS matches traffic destined to VIP address 192.168.1.10 and TCP port number 80, enter:

```
host1/Admin(config)# class-map L4VIPCLASS
host1/Admin(config-cmap)# match virtual-address 192.168.1.10 tcp port eq 80
```

Related Commands

[\(config-cmap\) description](#)

Class Map FTP Inspection Configuration Mode Commands

Class map File Transfer Protocol (FTP) inspection configuration mode commands allow you to create and configure a Layer 7 class map to be used for the inspection of FTP request commands. To create this class map and access class map FTP inspection configuration mode, use the **class-map type ftp inspect** command. The prompt changes to (config-cmap-ftp-insp). Use the **no** form of the 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.
<i>map_name</i>	Name assigned to the Layer 7 FTP command request class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the inspect feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To create a Layer 7 class map named FTP_INSPECT_L7CLASS that performs FTP command inspection, enter:

```
host1/Admin(config)# class-map type ftp inspect match-any FTP_INSPECT_L7CLASS
host1/Admin(config-cmap-ftp-insp)#
```

Related Commands

(config) [policy-map](#)

(config-cmap-ftp-insp) description

To provide a brief summary about the Layer 7 File Transfer Protocol (FTP) command inspection class map, use the **description** command. Use the **no** form of the command to remove the description from the class map.

description *text*

no description *text*

Syntax Description

<i>text</i>	Description about the class map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.
-------------	---

Command Modes

Class map FTP inspection configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description that the class map is to perform FTP command inspection, enter:

```
host1/Admin(config-cmap-ftp-insp)# description FTP command inspection of incoming traffic
```

To remove a description from the FTP class map, enter:

```
host1/Admin(config-cmap-ftp-insp)# no description FTP command inspection of incoming traffic
```

Related Commands

This command has no related commands.

(config-cmap-ftp-insp) match request-method

To define File Transfer Protocol (FTP) command inspection decisions by the ACE, use the **match request-method** command. The match command identifies the FTP commands that you want filtered by the ACE. Use the **no** form of the 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

<i>line_number</i>	(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 1024 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
<i>ftp_command</i>	FTP command in the class map to be subjected to FTP inspection by the ACE. The possible FTP commands are as follows: <ul style="list-style-type: none"> • 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. • sysd—Get system information.

Command Modes

Class map FTP inspection configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You can specify multiple **match request-method** commands within a class map.

Examples

To specify FTP_INSPECT_L7CLASS as the name of a class map and identify that at least one FTP inspection command in the class map must be satisfied for the ACE to indicate a match, enter:

```
(config)# class-map type ftp inspect match-any FTP_INSPECT_L7CLASS
host1/Admin(config-cmap-ftp-insp)# match request-method cdup
host1/Admin(config-cmap-ftp-insp)# match request-method get
host1/Admin(config-cmap-ftp-insp)# match request-method stou
host1/Admin(config-cmap-ftp-insp)# match request-method put
```

Related Commands

[\(config-cmap-ftp-insp\) description](#)

Class Map 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 the 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:
		<ul style="list-style-type: none"> 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—Specifies that 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 only for match statements of the same Layer 7 HTTP deep packet inspection type. For example, the ACE does not allow you to specify a match-any condition for URL, HTTP header, and URL content statements in the same class map but does allow you to specify a match-any condition for multiple URLs, multiple HTTP headers, or multiple URL content statements with different names in the same class map.
	<i>map_name</i>	Name assigned to the Layer 7 HTTP deep packet inspection class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes	Configuration mode Admin and user contexts
---------------	---

Command History	Release	Modification
	A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the inspect feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To create a Layer 7 class map named HTTP_INSPECT_L7CLASS that performs HTTP deep packet inspection, enter:

```
(config)# class-map type http inspect match-any HTTP_INSPECT_L7CLASS  
host1/Admin(config-cmap-http-insp)#
```

Related Commands

[\(config\) policy-map](#)

(config-cmap-http-insp) description

To provide a brief summary about the Layer 7 HTTP inspection class map, use the **description** command. Use the **no** form of the command to remove the description from the class map.

description *text*

no description

Syntax Description	<i>text</i>	Description about the class map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.
---------------------------	-------------	---

Command Modes	Class map HTTP inspection configuration mode Admin and user contexts
----------------------	---

Command History	Release	Modification
	A1(7)	This command was introduced.

