Sun Ethernet Fabric Operating System CLI Reference Manual, Vol. 8

Part No: E60932-02

August 2015

.

Contents

Using This Documentation

- **Overview** – Provides information on Oracle's SEFOS CLI commands
- **Audience** – Users and system administrators who configure SEFOS through the CLI
- **Required knowledge** – Basic knowledge of UNIX CLI command syntax

Product Documentation Library

Documentation and resources for this product and related products are available at http://www.oracle.com/goto/es2-72_es2-64/docs.

Acronyms

Refer to the *Sun Ethernet Fabric Operating System CLI Reference Manual, Vol. 1* for acronyms and abbreviations.

CLI Command Modes

Refer to the *Sun Ethernet Fabric Operating System CLI Reference Manual, Vol. 1* for CLI command modes.

Feedback

Provide feedback about this documentation at http://www.oracle.com/goto/docfeedback.

CHAPTER 47

ACL

ACLs on the system perform both access control and Layer 3 field classification.

47.1 aclcmd

CLI commands in this Fulcrum sub-category are listed below:

47.1.1 ip access-list

Command Objective	This command creates IP access-list and enters the IP access-list configuration mode. ACLs on the system perform both access control and Layer 3 field classification. To define Layer 3 fields' access-lists the `ip access-list` command is used. The no form of the command deletes the IP access-list.
Syntax	**`ip access-list {standard <access-list-number (1-10)> | extended <access-list-number (11-1024)> }`** **`no ip access-list {standard <access-list-number (1-10> | extended <access-list-number (11-1024)> }`**
Parameter Description	• **`standard <access-list-number (1-10)>`** - Configures the standard access-list number. Standard access-lists create filters based on IP address and network mask (L3 filters). This value ranges from 1 to 10. • **`extended <access-list-number (11-1024)>`** - Configures the extended access-list number. Extended access-lists enable specification of filters based on the type of protocol, range of TCP or UDP ports, as well as the IP address and network mask (L4 filters). This value ranges between 11 and 1024.
Mode	Global Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**`SEFOS (config)# ip access-list standard 1`** **`SEFOS (config-std-nacl)#`**
Related Command(s)	• **`permit -`** Specifies the packets to be forwarded depending upon the associated parameters. • **`deny -`** Denies traffic if the conditions defined in the deny statement are matched. • **`Permit`** – Permits the packets to be forwarded depending upon the associated parameters. • **`Deny`** - Denies the packets to be forwarded depending upon the associated parameters. • **`permit- ip/ospf/pim/protocol type -`** Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched.

- **permit ipv6** - Specifies IP packets to be forwarded based on protocol and associated parameters.
- **deny - ip/ospf/pim/protocol type**- Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched.
- **deny ipv6** - Specifies IPv6 packets to be rejected based on protocol and associated parameters.
- **permit tcp -** Specifies the TCP packets to be forwarded based on the associated parameters.
- **deny tcp -** Specifies the TCP packets to be rejected based on the associated parameters.
- **permit udp -** Specifies the UDP packets to be forwarded based on the associated parameters.
- **deny udp -** Specifies the UDP packets to be rejected based on the associated parameters.
- **permit icmp -** Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters
- **deny icmp -** Specifies the ICMP packets to be rejected based on the IP address and associated parameters.
- **ip access-group -** Enables access control for the packets on the interface.
- **show access-lists -** Displays the access-list configuration.

47.1.2 mac access-list extended

Command Objective	This command creates a MAC access-list and enters the MAC access-list configuration mode. This value ranges from 1 to 1024. The no form of the command deletes the MAC access-list.
Syntax	**mac access-list extended <access-list-number (1-1024)>** **no mac access-list extended <short (1-1024)>**
Mode	Global Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS (config)# mac access-list extended 5** **SEFOS (config-ext-macl)**
Related Command(s)	• **mac access-group –** Applies a MAC access control list (ACL) to a Layer 2 interface. • **permit – MAC** - Specifies the packets to be forwarded based on the MAC address and the associated parameters. • **deny – MAC** - Specifies the packets to be rejected based on the MAC address and the associated parameters. • **show access-lists –** Displays the access lists' configuration.

47.1.3 ipv6 access-list extended

Command Objective	This command creates IPv6 access-list and enters the IPv6 access-list configuration mode. This value ranges from 11 to 1024 The no form of the command deletes the IPv6 access-list.
Syntax	**ipv6 access-list extended <access-list-number (11-1024)>** **no ipv6 access-list extended <access-list-number (11-1024)>**
Mode	Global Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS (config)# ipv6 access-list extended 15** **SEFOS (config-ipv6-acl)#**

47.1.4 permit

Command Objective	This command permits the packets to be forwarded depending upon the associated parameters. Standard IP access lists use source addresses for matching operations.
Syntax	**permit { any | host <src-ip-address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-ip-address> <mask> }**
Parameter Description	• **any|host <src-ip-address>| < src-ip-address> <mask>** - Permits traffic with the specified source address. The sources are: ▪ **any –** Permits packets from any source. ▪ **host <src-ip-address>** - Permits packets with the specified host source IPv4 address. ▪ **< src-ip-address > <mask>** - Permits packets with the specified source IP address and the network mask to be used with the source IP address. • **any|host <dest-ip-address>| < dest-ip-address > <mask>** - Permits traffic with the specified destination address. The destination can be: ▪ **any –** Permits the packets with any destination. ▪ **host <dest-ip-address>** - Permits packets with the specified host destination IPv4 address. ▪ **< dest-ip-address > <mask>** - Permits packets with the specified destination IP address and the network mask for the given source IP address.
Mode	IP ACL Configuration (standard)
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS(config-std-nacl)# permit host 100.0.0.10 host 10.0.0.1**
Related Command(s)	• **ip access-list –** Creates IP access list and enters the IP access list configuration mode. • **show access-lists –** Displays the access list configuration.

47.1.5 deny

Command Objective	This command denies and discards packets depending upon the associated parameters. Standard IP access lists use source addresses for matching operations.
Syntax	**deny{ any | host <src-ip-address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-ip-address> <mask> }**
Parameter Description	• **any|host <src-ip-address>| < src-ip-address ><mask>** - Denies traffic with the specified source address. The sources are: ▪ **any –** Denies packets from any source. ▪ **host <src-ip-address>** - Denies packets with the specified host source IPv4 address. ▪ **< src-ip-address> <mask>** - Denies packets with the specified source IP addressand the network mask to be used with the source IP address. • **any|host <dest-ip-address>| < dest-ip-address > <mask>** - Denies traffic with the specified destination address. The destination can be: ▪ **any –** Denies the packets with any destination. ▪ **host <dest-ip-address>** - Denies packets with the specified host destination IPv4 address. ▪ **< dest-ip-address> <mask>** - Denies packets with the specified destination IP address and the network mask for the given destination IP address.
Mode	IP ACL Configuration (standard)
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS(config-std-nacl)# deny host 100.0.0.10 any**
Related Command(s)	• **ip access-list –** Creates IP access list and enters the IP access list configuration mode. • **show access-lists –** Displays the access list configuration.

