

Class-Map Configuration Mode Commands

Class-Map is used to configure a packet classifier for the flow-based Traffic Policing feature within destination context. It filters egress and/or ingress packets of a subscriber session based on rules configured in a subscriber context.

Command Modes

Exec > Global Configuration > Context Configuration > Class-Map Configuration

configure > context *context_name* **> class-map** *class_map_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-class-map)#
```

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

- end, on page 1
- exit, on page 2
- match any, on page 2
- match dst-ip-address, on page 3
- match dst-port-range, on page 3
- match ip-tos, on page 4
- match ipsec-spi, on page 5
- match packet-size, on page 6
- match protocol, on page 7
- match src-ip-address, on page 8
- match src-port-range, on page 9

end

Exits the current configuration mode and returns to the Exec mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **`end`**

Usage Guidelines Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **`exit`**

Usage Guidelines Use this command to return to the parent configuration mode.

match any

Allows all traffic types in this class map.

Product PDSN
HA
ASN-GW
HSGW
P-GW
SAEGW
SCM

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Class-Map Configuration

configure > context *context_name* **> class-map** *class_map_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-class-map)#`

Syntax Description **match any**

Usage Guidelines Sets the match rule to allow all traffic flow for specific class map.

Example

The following command allows all packets going to a system with this class map.

`match any`

match dst-ip-address

Specifies a traffic classification rule based on the destination IP address of packets.

Product

PDSN

HA

ASN-GW

HSGW

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Class-Map Configuration

configure > context *context_name* **> class-map** *class_map_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-class-map)#`

Syntax Description

match dst-ip-address *dst_ip_address* **/***subnet_mask*

dst_ip_address/subnet_mask

Specifies the destination IP address of the packets.

dst_ip_address must be entered in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

subnet_mask is an option that is entered in CIDR notation.

Usage Guidelines

Sets the match rule based on the destination IP address of packets for specific Class Map.

Example

The following command specifies the rule for packets going to a system having an IP address *10.1.2.6*.

```
match dst-ip-address 10.1.2.6
```

match dst-port-range

Specifies a traffic classification rule based on the range of destination ports for L4 packets.

Product

PDSN

HA

ASN-GW

HSGW

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Class-Map Configuration

configure > **context** *context_name* > **class-map** *class_map_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-class-map)#
```

Syntax Description

match dst-port-range *initial_port_number* **[to** *last_port_number* **]**

initial_port_number **[to** ***last_port_number*** **]**

Specifies the destination port or range of ports of L4 packets.

initial_port_number is the starting port number and must be an integer 1 to 65535 but less than *last_port_number*, if specified.

last_port_number is the end port number and must be an integer from 1 to 65535 but more than *initial_port_number*.

Usage Guidelines

Sets the match rule based on the destination port number or range of ports of L4 packets for specific Class Map.

Example

The following command specifies the rule for packets having destination port number from *23* to *88*.

```
match dst-port-range 23 to 88
```

match ip-tos

Specifies a traffic classification rule based on the IP Type of Service value in ToS field of packet.

Product

PDSN

HA

ASN-GW

HSGW

P-GW

SAEGW

SCM

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Class-Map Configuration

configure > context *context_name* **> class-map** *class_map_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-class-map)#
```

Syntax Description

match ip-tos { *service_value* **[ip-tos-mask** *mask_value* **] | tos-range** *low_value* **to** *high_value* **}**

service_value

Specifies the IP Type-of-Service value to match inside the ToS field of packets as an integer from 0 to 255.

ip-tos-mask ***mask_value***

Specifies the IP Type-of-Service mask value to match inside the ToS field of packets as an integer from 1 to 255.

tos-range ***low_value*** **to** ***high_value***

Specifies a range that a ToS value in a received packet must fall within to be considered a match. *low_value* and *high_value* must be an integer from 0 to 255.

Usage Guidelines

Sets the match rule based on the IP ToS value in ToS field of packets for specific Class Map.

Example

The following commands specifies the IP ToS value of *3* is the value to match in a ToS field in received packets.