Usage Guidelines	This command has no usage guidelines.
-------------------------	---------------------------------------

Examples	To add a description that the class map is to perform HTTP deep packet inspection, enter: <pre>host1/Admin(config-cmap-http-insp)# description HTTP protocol deep inspection of incoming traffic</pre>
-----------------	--

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 the 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

<i>[line_number]</i>	(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 1024 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
<i>expression</i>	Content expression contained within the HTTP entity body. The range is from 1 to 255 alphanumeric characters. For a list of the supported characters that you can use in regular expressions, see Table 2-4 .
<i>offset number</i>	(Optional) Provides an absolute offset where the content expression search string starts. The offset starts at the first byte of the message body, after the empty line (CR, LF, CR, LF) between the headers and the body of the message. The offset value is from 1 to 4000 bytes.

Command Modes

Class map HTTP inspection configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To specify a content expression contained within the entity body sent with an HTTP request, enter:

```
(config)# class-map type http inspect match-any HTTP_INSPECT_L7CLASS
host1/Admin(config-cmap-http-insp)# match content .*newp2psig
```

Related Commands

[\(config-cmap-http-insp\) description](#)

(config-cmap-http-insp) match content length

To configure the class map to define application inspection decisions on HTTP traffic up to the configured maximum content parse length, use the **match content length** command. Messages that meet the specified criteria will be either allowed or denied based on the Layer 7 HTTP deep packet inspection policy map action. Use the **no** form of the command to clear the HTTP content length match criteria from the class map.

```
[line_number] match content length {eq bytes | gt bytes | lt bytes | range bytes1 bytes 2}
```

```
no [line_number] match content length {eq bytes | gt bytes | lt bytes | range bytes1 bytes 2}
```

Syntax Description	
[line_number]	(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 1024 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
eq bytes	Specifies a value for the content parse length in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with a content length size equal to the specified value. Valid entries are from 1 to 65535 bytes.
gt bytes	Specifies a minimum value for the content parse length in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with a content length size greater than the specified value. Valid entries are from 1 to 65535 bytes.
lt bytes	Specifies a maximum value for the content parse length in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with a content length size less than the specified value. Valid entries are from 1 to 65535 bytes.
range bytes1 bytes	Specifies a size range for the content parse length in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with a content length size within this range. The range is from 1 to 65535 bytes.

Command Modes	
	Class map HTTP inspection configuration mode Admin and user contexts

Command History	Release	Modification
	A1(7)	This command was introduced.

Usage Guidelines	
	This command has no usage guidelines.

Examples

To identify content parse length in an HTTP message that can be received by the ACE, enter:

```
(config)# class-map type http inspect match-any HTTP_INSPECT_L7CLASS  
host1/Admin(config-cmap-http-insp)# match content length eq 3495
```

Related Commands

[\(config-cmap-http-insp\) description](#)

(config-cmap-http-insp) match 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 the 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

<i>line_number</i>	(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 1024 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
<i>header_name</i>	Name of the HTTP header to match (for example, www.example1.com.) The range is from 1 to 64 alphanumeric characters. Note The <i>header_name</i> 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 <i>expression</i>	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 2-4 lists the supported characters that you can use in regular expressions.
---------------------------------------	--

Command Modes

Class map HTTP inspection configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The ACE supports the use of regular expressions for matching. Expressions are stored in a header map in the form *header-name: expression*. Header expressions allow spaces, provided that the spaces are escaped or quoted. [Table 2-4](#) lists the supported characters that you can use in regular expressions.