47.1.6 permit- ip/ospf/pim/protocol type

Command Objective	This command permits data packets for a particular protocol packet if the conditions defined in the permit statement are matched.
Syntax	**permit { ip | ospf | pim | <protocol-type (1-255)>}{ any | host <src-ip-address> | <src-ip-address> <mask> }{ any | host <dest-ip-address> | <dest-ip-address> <mask> }[{tos{max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp {<value (0-63)> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef}}][priority <value (1-7)>] [{precedence (0-7)> | fragments | log | log-input | reflect <access list> | time-range <value>}]**
Parameter Description	• **ip** - Allows IP protocol packets. • **ospf** - Allows OSPF protocol packets. • **pim** - Allows PIM protocol packets. • **<protocol-type (1-255)>** - Configures the type of protocol to be checked against the packet. It can also be a protocol number. Note: Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed. • **any|host <src-ip-address>| < src-ip-address> <mask>** - Permits traffic with the specified source address. The sources are: ▪ **any –** Permits packets from any source. ▪ **host <src-ip-address>** - Permits packets with the specified host source IPv4 address. ▪ **<src-ip-address> <mask>** - Permits packets with the specified source IP address and the network mask to be used with the source IP address. • **any|host <dest-ip-address>| < dest-ip-address > <mask>** - Permits traffic with the specified destination address. The destination can be: ▪ **any –** Permits the packets with any destination. ▪ **host <dest-ip-address>** - Permits packets with the specified host destination IPv4 address. ▪ **<dest-ip-address> <mask>** - Permits packets with the specified destination IP address and the network mask for the given destination IP address.

- **tos** - Allows the protocol packets based on the following types of service configurations. The options are,
  - **max-reliability** - Allows the protocol packets having TOS field set as high reliability.
  - **max-throughput** - Allows the protocol packets having TOS field set as high throughput.
  - **min-delay –** Allows the protocol packets having TOS field set as low delay.
  - **normal** - Allows all protocol packets. Does not check for the TOS field in the packets.
  - **<value (0-7)>** - Allows the protocol packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS.
    - **0** - Allows all protocol packets. Does not check for the TOS field in the packets.
    - **1** - Allows the protocol packets having TOS field set as high reliability.
    - **2** - Allows the protocol packets having TOS field set as high throughput.
    - **3** - Allows the protocol packets having TOS field set either as high reliability or high throughput.
    - **4** - Allows the protocol packets having TOS field set as low delay.
    - **5** - Allows the protocol packets having TOS field set either as low delay or high reliability.
    - **6** - Allows the protocol packets having TOS field set either as low delay or high throughput.
    - **7** - Allows the protocol packets having TOS field set either as low delay, high reliability, or high throughput.

- **dscp** – Configures the Differentiated Services Code Point (DSCP) which provides the quality of service control. The various options available are:
  - **<value (0-63)>** – Configures the Differentiated Services Code Point value. This value ranges from 0 to 63.
  - **af11** - Matches packets with AF11 DSCP (001010).
  - **af12** - Matches packets with AF12 DSCP (001100).
  - **af13** - Matches packets with AF13 DSCP (001110).
  - **af21** - Matches packets with AF21 DSCP (010010).
  - **af22** - Matches packets with AF22 DSCP (010100).
  - **af23** - Matches packets with AF23 DSCP (010110).
  - **af31** - Matches packets with AF31 DSCP (011010).
  - **af32** - Matches packets with AF32 DSCP (011100).
  - **af33** - Matches packets with AF33 DSCP (011110).
  - **af41** - Matches packets with AF41 DSCP (100010).
  - **af42** - Matches packets with AF42 DSCP (100100).

- **af43** - Matches packets with AF43 DSCP (100110).
- **cs1** - Matches packets with CS1 (precedence 1) DSCP (001000).
- **cs2** - Matches packets with CS2 (precedence 2) DSCP (010000).
- **cs3** - Matches packets with CS3 (precedence 3) DSCP (011000).
- **cs4** - Matches packets with CS4 (precedence 4) DSCP (100000).
- **cs5** - Matches packets with CS5 (precedence 5) DSCP (101000).
- **cs6** - Matches packets with CS6 (precedence 6) DSCP (110000).
- **cs7** - Matches packets with CS7 (precedence 7) DSCP (111000).
- **default** - Default DSCP (000000).
- **ef** - Matches packets with EF DSCP (101110).

- **priority <(1-7)>** – Configures the priority value of the L3 filter to be used when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 7.

- **<precedence (0-7)> –** Precedence level to be used for filtering packets. This parameter is newly added in the existing command for industry standard CLI. The values are:
  - **0** - Matches packets with routine precedence.
  - **1** - Matches packets with priority precedence.
  - **2** - Matches packets with immediate precedence.
  - **3** - Matches packets with flash precedence.
  - **4** - Matches packets with flash override precedence.
  - **5** - Matches packets with critical precedence.
  - **6** - Matches packets with internetwork control precedence.
  - **7** - Matches packets with network control precedence.

- **fragments** - Considers fragments in the access list entry and examines non-initial fragments of IPv4 packets, when applying the access list entry.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **log** - Creates informational logging message about the packets that match the entry to be sent to the console. This message includes the access list number, whether the packet is permitted or denied, the protocol, whether the protocol is TCP (Transport Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol) or a number, and, if appropriate, the source and destination addresses and source and destination port numbers. This message is generated for the first packet that matches a flow. This message is then generated at five minute intervals with the number of packets permitted or denied in the prior five minute interval.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **log-input** - Creates information logging message along with the information about the input interface.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **reflect <access-list>** – Reflects the name of the reflexive access list.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **time-range <value>** - Applies the time range. Time range defines the time when the permit or deny statements of the access control list are in effect.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode

ACL Extended Access List Configuration Mode

Package

Workgroup, Enterprise, Metro_E, and Metro

Defaults

- protocol-type - 255
- priority - 1
- dscp - -1

Note: Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed.

Example

```
SEFOS (config-ext-nacl)# permit 255 12.0.0.1 255.0 any
dscp af11
```

Related Command(s)

- **ip access-list –** Creates IP ACLs and enters the IP access list configuration mode.
- **deny – ip/ospf/pim/protocol type –** Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched.
- **show access-lists –** Displays the access list configuration.