```
match ip-tos 3
```

match ipsec-spi

Specifies a traffic classification rule based on the IPSec Security Parameter Index (SPI) value in the SPI field of packet.

Product

PDSN

HA

ASN-GW

HSGW

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Class-Map Configuration

configure > context *context_name* **> class-map** *class_map_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-class-map)#`

Syntax Description

match ipsec-spi *index_value*

index_value

Specifies the IPSec SPI value to match inside the SPI field of packets as an integer from 1 to 65535.

Usage Guidelines

Sets the match rule based on the IPSec SPI value in SPI field of packets for specific Class Map.

Example

The following command specifies the IPSec SPI value as *1234* for the SPI field in packets.

```
match ipsec-spi 1234
```

match packet-size

Specifies a traffic classification rule based on the size of packet.

Product

PDSN

HA

ASN-GW

HSGW

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Class-Map Configuration

configure > context *context_name* **> class-map** *class_map_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-class-map)#`

Syntax Description

match packet-size [gt | lt] *size*

[gt | lt] ***size***

Specifies the packet length in bytes.

gt: indicates a packet size greater than the specified size.

lt: indicates a packet size less than the specified size.

size must be an integer from 1 to 65535.

Usage Guidelines Sets the match rule based on the size of packets for specific Class Map. This command is only applicable for static policies; it is not available for dynamic policies.

Example

The following command specifies the packet length to be *1024* bytes.

```
match packet-size 1024
```

match protocol

Specifies a traffic classification rule based on the protocol used for session flow.

Product

PDSN

HA

ASN-GW

HSGW

P-GW

SAEGW

SCM

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Class-Map Configuration

configure > **context** *context_name* > **class-map** *class_map_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-class-map)#
```

Syntax Description **match protocol { gre | ip-in-ip | number | rtp | sip | tcp | udp }**

gre

Sets the match rule for session flow using Generic Routing Encapsulation (GRE) Protocol. It matches the protocol field to GRE inside the packet.

ip-in-ip

Sets the match rule for session flow using IP-in-IP encapsulation protocol. It matches the protocol field to ip-in-ip inside the packet.

number

Sets the match rule for a session flow using Transmission Control Protocol (TCP). It matches the specified protocol field inside the packet.

rtp

Sets the match rule for a session flow using Real Time Protocol (RTP). It matches the specified protocol field inside the packet.

sip

Sets the match rule for a session flow using Session Initiation Protocol (SIP). It matches the specified protocol field inside the packet.

tcp

Sets the match rule for a session flow using Transmission Control Protocol (TCP). It matches the protocol field to TCP inside the packet.

udp

Sets the match rule for a session flow having User Datagram Protocol (UDP). It matches the protocol field to UDP inside the packet.

Usage Guidelines

Sets the match rule based on the protocol of packet flow for a specific Class Map.

Example

The following command specifies the rule for packet flow using IP-in-IP protocol.

```
match protocol ip-in-ip
```

match src-ip-address

Specifies a traffic classification rule based on the source IP address of packets.

Product

PDSN

HA

ASN-GW

HSGW

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Class-Map Configuration

configure > **context** *context_name* > **class-map** *class_map_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-class-map)#`

Syntax Description

match src-ip-address *src_ip_address* **/***subnet_mask*

src_ip_address/subnet_mask

Specifies the destination IP address of the packets.

src_ip_address must be entered in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

subnet_mask is an option that is entered in CIDR notation.

Usage Guidelines

Sets the match rule based on the source IP address of packets for specific Class Map.

Example

The following command specifies the rule for packets coming from a system having an IP address *10.1.2.3*.

```
match src-ip-address 10.1.2.3
```

match src-port-range

Specifies a traffic classification rule based on the range of source ports of L4 packets.

Product

PDSN

HA

ASN-GW

HSGW

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Class-Map Configuration

configure > **context** *context_name* > **class-map** *class_map_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-class-map)#`

Syntax Description

match src-port-range *initial_port_number* **[to** *last_port_number* **]**

initial_port_number **[to** ***last_port_number*** **]**

Specifies the source port or range of ports of the L4 packets.

initial_port_number is the starting port number and must be an integer from 1 to 65535 but less than *last_port_number*, if specified.

last_port_number is the end port number and must be an integer from 1 to 65535 but more than *initial_port_number*.

Usage Guidelines

Sets the match rule based on source port number or range of ports of L4 packets for specific Class Map.

Example

The following command specifies the rule for packets having source port number from *23* to *88*.

```
match src-port-range 23 to 88
```