Table 2-4 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 <i>m</i> and <i>n</i> times; valid entries are from 1 to 255.
(expr{m})	Matches the previous item exactly <i>m</i> times; valid entries are from 1 to 255.
(expr{m,})	Matches the previous item <i>m</i> or more times; valid entries are from 1 to 255.
\a	Alert (ASCII 7).
\b	Backspace (ASCII 8).
\f	Form-feed (ASCII 12).
\n	New line (ASCII 10).
\r	Carriage return (ASCII 13).
\t	Tab (ASCII 9).
\v	Vertical tab (ASCII 11).
\0	Null (ASCII 0).
\\.\\	Backslash.

Examples

To 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

By default, the maximum header length for HTTP deep packet inspection is 2048 bytes. 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 the 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

<i>line_number</i>	(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 1024 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
request	Specifies the size of the HTTP header request message that can be received by the ACE.
response	Specifies the size of the HTTP header response message sent by the ACE.
eq bytes	Specifies a value for the entity body in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with an entity body size equal to the specified value. Valid entries are from 1 to 65535 bytes.
gt bytes	Specifies a minimum value for the entity body in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with an entity body size greater than the specified value. Valid entries are from 1 to 65535 bytes.
lt bytes	Specifies a maximum value for the entity body in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with an entity body size less than the specified value. Valid entries are from 1 to 65535 bytes.
range bytes1 bytes 2	Specifies a size range for the entity body in an HTTP message received by the ACE. Based on the policy map action, the ACE allows or denies messages with a entity body size within this range. The range is from 1 to 65535 bytes.

Command Modes

Class map HTTP inspection configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines This command has no usage guidelines.

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 [\(config-cmap-http-insp\) description](#)

(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, nontextual messages, multipart message bodies, and non-US-ASCII information in message headers. Use the **no** form of the 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	<p><i>[line_number]</i> (Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 1024 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.</p>
	<p><i>mime_type</i> The 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.</p> <p>The following lists the supported MIME types:</p> <ul style="list-style-type: none"> • 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-flt**
-

Command Modes

Class map HTTP inspection configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

To define MIME-type messages in addition to what is supported under the **match header mime-type** command, use the **match header** command (see the [\(config-cmap-http-insp\) 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

[\(config-cmap-http-insp\) description](#)

(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 the 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		
	<i>line_number</i>	(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 1024 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
	im	Defines the instant messaging application category. The ACE checks for the Yahoo Messenger instant messaging application.
	p2p	Defines the peer-to-peer application category. The applications checked include Kazaa and Gnutella.
	tunneling	Defines the tunneling application category. The applications checked include HTTPPort/HTTHost, GNU httptunnel, GoToMyPC, FireThru, and Http-Tunnel Client.

Command Modes Class map HTTP inspection configuration mode
Admin and user contexts

Command History	Release	Modification
	A1(7)	This command was introduced.

Usage Guidelines You can specify multiple **match port-misuse** commands within a class map. Each **match port-misuse** command configures a single application type.

The port misuse application inspection process requires a search of the entity body of the HTTP message, which may degrade performance of the ACE.

The ACE disables the **match port-misuse** command by default. If you do not configure a restricted HTTP application category, the default action by the ACE is to allow the applications without generating a log.

Examples To identify that peer-to-peer applications are restricted HTTP traffic, enter:

```
(config)# class-map type http inspect HTTP_INSPECT_L7CLASS
host1/Admin(config-cmap-http-insp)# match port-misuse p2p
```

Related Commands [\(config-cmap-http-insp\) description](#)

(config-cmap-http-insp) match request-method

By default, the ACE allows all request and extension methods. 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 the 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		
<i>line_number</i>	(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 1024 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.	
<i>ext method</i>	Specifies an HTTP extension method. If the RFC request messages do not contain one of the RFC 2616 HTTP request methods, the ACE verifies whether it is an extension method. The ACE supports the inspection of the following HTTP request extension methods: copy , edit , getattr , getattrname , getprops , index , lock , mkdir , move , revadd , relabel , revlog , revnum , save , setattr , startrev , stoprev , unedit , and unlock .	
<i>rfc method</i>	Specifies an RFC 2616 HTTP request method that you want to perform an RFC compliance check on. The ACE supports the inspection of the following RFC 2616 HTTP request methods: connect , delete , get , head , options , post , put , and trace .	