47.1.7 deny - ip/ospf/pim/protocol type

Command Objective	This command denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched.
Syntax	**deny { ip | ospf | pim | <protocol-type (1-255)>}{ any | host <src-ip-address> | <src-ip-address> <mask> }{ any | host <dest-ip-address> | <dest-ip-address> <mask> }[{tos{max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp {<value (0-63)> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef}}][priority <value (1-7)>] [{precedence (0-7)> | fragments | log | log-input | reflect <access list> | time-range <value>}]**
Parameter Description	• **ip** - Denies P protocol packets. • **ospf** - Denies OSPF protocol packets. • **pim** - Denies PIM protocol packets. • **<protocol-type (1-255)>** - Denies the packets for the specified protocol number. This value ranges from 1 to 255. Note: Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed. • **any|host <src-ip-address>| < src-ip-address> <mask>** - Denies traffic with the specified source address. The sources are: ▪ **any –** Denies packets from any source. ▪ **host <src-ip-address>** - Denies packets with the specified host source IPv4 address. ▪ **<src-ip-address> <mask>** - Denies packets with the specified source IP address and the network mask to be used with the source IP address. • **any|host <dest-ip-address>| < dest-ip-address > <mask>** - Denies traffic with the specified destination address. The destination can be: ▪ **any –** Denies the packets with any destination. ▪ **host <dest-ip-address>** - Denies packets with the specified host destination IPv4 address. ▪ **<dest-ip-address> <mask>** - Denies packets with the specified destination IP address and the network mask for the given destination IP address.

- **tos** - Denies the protocol packets based on the following type of service configuration. The options are,
  - **max-reliability** - Denies the protocol packets having TOS field set as high reliability.
  - **max-throughput** - Denies the protocol packets having TOS field set as high throughput.
  - **min-delay –** Denies the protocol packets having TOS field set as low delay.
  - **normal** - Denies all protocol packets. Does not check for the TOS field in the packets.
  - **<value (0-7)>** - Denies the protocol packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS.
    - **0** - Denies all protocol packets. Does not check for the TOS field in the packets.
    - **1** - Denies the protocol packets having TOS field set as high reliability.
    - **2** - Denies the protocol packets having TOS field set as high throughput.
    - **3** - Denies the protocol packets having TOS field set either as high reliability or high throughput.
    - **4** - Denies the protocol packets having TOS field set as low delay.
    - **5** - Denies the protocol packets having TOS field set either as low delay or high reliability.
    - **6** - Denies the protocol packets having TOS field set either as low delay or high throughput.
    - **7** - Denies the protocol packets having TOS field set either as low delay, high reliability, or high throughput.

- **dscp** – Configures the Differentiated Services Code Point (DSCP) which provides the quality of service control. The various options available are:
  - **<value (0-63)>** – Configures the Differentiated Services Code Point value. This value ranges from 0 to 63.
  - **af11** - Matches packets with AF11 DSCP (001010).
  - **af12** - Matches packets with AF12 DSCP (001100).
  - **af13** - Matches packets with AF13 DSCP (001110).
  - **af21** - Matches packets with AF21 DSCP (010010).
  - **af22** - Matches packets with AF22 DSCP (010100).
  - **af23** - Matches packets with AF23 DSCP (010110).
  - **af31** - Matches packets with AF31 DSCP (011010).
  - **af32** - Matches packets with AF32 DSCP (011100).
  - **af33** - Matches packets with AF33 DSCP (011110).
  - **af41** - Matches packets with AF41 DSCP (100010).
  - **af42** - Matches packets with AF42 DSCP (100100).

- **af43** - Matches packets with AF43 DSCP (100110).
- **cs1** - Matches packets with CS1 (precedence 1) DSCP (001000).
- **cs2** - Matches packets with CS2 (precedence 2) DSCP (010000).
- **cs3** - Matches packets with CS3 (precedence 3) DSCP (011000).
- **cs4** - Matches packets with CS4 (precedence 4) DSCP (100000).
- **cs5** - Matches packets with CS5 (precedence 5) DSCP (101000).
- **cs6** - Matches packets with CS6 (precedence 6) DSCP (110000).
- **cs7** - Matches packets with CS7 (precedence 7) DSCP (111000).
- **default** - Default DSCP (000000).
- **ef** - Matches packets with EF DSCP (101110).

- **priority <(1-7)>** – Configures the priority value of the L3 filter to be used when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 7.

- **<precedence (0-7)> –** Precedence level to be used for filtering packets. This parameter is newly added in the existing command for industry standard CLI. The values are:
  - **0** - Matches packets with routine precedence.
  - **1** - Matches packets with priority precedence.
  - **2** - Matches packets with immediate precedence.
  - **3** - Matches packets with flash precedence.
  - **4** - Matches packets with flash override precedence.
  - **5** - Matches packets with critical precedence.
  - **6** - Matches packets with internetwork control precedence.
  - **7** - Matches packets with network control precedence.

- **fragments** - Considers fragments in the access list entry and examines non-initial fragments of IPv4 packets, when applying the access list entry.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **log** - Creates informational logging message about the packets that match the entry to be sent to the console. This message includes the access list number, whether the packet is permitted or denied, the protocol, whether the protocol is TCP, UDP, ICMP, or a number, and, if appropriate, the source and destination addresses and source and destination port numbers. This message is generated for the first packet that matches a flow. This message is then generated at five minute intervals with the number of packets permitted or denied in the prior five minute interval.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **log-input** - Creates information logging message along with the

information about the input interface.

Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **`reflect <access-list>`** – Reflects the name of the reflexive access list.

Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **`time-range <value>`** - Applies the time range. Time range defines the time when the permit or deny statements of the access control list are in effect.

Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode

MAC Access List Configuration Mode

Package

Workgroup, Enterprise, Metro_E, and Metro

Defaults

- protocol type - 255
- priority - 1
- dscp - -1

Note:

- Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed.
- Service VLAN, Service VLAN Priority, Customer VLAN and Customer VLAN Priority options are applicable only for Metro Solution, when the bridge mode is “Provider Bridge”.

Example

```
SEFOS (config-ext-nacl)# deny ospf any host 10.0.0.1 tos
max-throughput
```

Related Command(s)

- **`ip access-list -`** Creates IP ACLs and enters the IP access list configuration mode.
- **`permit- ip/ospf/pim/protocol type -`** Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched.
- **`show access-lists -`** Displays the access list configuration.

47.1.8 permit tcp

Command Objective	This command specifies the TCP packets to be forwarded based on the associated parameters.
Syntax	**permit tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> }[{gt <port-number (1-65535)> | lt <port-number (1-65535)>|eq <port-number (1-65535)> |range <port-number (1-65535)> <port-number (1-65535)>}]{ any | host <dest-ip-address> | <dest-ip-address> <dest-mask> }[{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> |range <port-number (1-65535)> <port-number (1-65535)>}][{ ack | rst }][{tos{max-reliability|max-throughput|min-delay|normal|<tos-value(0-7)>}|dscp {<value (0-63)> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef}}][priority <value(1-7)>] [{precedence <short(0-7)> | fragments | log | log-input | reflect <access-list> | time-range <value>}]**
Parameter Description	• **any|host <src-ip-address>| < src-ip-address> < src-mask>** - Permits traffic with the specified source address. The sources are: ▪ **any –** Permits TCP packets from any source. ▪ **host <src-ip-address>** - Permits TCP packets from the specified host source IPv4 address. ▪ **<src-ip-address> <src-mask>** - Permits TCP packets from the specified source IP address and the network mask to be used with the source IP address. • **gt <port-number (1-65535)>** - Allows only the TCP control packets having the TCP source port numbers greater than the specified port number. This value ranges from 1 to 65535. • **lt <port-number (1-65535)>** - Allows only the TCP control packets having the TCP source port numbers lesser than the specified port number. This value ranges from 1 to 65535. • **eq <port-number (1-65535)>** - Allows only the TCP control packets having the specified TCP source port numbers. This value ranges from 1 to 65535. • **range <port-number (1-65535)> <port-number (1-65535)>**- Allows only the TCP control packets having the TCP source port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values. • **any|host <dest-ip-address>| < dest-ip-address > < dest-mask>** - Permits the TCP packets with the specified destination address.

The destination can be:

- **any –** Permits TCP packets with any destination.
- **host <dest-ip-address>** - Permits TCP packets with specified host destination IPv4 address.
- **<dest-ip-address> < dest-mask>** - Permits TCP packets with the specified destination IP address and the network mask for the given destination IP address.

- **gt <port-number (1-65535)>** - Allows only the TCP control packets having the TCP destination port numbers greater than the specified port number. This value ranges from 1 to 65535.

- **lt <port-number (1-65535)>** - Allows only the TCP control packets having the TCP destination port numbers lesser than the specified port number. This value ranges from 1 to 65535.

- **eq <port-number (1-65535)>** - Allows only the TCP control packets having the specified TCP destination port numbers. This value ranges from 1 to 65535.

- **range <port-number (1-65535)> <port-number (1-65535)>** - Allows only the TCP control packets having the TCP destination port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values.

- **ack** - Configures the TCP ACK bit to be checked against the packet.

- **rst** - Configures the TCP RST bit to be checked against the packet.

- **tos** - Allows the protocol packets based on the following types of service configuration:
  - **max-reliability** - Allows the protocol packets having TOS field set as high reliability.
  - **max-throughput** - Allows the protocol packets having TOS field set as high throughput.
  - **min-delay –** Allows the protocol packets having TOS field set as low delay.
  - **normal** - Allows all protocol packets. Does not check for the TOS field in the packets.
  - **<value (0-7)>** - Allows the protocol packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS.
    - **0** - Allows all protocol packets. Does not check for the TOS field in the packets.
    - **1** - Allows the protocol packets having TOS field set as high reliability.
    - **2** - Allows the protocol packets having TOS field set as high throughput.

- **3** - Allows the protocol packets having TOS field set either as high reliability or high throughput.
- **4** - Allows the protocol packets having TOS field set as low delay.
- **5** - Allows the protocol packets having TOS field set either as low delay or high reliability.
- **6** - Allows the protocol packets having TOS field set either as low delay or high throughput.
- **7** - Allows the protocol packets having TOS field set either as low delay, high reliability, or high throughput.

- **dscp** – Configures the Differentiated Services Code Point (DSCP) which provides the quality of service control. The various options available are:
  - **<value (0-63)>** – Configures the Differentiated Services Code Point value. This value ranges from 0 to 63.
  - **af11** - Matches packets with AF11 DSCP (001010).
  - **af12** - Matches packets with AF12 DSCP (001100).
  - **af13** - Matches packets with AF13 DSCP (001110).
  - **af21** - Matches packets with AF21 DSCP (010010).
  - **af22** - Matches packets with AF22 DSCP (010100).
  - **af23** - Matches packets with AF23 DSCP (010110).
  - **af31** - Matches packets with AF31 DSCP (011010).
  - **af32** - Matches packets with AF32 DSCP (011100).
  - **af33** - Matches packets with AF33 DSCP (011110).
  - **af41** - Matches packets with AF41 DSCP (100010).
  - **af42** - Matches packets with AF42 DSCP (100100).
  - **af43** - Matches packets with AF43 DSCP (100110).
  - **cs1** - Matches packets with CS1 (precedence 1) DSCP (001000).
  - **cs2** - Matches packets with CS2 (precedence 2) DSCP (010000).
  - **cs3** - Matches packets with CS3 (precedence 3) DSCP (011000).
  - **cs4** - Matches packets with CS4 (precedence 4) DSCP (100000).
  - **cs5** - Matches packets with CS5 (precedence 5) DSCP (101000).
  - **cs6** - Matches packets with CS6 (precedence 6) DSCP (110000).
  - **cs7** - Matches packets with CS7 (precedence 7) DSCP (111000).
  - **default** - Default DSCP (000000).
  - **ef** - Matches packets with EF DSCP (101110).

- **priority <(1-7)>** – Configures the priority value of the L3 filter to be used when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 7.

- **<precedence (0-7)>** - Precedence level to be used for filtering packets. This parameter is newly added in the existing command for industry standard CLI. The values are:

- **0** - Matches packets with routine precedence.
- **1** - Matches packets with priority precedence.
- **2** - Matches packets with immediate precedence.
- **3** - Matches packets with flash precedence.
- **4** - Matches packets with flash override precedence.
- **5** - Matches packets with critical precedence.
- **6** - Matches packets with internetwork control precedence.
- **7** - Matches packets with network control precedence.

- **fragments** - Considers fragments in the access list entry and examines non-initial fragments of IPv4 packets, when applying the access list entry.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **log** - Creates informational logging message about the packets that match the entry to be sent to the console. This message includes the access list number, whether the packet is permitted or denied, the protocol, whether the protocol is TCP (Transport Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol) or a number, and, if appropriate, the source and destination addresses and source and destination port numbers. This message is generated for the first packet that matches a flow. This message is then generated at five minute intervals with the number of packets permitted or denied in the prior five minute interval.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **log-input** - Creates information logging message along with the information about the input interface.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **reflect <access-list>** – Reflects the name of the reflexive access list.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **time-range <value>** - Applies the time range. Time range defines the time when the permit or deny statements of the access control list are in effect.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode	ACL Extended Access List Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	• tos-value - 0 • dscp - 1 • priority - 1
Example	**SEFOS (config-ext-nacl)# permit tcp any range 1 2 12.0.0.1 255.0 gt 1**
Related Command(s)	• **ip access-list -** Creates IP access lists and enters the IP access list configuration mode. • **deny tcp -** Specifies the TCP packets to be rejected based on the associated parameters. • **show access-lists -** Displays the access list configuration.