Command Modes
Class map HTTP inspection configuration mode
Admin and user contexts

Command History	Release	Modification
	A1(7)	This command was introduced.

Usage Guidelines

You can specify multiple **match request-method** commands within a class map. Each **match request-method** command configures a single request method.

For unsupported HTTP request methods, include the **inspect http strict** command as an action in the Layer 3 and Layer 4 policy map.

The ACE disables the **match request-method** command by default. If you do not configure a request method, the default action by the ACE is to allow the RFC 2616 HTTP request method without generating a log.

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 the 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

<i>line_number</i>	(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 1024 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
chunked	Transfers the message body as a series of chunks.
compressed	Defines the encoding format produced by the common UNIX file compression program “compress.” This format is an adaptive Lempel-Ziv-Welch coding (LZW).
deflate	Defines the .zlib format defined in RFC 1950 in combination with the deflate compression mechanism described in RFC 1951.
gzip	Defines the encoding format produced by the file compression program gzip (GNU zip) as described in RFC 1952. This format is a Lempel-Ziv coding (LZ77) with a 32-bit CRC.
identity	Defines the default (identity) encoding, which does not require the use of transformation.

Command Modes

Class map HTTP inspection configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

You can specify multiple **match transfer-encoding** commands within a class map. Each **match transfer-encoding** command configures a single application type.

The ACE disables the **match transfer-encoding** command by default. If you do not configure a transfer-encoding type, the default action by the ACE is to allow the HTTP transfer-encoding types without generating a log.

Examples

To specify a chunked HTTP transfer encoding type to limit the HTTP traffic that flows through the ACE, enter:

```
(config)# class-map type http inspect HTTP_INSPECT_L7CLASS
host1/Admin(config-cmap-http-insp)# match transfer-encoding chunked
```

Related Commands

[\(config-cmap-http-insp\) description](#)

(config-cmap-http-insp) match url

To configure the class map to define application inspection decisions based on the URL name and, optionally, the HTTP method, use the **match url** command. HTTP performs regular expression matching against the received packet data from a particular connection based on the URL expression. Use the **no** form of the command to clear a URL match criteria from the class map.

[line_number] match url expression

no [line_number] match url expression

Syntax Description

<i>line_number</i>	(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 1024 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
<i>expression</i>	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 for regular expressions, see Table 2-4 .

Command Modes

Class map HTTP inspection configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Include only the portion of the URL 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 2-4](#).

The period (.) does not have a literal meaning in regular expressions. Use either brackets ([]) or the backslash character (\) to match this character. 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 the 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

<i>line_number</i>	(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 1024 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
eq bytes	Specifies a value for the HTTP URL length received by the ACE. Based on the policy map action, the ACE allows or denies messages with an HTTP URL length equal to the specified value. Valid entries are from 1 to 65535 bytes.
gt bytes	Specifies a minimum value value for the HTTP URL length received by the ACE. Based on the policy map action, the ACE allows or denies messages with an HTTP URL length greater than the specified value. Valid entries are from 1 to 65535 bytes.

lt <i>bytes</i>	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 <i>bytes1 bytes</i>	Specifies a size range for the HTTP URL length received by the ACE. Based on the policy map action, the ACE allows or denies messages with an HTTP URL length within this range. The range is from 1 to 65535 bytes.