47.1.9 deny tcp

Command Objective	This command specifies the TCP packets to be rejected based on the associated parameters.
Syntax	**deny tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> }[{gt <port-number (1-65535)> | lt <port-number (1-65535)>|eq <port-number (1-65535)> |range <port-number (1-65535)> <port-number (1-65535)>}]{ any | host <dest-ip-address> | <dest-ip-address> <dest-mask> }[{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> |range <port-number (1-65535)> <port-number (1-65535)>}][{ ack | rst }][{tos{max-reliability|max-throughput|min-delay|normal|<tos-value(0-7)>}|dscp {<value (0-63)> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef}}][priority <value(1-7)>] [{precedence <short(0-7)> | fragments | log | log-input | reflect <access-list> | time-range <value>}]**
Parameter Description	• **any|host <src-ip-address>| < src-ip-address> < src-mask>** - Denies traffic with the specified source address. The sources are: ▪ **any –** Denies TCP packets from any source. ▪ **host <src-ip-address>** - Denies TCP packets with the specified host source IPv4 address. ▪ **<src-ip-address> < src-mask>** - Denies TCP packets with the specified source IP address and the network mask to be used with the source IP address. • **gt <port-number (1-65535)>** - Denies only the TCP control packets having the TCP source port numbers greater than the specified port number. This value ranges from 1 to 65535. • **lt <port-number (1-65535)>** - Denies only the TCP control packets having the TCP source port numbers lesser than the specified port number. This value ranges from 1 to 65535. • **eq <port-number (1-65535)>** - Denies only the TCP control packets having the specified TCP source port numbers. This value ranges from 1 to 65535. • **range <port-number (1-65535)> <port-number (1-65535)>** - Denies only the TCP control packets having the TCP source port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values. • **any|host <dest-ip-address>| < dest-ip-address > < dest-**

mask> - Denies the TCP packets with the specified destination address. The destination can be:

- **any -** Denies TCP packets with any destination.
- **host <dest-ip-address>** - Denies TCP packets with specified host destination IPv4 address.
- **<dest-ip-address> <dest-mask>** - Denies TCP packets with the specified destination IP address and the network mask for the given destination IP address.

- **gt <port-number (1-65535)>** - Denies only the TCP control packets having the TCP destination port numbers greater than the specified port number. This value ranges from 1 to 65535.

- **lt <port-number (1-65535)>** - Denies only the TCP control packets having the TCP destination port numbers lesser than the specified port number. This value ranges from 1 to 65535.

- **eq <port-number (1-65535)>** - Denies only the TCP control packets having the specified TCP destination port numbers. This value ranges from 1 to 65535.

- **range <port-number (1-65535)> <port-number (1-65535)>** - Denies only the TCP control packets having the TCP destination port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values.

- **ack** - Configures the TCP ACK bit to be checked against the packet.

- **rst** - Configures the TCP RST bit to be checked against the packet.

- **tos** - Denies the protocol packets based on the following type of service configuration. The options are,
  - **max-reliability** - Denies the protocol packets having TOS field set as high reliability.
  - **max-throughput** - Denies the protocol packets having TOS field set as high throughput.
  - **min-delay** - Denies the protocol packets having TOS field set as low delay.
  - **normal** - Denies all protocol packets. Does not check for the TOS field in the packets.
  - **<value (0-7)>** - Denies the TCP packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS.
    - **0** - Denies all packets. Does not check for the TOS field in the packets.
    - **1** - Denies the packets having TOS field set as high reliability.
    - **2** - Denies the packets having TOS field set as high throughput.
    - **3** - Denies the packets having TOS field set either as high reliability

or high throughput.
    - **4** - Denies the packets having TOS field set as low delay.
    - **5** - Denies the packets having TOS field set either as low delay or high reliability.
    - **6** - Denies the packets having TOS field set either as low delay or high throughput.
    - **7** - Denies the packets having TOS field set either as low delay, high reliability, or high throughput.

- **dscp** – Configures the Differentiated Services Code Point (DSCP) which provides the quality of service control. The various options available are:
    - **<value (0-63)>** – Configures the Differentiated Services Code Point value. This value ranges from 0 to 63.
    - **af11** - Matches packets with AF11 DSCP (001010).
    - **af12** - Matches packets with AF12 DSCP (001100).
    - **af13** - Matches packets with AF13 DSCP (001110).
    - **af21** - Matches packets with AF21 DSCP (010010).
    - **af22** - Matches packets with AF22 DSCP (010100).
    - **af23** - Matches packets with AF23 DSCP (010110).
    - **af31** - Matches packets with AF31 DSCP (011010).
    - **af32** - Matches packets with AF32 DSCP (011100).
    - **af33** - Matches packets with AF33 DSCP (011110).
    - **af41** - Matches packets with AF41 DSCP (100010).
    - **af42** - Matches packets with AF42 DSCP (100100).
    - **af43** - Matches packets with AF43 DSCP (100110).
    - **cs1** - Matches packets with CS1 (precedence 1) DSCP (001000).
    - **cs2** - Matches packets with CS2 (precedence 2) DSCP (010000).
    - **cs3** - Matches packets with CS3 (precedence 3) DSCP (011000).
    - **cs4** - Matches packets with CS4 (precedence 4) DSCP (100000).
    - **cs5** - Matches packets with CS5 (precedence 5) DSCP (101000).
    - **cs6** - Matches packets with CS6 (precedence 6) DSCP (110000).
    - **cs7** - Matches packets with CS7 (precedence 7) DSCP (111000).
    - **default** - Default DSCP (000000).
    - **ef** - Matches packets with EF DSCP (101110).

- **priority <(1-7)>** – Configures the priority value of the L3 filter to be used when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 7.

- **<precedence (0-7)>** - Precedence level to be used for filtering packets. This parameter is newly added in the existing command for industry standard CLI. The values are:
    - **0** - Matches packets with routine precedence.

- **1** - Matches packets with priority precedence.
- **2** - Matches packets with immediate precedence.
- **3** - Matches packets with flash precedence.
- **4** - Matches packets with flash override precedence.
- **5** - Matches packets with critical precedence.
- **6** - Matches packets with internetwork control precedence.
- **7** - Matches packets with network control precedence.

- **fragments** - Considers fragments in the access list entry and examines non-initial fragments of IPv4 packets, when applying the access list entry.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **log** - Creates informational logging message about the packets that match the entry to be sent to the console. This message includes the access list number, whether the packet is permitted or denied, the protocol, whether the protocol is TCP (Transport Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol) or a number, and, if appropriate, the source and destination addresses and source and destination port numbers. This message is generated for the first packet that matches a flow. This message is then generated at five minute intervals with the number of packets permitted or denied in the prior five minute interval.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **log-input** - Creates information logging message along with the information about the input interface.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **reflect <access-list>** – Reflects the name of the reflexive access list.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **time-range <value>** - Applies the time range. Time range defines the time when the permit or deny statements of the access control list are in effect.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode	ACL Extended Access List Configuration Mode

Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	• tos-value - 0 • dscp - 1 • priority - 1
Example	**SEFOS (config-ext-nacl)# deny tcp any range 1 2 12.0.0.1 255.0 gt 1**
Related Command(s)	• **ip access-list -** Creates IP access list and enters the IP access list configuration mode. • **permit tcp -** Specifies the TCP packets to be forwarded based on the associated parameters. • **show access-lists -** Displays the access list configuration.