Command Modes

Class map HTTP inspection configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To specify that the class map is to match on a URL with a length equal to 10000 bytes in the request message, enter:

```
(config)# class-map type http inspect HTTP_INSPECT_L7CLASS
host1/Admin(config-cmap-http-insp)# match url length eq 10000
```

Related Commands

[\(config-cmap-http-insp\) description](#)

Class Map HTTP Load Balancing Configuration Mode Commands

Class map HTTP load balancing configuration mode commands allow you to create a Layer 7 HTTP server load balancing (SLB) class map. To create this class map and access class map HTTP load balancing configuration mode, use the **class-map type http loadbalance** command. The prompt changes to (config-cmap-http-lb). Use the **no** form of the 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:
		<ul style="list-style-type: none"> • 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.
	<i>map_name</i>	Name assigned to the Layer 7 HTTP SLB class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the loadbalance feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To create a Layer 7 class map named L7SLB_CLASS that performs server load balancing, enter:

```
host1/Admin(config)# class-map type http loadbalance match-any L7SLB_CLASS  
host1/Admin(config-cmap-http-lb)#
```

Related Commands

[\(config\) policy-map](#)

(config-cmap-http-lb) description

To provide a brief summary about the Layer 7 HTTP SLB class map, use the **description** command. Use the **no** form of the command to remove the description from the class map.

description *text*

no description

Syntax Description	<i>text</i>	Description about the class map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.
---------------------------	-------------	---

Command Modes	Class map HTTP load balancing configuration mode Admin and user contexts
----------------------	---

Command History	Release	Modification
	A1(7)	This command was introduced.

Usage Guidelines	This command has no usage guidelines.
-------------------------	---------------------------------------

Examples	To add a description that the class map is to perform server load balancing, enter: host1/Admin(config-cmap-http-lb)# description HTTP LOAD BALANCE PROTOCOL 1
-----------------	--

Related Commands	This command has no keywords or arguments.
-------------------------	--

(config-cmap-http-lb) match class-map

To identify one Layer 7 HTTP SLB class map that is to be used as a matching criterion for another Layer 7 class map, use the **match class-map** command. The nesting of class maps allows you to achieve complex logical expressions for Layer 7 HTTP-based SLB. Use the **no** form of the command to remove the nested class map from the class7 class map.

```
[line_number] match class-map name
```

```
no [line_number] match class-map name
```

Syntax Description	
<i>line_number</i>	(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 1024 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
<i>name</i>	Name of an existing Layer 7 load-balancing class map.

Command Modes	Class map HTTP load balancing configuration mode Admin and user contexts
---------------	---

Command History	Release	Modification
	A1(7)	This command was introduced.

Usage Guidelines	<p>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.</p> <p>See the <i>Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide</i> for details about configuring the ACE to perform server load balancing.</p>
------------------	---

Examples	<p>These examples show how to combine the characteristics of two class maps, one with match-any and one with match-all characteristics, into a single class map by using the match class-map command.</p>
----------	--

```
(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 http cookie

To configure the class map to make Layer 7 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 the 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

<i>line_number</i>	(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 1024 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
<i>name</i>	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 2-4 .

Command Modes

Class map HTTP load balancing configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To specify that the Layer 7 class map load balances on a cookie with the name of testcookie1 or testcookie2, enter:

```
(config)# class-map type http loadbalance match-any L7SLBCLASS
(config-cmap-http-lb)# 100 match http cookie testcookie1 cookie-value 123456
(config-cmap-http-lb)# 200 match http cookie testcookie2 cookie-value 789987
```

Related Commands

[\(config-cmap-http-lb\) description](#)

(config-cmap-http-lb) match http header

To configure a class map to make Layer 7 SLB decisions based on the name and value of an HTTP header, use the **match http header** command. The ACE performs regular expression matching against the received packet data from a particular connection based on the HTTP header expression. You can configure a maximum of five HTTP header names per VIP. Use the **no** form of the command to remove all HTTP header match criteria from the class map.

```
[line_number] match http header {header_name | header_field} header-value expression
```

```
no [line_number] match http header {header_name | header_field} header-value expression
```

Syntax Description

<i>line_number</i>	(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 1024 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
<i>header_name</i>	Name of the HTTP header to match (for example, www.example1.com.) The range is from 1 to 64 alphanumeric characters. Note The <i>header_name</i> argument cannot include the colon in the name of the HTTP header; the ACE rejects the colon as an invalid token.
<i>header_field</i>	Standard HTTP/1.1 header field. Valid selections include request-header fields, general-header fields, and entity-header field. The supported selections are as follows: <ul style="list-style-type: none"> • Accept—Semicolon-separated list of representation schemes (content type meta-information values) that will be accepted in the response to the request. • Accept-Charset—Character sets that are acceptable for the response. This field allows clients capable of understanding more comprehensive or special-purpose character sets to signal that capability to a server that can represent documents in those character sets. • Accept-Encoding—Restricts the content encoding that a user will accept from the server. • Accept-Language—ISO code for the language in which the document is written. The language code is an ISO 3316 language code with an optional ISO639 country code to specify a national variant. • Authorization—Specifies that the user agent wants to authenticate itself with a server, usually after receiving a 401 response.

- **Cache-Control**—Directives that must be obeyed by all caching mechanisms along the request/response chain. The directives specify behavior intended to prevent caches from adversely interfering with the request or response.
- **Connection**—Allows the sender to specify connection options.
- **Content-MD5**—MD5 digest of the entity body that provides an end-to-end integrity check. Only a client or an origin server can generate this header field.
- **Expect**—Used by a client to inform the server about the behaviors that the client requires.
- **From**—Contains the e-mail address of the person that controls the requesting user agent.
- **Host**—Internet host and port number of the resource being requested, as obtained from the original URI given by the user or referring resource. The Host field value must represent the naming authority of the origin server or gateway given by the original URL.
- **If-Match**—Used with a method to make it conditional. A client that has one or more entities previously obtained from the resource can verify that one of those entities is current by including a list of their associated entity tags in the If-Match header field. This feature allows efficient updates of cached information with a minimum amount of transaction overhead. It is also used on updating requests to prevent inadvertent modification of the wrong version of a resource. As a special case, the value “*” matches any current entity of the resource.
- **Pragma**—Pragma directives that are understood by servers to whom the directives are relevant. The syntax is the same as for other multiple-value fields in HTTP. For example, the accept field is a comma-separated list of entries for which the optional parameters are separated by semicolons.
- **Referer**—Address (URI) of the resource from which the URI in the request was obtained.
- **Transfer-Encoding**—Indicates what (if any) type of transformation has been applied to the message body in order to safely transfer it between the sender and the recipient.
- **User-Agent**—Information about the user agent (for example, a software program that originates the request). This information is for statistical purposes, the tracing of protocol violations, and automated recognition of user agents.
- **Via**—Used by gateways and proxies to indicate the intermediate protocols and recipients between the user agent and the server on requests and between the origin server and the client on responses.

header-value *expression*

Specifies the header value expression string to compare against the value in the specified field in the HTTP header. The range is from 1 to 255 alphanumeric characters. For a list of the supported characters that you can use for regular expressions, see [Table 2-4](#).

Command Modes Class map HTTP load balancing configuration mode
Admin and user contexts

Command History	Release	Modification
	A1(7)	This command was introduced.

Usage Guidelines The ACE supports the use of regular expressions for matching. Expressions are stored in a header map in the form *header-name: expression*. Header expressions allow spaces, provided that the spaces are escaped or quoted. For a list of the supported characters that you can use for regular expressions, see [Table 2-4](#).

Examples To specify that the Layer 7 class map performs SLB on an HTTP header named Host, enter:

```
(config)# class-map type http loadbalance 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)# 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 the 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

<i>line_number</i>	(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 1024 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
<i>expression</i>	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 <i>www.hostname.domain</i> in the match statement. For a list of the supported characters that you can use for regular expressions, see Table 2-4 .
method name	(Optional) Specifies the HTTP method to match. Enter a method name as an unquoted text string with no spaces and a maximum of 15 alphanumeric characters. The method can either be one of the standard HTTP 1.1 method names (OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, or CONNECT) or a text string that must be matched exactly (for example, CORVETTE).