47.1.10 permit udp

Command Objective	This command specifies the UDP packets to be forwarded based on the associated parameters.
Syntax	**permit udp { any | host <src-ip-address> | <src-ip-address> <src-mask>}[{gt <port-number (1-65535)> | lt <port-number (1-65535)>| eq <port-number (1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}]{ any | host <dest-ip-address> | <dest-ip-address> <dest-mask> }[{ gt <port-number (1-65535)> | lt <port-number (1-65535)>| eq <port-number (1-65535)>| range <port-number (1-65535)> <port-number (1-65535)>}][{tos{max-reliability|max-throughput|min-delay|normal|<tos-value(0-7)>} | dscp {<value (0-63)> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef} }] [priority <(1-7)>] [{precedence (0-7)> | fragments | log | log-input | reflect <access-list> | time-range <value>}]**
Parameter Description	• **any|host <src-ip-address>| < src-ip-address> <src-mask>** - Permits traffic with the specified source address. The sources are: ▪ **any –** Permits UDP packets from any source. ▪ **host <src-ip-address>** - Permits UDP packets from the specified host source IPv4 address. ▪ **<src-ip-address> <src-mask>** - Permits UDP packets from the specified source IP address and the network mask to be used with the source IP address • **gt <port-number (1-65535)>** - Allows only the UDP control packets having the TCP source port numbers greater than the specified port number. This value ranges from 1 to 65535. • **lt <port-number (1-65535)>** - Allows only the UDP control packets having the UDP source port numbers lesser than the specified port number. This value ranges from 1 to 65535. • **eq <port-number (1-65535)>** - Allows only the UDP control packets having the specified UDP source port numbers. This value ranges from 1 to 65535. • **range <port-number (1-65535)> <port-number (1-65535)>** - Allows only the UDP control packets having the UDP source port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values. • **any|host <dest-ip-address>| < dest-ip-address > <dest-mask>** - Permits traffic with the specified destination address. The

destination can be:

- **any –** Permits UDP packets with any destination.
- **host <dest-ip-address>** - Permits UDP packets with specified host destination IPv4 address.
- **<dest-ip-address> <dest-mask>** - Permits UDP packets with the specified destination IP address and the network mask for the given source IP address.

- **gt <port-number (1-65535)>** - Allows only the UDP control packets having the UDP destination port numbers greater than the specified port number. This value ranges from 1 to 65535.

- **lt <port-number (1-65535)>** - Allows only the UDP control packets having the UDP destination port numbers lesser than the specified port number. This value ranges from 1 to 65535.

- **eq <port-number (1-65535)>** - Allows only the UDP control packets having the specified UDP destination port numbers. This value ranges from 1 to 65535.

- **range <port-number (1-65535)> <port-number (1-65535)>** - Allows only the UDP control packets having the UDP destination port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values.

- **tos** - Allows the protocol packets based on the following types of service configuration:
  - **max-reliability** - Allows the protocol packets having TOS field set as high reliability.
  - **max-throughput** - Allows the protocol packets having TOS field set as high throughput.
  - **min-delay –** Allows the protocol packets having TOS field set as low delay.
  - **normal** - Allows all protocol packets. Does not check for the TOS field in the packets.
  - **<value (0-7)>** - Allows the protocol packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS.
    - **0** - Allows all protocol packets. Does not check for the TOS field in the packets.
    - **1** - Allows the protocol packets having TOS field set as high reliability.
    - **2** - Allows the protocol packets having TOS field set as high throughput.
    - **3** - Allows the protocol packets having TOS field set either as high reliability or high throughput.
    - **4** - Allows the protocol packets having TOS field set as low delay.
    - **5** - Allows the protocol packets having TOS field set either as low

delay or high reliability.

- **6** - Allows the protocol packets having TOS field set either as low delay or high throughput.
- **7** - Allows the protocol packets having TOS field set either as low delay, high reliability, or high throughput.

- **dscp** – Configures the Differentiated Services Code Point (DSCP) which provides the quality of service control. The various options available are:
  - **<value (0-63)>** – Configures the Differentiated Services Code Point value. This value ranges from 0 to 63.
  - **af11** - Matches packets with AF11 DSCP (001010).
  - **af12** - Matches packets with AF12 DSCP (001100).
  - **af13** - Matches packets with AF13 DSCP (001110).
  - **af21** - Matches packets with AF21 DSCP (010010).
  - **af22** - Matches packets with AF22 DSCP (010100).
  - **af23** - Matches packets with AF23 DSCP (010110).
  - **af31** - Matches packets with AF31 DSCP (011010).
  - **af32** - Matches packets with AF32 DSCP (011100).
  - **af33** - Matches packets with AF33 DSCP (011110).
  - **af41** - Matches packets with AF41 DSCP (100010).
  - **af42** - Matches packets with AF42 DSCP (100100).
  - **af43** - Matches packets with AF43 DSCP (100110).
  - **cs1** - Matches packets with CS1 (precedence 1) DSCP (001000).
  - **cs2** - Matches packets with CS2 (precedence 2) DSCP (010000).
  - **cs3** - Matches packets with CS3 (precedence 3) DSCP (011000).
  - **cs4** - Matches packets with CS4 (precedence 4) DSCP (100000).
  - **cs5** - Matches packets with CS5 (precedence 5) DSCP (101000).
  - **cs6** - Matches packets with CS6 (precedence 6) DSCP (110000).
  - **cs7** - Matches packets with CS7 (precedence 7) DSCP (111000).
  - **default** - Default DSCP (000000).
  - **ef** - Matches packets with EF DSCP (101110).

- **priority <(1-7)>** – Configures the priority value of the L3 filter to be used when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 7.

- **<precedence (0-7)> –** Precedence level to be used for filtering packets. This parameter is newly added in the existing command for industry standard CLI. The values are:
  - **0** - Matches packets with routine precedence.
  - **1** - Matches packets with priority precedence.
  - **2** - Matches packets with immediate precedence.
  - **3** - Matches packets with flash precedence.

- **4** - Matches packets with flash override precedence.
- **5** - Matches packets with critical precedence.
- **6** - Matches packets with internetwork control precedence.
- **7** - Matches packets with network control precedence.

- **fragments** - Considers fragments in the access list entry and examines non-initial fragments of IPv4 packets, when applying the access list entry.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **log** - Creates informational logging message about the packets that match the entry to be sent to the console. This message includes the access list number, whether the packet is permitted or denied, the protocol, whether the protocol is TCP (Transport Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol) or a number, and, if appropriate, the source and destination addresses and source and destination port numbers. This message is generated for the first packet that matches a flow. This message is then generated at five minute intervals with the number of packets permitted or denied in the prior five minute interval.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **log-input** - Creates information logging message along with the information about the input interface.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **reflect <access-list>** – Reflects the name of the reflexive access list.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **time-range <value>** - Applies the time range. Time range defines the time when the permit or deny statements of the access control list are in effect.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode	ACL Extended Access List Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro

Defaults	• dscp - -1 • priority - 1
Example	**SEFOS (config-ext-nacl)# permit udp any range 1 2 12.0.0.1 255.0 gt 1**
Related Command(s)	• **ip access-list –** Creates IP ACLs and enters the IP access list configuration mode. • **deny udp –** Specifies the UDP packets to be rejected based on the associated parameters. • **show access-lists –** Displays the access list configuration.