Command Modes

Class map HTTP load balancing configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

Include only the portion of the URL that follows *www.hostname.domain* in the match statement. For example, in the URL *www.anydomain.com/latest/whatsnew.html*, include only */latest/whatsnew.html*. To match the *www.anydomain.com* portion, the URL string can take the form of a URL regular expression. The ACE supports the use of regular expressions for matching URL strings. For a list of the supported characters that you can use for regular expressions, see [Table 2-4](#).

The period (.) does not have a literal meaning in regular expressions. Use either brackets ([]) or the backslash character (\) to match this character. For example, specify *www[.]xyz[.]com* instead of *www.xyz.com*.

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 the 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

<i>line_number</i>	(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 1024 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
<i>ip_address</i>	Source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.2).
<i>netmask</i>	(Optional) Subnet mask of the IP address. Enter the netmask in dotted-decimal notation (for example, 255.255.255.0). The default is 255.255.255.255.

Command Modes

Class map HTTP load balancing configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To specify that the class map match on source IP address 192.168.11.2 255.255.255.0, enter:

```
host1/Admin(config)# class-map http type 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. <ul style="list-style-type: none"> 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).
<i>map_name</i>	Name assigned to the Layer 3 and Layer 4 network management protocol class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Command Modes

Configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

The commands in this mode require the context Admin user role. For details about role-based access control (RBAC) and user roles, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Examples

To create a Layer 3 and Layer 4 class map named MGMT-ACCESS_CLASS that classifies the network management protocols that can be received by the ACE, enter:

```
host1/Admin# class-map type management match-any MGMT-ACCESS_CLASS
host1/Admin(config-cmap-mgmt)#
```

Related Commands

This command has no related commands.

(config-cmap-mgmt) description

To provide a brief summary about the Layer 3 and Layer 4 management class map, use the **description** command. Use the **no** form of the command to remove the description from the class map.

description *text*

no description

Syntax Description

<i>text</i>	Description about the class map. Enter an unquoted text string with a maximum of 240 alphanumeric characters.
-------------	---

Command Modes

Class map management configuration mode
Admin and user contexts

Command History

Release	Modification
A1(7)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

To add a description that the class map is to allow remote Telnet access, enter:

```
host1/Admin# class-map type management TELNET-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# description Allow Telnet access to the ACE
```

Related Commands

This command has no related commands.

(config-cmap-mgmt) match protocol

To configure the class map to identify the network management protocols that can be received by the ACE, use the **match protocol** command. You configure the associated policy map to permit access to the ACE for the specified management protocol(s). 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 the command to deselect the specified network management protocol match criteria from the class map.

```
[line_number] match protocol {http | https | icmp | snmp | ssh | telnet | xml-https} {any |
source-address ip_address mask}
```

```
no [line_number] match protocol {http | https | icmp | snmp | ssh | telnet | xml-https} {any |
source-address ip_address mask}
```

Syntax Description	
<i>line_number</i>	(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 255 as the line number. You can enter no line_number to delete long match commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
http	Specifies the Hypertext Transfer Protocol (HTTP).
https	Specifies secure (SSL) Hypertext Transfer Protocol (HTTP) for connectivity with the Device Manager GUI on the ACE.
icmp	Specifies the Internet Control Message Protocol (ping).
snmp	Specifies the Simple Network Management Protocol (SNMP).
ssh	Specifies a Secure Shell (SSH) connection to the ACE.
telnet	Specifies a Telnet connection to the ACE.
xml-https	Specifies HTTPS as transfer protocol to send and receive XML documents between the ACE and a Network Management System (NMS).
any	Specifies any client source address for the management traffic classification.
source-address	Specifies a client source host IP address and subnet mask as the network traffic matching criteria. As part of the classification, the ACE implicitly obtains the destination IP address from the interface on which you apply the policy map.
<i>ip_address</i>	Source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
<i>mask</i>	Subnet mask of the client entry in dotted-decimal notation (for example, 255.255.255.0).

Command Modes Class map management configuration mode
Admin and user contexts

Command History	Release	Modification
	A1(7)	This command was introduced.

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](#)