47.1.11 deny udp

Command Objective	This command specifies the UDP packets to be rejected based on the associated parameters.
Syntax	**deny udp { any | host <src-ip-address> | <src-ip-address> <src-mask>}[{gt <port-number (1-65535)> | lt <port-number (1-65535)>| eq <port-number (1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}]{ any | host <dest-ip-address> | <dest-ip-address> <dest-mask> }[{ gt <port-number (1-65535)> | lt <port-number (1-65535)>| eq <port-number (1-65535)>| range <port-number (1-65535)> <port-number (1-65535)>}][{tos{max-reliability|max-throughput|min-delay|normal|<tos-value(0-7)>} | dscp {<value (0-63)> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef} }] [priority <(1-7)>] [{precedence (0-7)> | fragments | log | log-input | reflect <access-list> | time-range <value>}]**
Parameter Description	• **any|host <src-ip-address>| < src-ip-address><src-mask>** - Denies the UDP packets with the specified source address. The sources are: ▪ **any** – Denies UDP packets from any source. ▪ **host <src-ip-address>** - Denies UDP packets with the specified host source IPv4 address. ▪ **<src-ip-address> <src-mask>** - Denies UDP packets with the specified source IP addressand the network mask to be used with the source IP address. • **gt <port-number (1-65535)>** - Denies only the UDP control packets having the TCP source port numbers greater than the specified port number. This value ranges from 1 to 65535. • **lt <port-number (1-65535)>** - Denies only the UDP control packets having the UDP source port numbers lesser than the specified port number. This value ranges from 1 to 65535. • **eq <port-number (1-65535)>** - Denies only the UDP control packets having the specified UDP source port numbers. This value ranges from 1 to 65535. • **range <port-number (1-65535)> <port-number (1-65535)>** - Denies only the UDP control packets having the UDP source port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values. • **any|host <dest-ip-address>| < dest-ip-address > <dest-**

mask> - Denies the UDP packets with the specified destination address. The destination can be:

- **any -** Denies UDP packets with any destination
- **host <dest-ip-address>** - Denies UDP packets with specified host destination IPv4 address
- **<dest-ip-address> <dest-mask>** - Denies UDP packets with the specified destination IP address and the network mask for the given source IP address

- **gt <port-number (1-65535)>** - Denies only the UDP control packets having the UDP destination port numbers greater than the specified port number. This value ranges from 1 to 65535.

- **lt <port-number (1-65535)>** - Denies only the UDP control packets having the UDP destination port numbers lesser than the specified port number. This value ranges from 1 to 65535.

- **eq <port-number (1-65535)>** - Denies only the UDP control packets having the specified UDP destination port numbers. This value ranges from 1 to 65535.

- **range <port-number (1-65535)> <port-number (1-65535)>** - Denies only the UDP control packets having the UDP destination port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values.

- **tos** - Denies the protocol packets based on the following Type Of Service configurations:
  - **max-reliability** - Denies the protocol packets having TOS field set as high reliability.
  - **max-throughput** - Denies the protocol packets having TOS field set as high throughput.
  - **min-delay -** Denies the protocol packets having TOS field set as low delay.
  - **normal** - Denies all protocol packets. Does not check for the TOS field in the packets.
  - **<value (0-7)>** - Denies the protocol packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS.
    - **0** - Denies all protocol packets. Does not check for the TOS field in the packets.
    - **1** - Denies the protocol packets having TOS field set as high reliability.
    - **2** - Denies the protocol packets having TOS field set as high throughput.
    - **3** - Denies the protocol packets having TOS field set either as high reliability or high throughput.
    - **4** - Denies the protocol packets having TOS field set as low delay.

- **5** - Denies the protocol packets having TOS field set either as low delay or high reliability.
- **6** - Denies the protocol packets having TOS field set either as low delay or high throughput.
- **7** - Denies the protocol packets having TOS field set either as low delay, high reliability, or high throughput.

- **dscp** – Configures the Differentiated Services Code Point (DSCP) which provides the quality of service control. The various options available are:
  - **<value (0-63)>** – Configures the Differentiated Services Code Point value. This value ranges from 0 to 63.
  - **af11** - Matches packets with AF11 DSCP (001010).
  - **af12** - Matches packets with AF12 DSCP (001100).
  - **af13** - Matches packets with AF13 DSCP (001110).
  - **af21** - Matches packets with AF21 DSCP (010010).
  - **af22** - Matches packets with AF22 DSCP (010100).
  - **af23** - Matches packets with AF23 DSCP (010110).
  - **af31** - Matches packets with AF31 DSCP (011010).
  - **af32** - Matches packets with AF32 DSCP (011100).
  - **af33** - Matches packets with AF33 DSCP (011110).
  - **af41** - Matches packets with AF41 DSCP (100010).
  - **af42** - Matches packets with AF42 DSCP (100100).
  - **af43** - Matches packets with AF43 DSCP (100110).
  - **cs1** - Matches packets with CS1 (precedence 1) DSCP (001000).
  - **cs2** - Matches packets with CS2 (precedence 2) DSCP (010000).
  - **cs3** - Matches packets with CS3 (precedence 3) DSCP (011000).
  - **cs4** - Matches packets with CS4 (precedence 4) DSCP (100000).
  - **cs5** - Matches packets with CS5 (precedence 5) DSCP (101000).
  - **cs6** - Matches packets with CS6 (precedence 6) DSCP (110000).
  - **cs7** - Matches packets with CS7 (precedence 7) DSCP (111000).
  - **default** - Default DSCP (000000).
  - **ef** - Matches packets with EF DSCP (101110).

- **priority <(1-7)>** – Configures the priority value of the L3 filter to be used when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 7.

- **<precedence (0-7)> –** Precedence level to be used for filtering packets. This parameter is newly added in the existing command for industry standard CLI. The values are:
  - **0** - Matches packets with routine precedence.
  - **1** - Matches packets with priority precedence.
  - **2** - Matches packets with immediate precedence.

- **3** - Matches packets with flash precedence.
- **4** - Matches packets with flash override precedence.
- **5** - Matches packets with critical precedence.
- **6** - Matches packets with internetwork control precedence.
- **7** - Matches packets with network control precedence.

- **fragments** - Considers fragments in the access list entry and examines non-initial fragments of IPv4 packets, when applying the access list entry.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **log** - Creates informational logging message about the packets that match the entry to be sent to the console. This message includes the access list number, whether the packet is permitted or denied, the protocol, whether the protocol is TCP (Transport Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol) or a number, and, if appropriate, the source and destination addresses and source and destination port numbers. This message is generated for the first packet that matches a flow. This message is then generated at five minute intervals with the number of packets permitted or denied in the prior five minute interval.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **log-input** - Creates information logging message along with the information about the input interface.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **reflect <access-list>** – Reflects the name of the reflexive access list.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

- **time-range <value>** - Applies the time range. Time range defines the time when the permit or deny statements of the access control list are in effect.

  Note: This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

Mode	ACL Extended Access List Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro

Defaults	• dscp - -1 • priority - 1
Example	**SEFOS (config-ext-nacl)# deny udp any range 1 2 12.0.0.1 255.0 gt 1**
Related Command(s)	• **ip access-list –** Creates IP ACLs and enters the IP access list configuration mode. • **permit udp –** Specifies the UDP packets to be forwarded based on the associated parameters. • **show access-lists –** Displays the access list configuration.

47.1.12 permit icmp

Command Objective	This command specifies the ICMP packets to be forwarded based on the IP address and the associated parameters.
Syntax	**permit icmp {any |host <src-ip-address>|<src-ip-address> <mask>}{any | host <dest-ip-address> | <dest-ip-address> <mask> }**message-type <short (0-255)> message-code <short (0-255)>] **[priority <(1-7)>]**
Parameter Description	• **any|host <src-ip-address>| < src-ip-address> <mask>** - Permits the ICMP packet with the specified source address. The sources are: ▪ **any -** Permits ICMP packets from any source. ▪ **host <src-ip-address>** - Permits ICMP packets from the specified host source IPv4 address. ▪ **<src-ip-address> <mask>** - Permits ICMP packets from the specified source IP address and the network mask to be used with the source IP address. • **any|host <dest-ip-address>| < dest-ip-address > <mask>** - Permits the ICMP packets with the specified destination address. The destination can be: ▪ **any -** Permits ICMP packets with any destination. ▪ **host <dest-ip-address>** - Permits ICMP packets with specified host destination IPv4 address. ▪ **<dest-ip-address> <mask>** - Permits ICMP packets with the specified destination IP address and the network mask for the given destination IP address. • **message-type <short (0-255)>** - Configures the ICMP message type to be checked against the packet. The packet will be allowed if it matches the message type. This value ranges from 0 to 255. Some of the ICMP message types are:

Value	ICMP Message type
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo Request
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply

	15 Information Request 16 Information Reply 17 Address Mask Request 18 Address Mask Reply 255 No ICMP type • **message-code <short (0-255)>** - Configures the ICMP message code to be checked against the packet. The packet will be allowed if it matches the message code. This value ranges from 0 to 255. Some of the ICMP message codes are: **Value ICMP code** 0 Network Unreachable 1 Host Unreachable 2 Protocol Unreachable 3 Port Unreachable 4 Fragment Need 5 Source Route Fail 6 Destination Network Unknown 7 Destination Host Unknown 8 Source Host Isolated 9 Destination Network Administratively Prohibited 10 Destination Host Administratively Prohibited 11 Network Unreachable TOS 12 Host Unreachable TOS 255 No ICMP Code • **priority <(1-7)>**– Configures the priority value of the L3 filter to be used when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 7.
Mode	ACL Extended Access List Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	• priority - 1 • dscp – 1 • message-type / message code - 255
Example	**SEFOS (config-ext-nacl)# permit icmp any 13.0.0.1 255.0 25 0 priority 1**
Related Command(s)	• **ip access-list -** Creates IP ACLs and enters the IP access list configuration mode. • **deny icmp -** Specifies the ICMP packets to be rejected based on the IP

address and associated parameters.

- **`show access-lists -`** Displays the access list configuration.

47.1.13 deny icmp

Command Objective	This command specifies the ICMP packets to be rejected based on the IP address and associated parameters.
Syntax	**deny icmp {any |host <src-ip-address>|<src-ip-address> <mask>}{any | host <dest-ip-address> | <dest-ip-address> <mask> }**message-type <short (0-255)> message-code <short (0-255)>] **[priority <(1-7)>]**
Parameter Description	• **any|host <src-ip-address>| < src-ip-address> <mask>** - Denies the ICMP packet with the specified source address. The sources are: ▪ **any -** Denies ICMP packets from any source. ▪ **host <src-ip-address>** - Denies ICMP packets from the specified host source IPv4 address. ▪ **<src-ip-address> <mask>** - Denies ICMP packets from the specified source IP address and the network mask to be used with the source IP address. • **any|host <dest-ip-address>| < dest-ip-address > <mask>** - Denies the ICMP packets with the specified destination address. The destination can be: ▪ **any -** Denies ICMP packets with any destination. ▪ **host <dest-ip-address>** - Denies ICMP packets with specified host destination IPv4 address. ▪ **<dest-ip-address> <mask>** - Denies ICMP packets with the specified destination IP address and the network mask for the given destination IP address. • **message-type <short (0-255)>** - Configures the ICMP message type to be checked against the packet. The packet will be denied if it matches with the message type. This value ranges from 0 to 255. Some of the ICMP message types are:

Value	ICMP Message type
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo Request
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply

	15 Information Request 16 Information Reply 17 Address Mask Request 18 Address Mask Reply 255 No ICMP type • **message-code <short (0-255)>-** Configures the ICMP message code to be checked against the packet. The packet will be denied if it matches with the message code. This value ranges from 0 to 255. Some of the ICMP message codes are: **Value ICMP code** 0 Network Unreachable 1 Host Unreachable 2 Protocol Unreachable 3 Port Unreachable 4 Fragment Need 5 Source Route Fail 6 Destination Network Unknown 7 Destination Host Unknown 8 Source Host Isolated 9 Destination Network Administratively Prohibited 10 Destination Host Administratively Prohibited 11 Network Unreachable TOS 12 Host Unreachable TOS 255 No ICMP Code • **priority <(1-7)>–** Configures the priority value of the L3 filter to be used when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 7.
Mode	ACL Extended Access List Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	• priority - 1 • dscp – 1 • message-type / message code - 255
Example	**SEFOS (config-ext-nacl)# deny icmp any 13.0.0.1 255.0 25 0 priority 1**
Related Command(s)	• **ip access-list -** Creates IP ACLs and enters the IP access list configuration mode. • **permit icmp -** Specifies the ICMP packets to be forwarded based on

the IP address and the associated parameters.

- **`show access-lists -`** Displays the access list configuration.

47.1.14 ip access-group

Command Objective	This command enables access control for the packets on the interface. It controls access to a Layer 2 or Layer 3 interface. The no form of this command removes all access groups or the specified access group from the interface. The direction of filtering is specified using the token in or out.
Syntax	**ip access-group <access-list-number (1-1024)> {in | out}** **no ip access-group <access-list-number (1-1024)> {in | out}**
Parameter Description	• **<access-list-number (1-1024)>**– Configures the IP access control list number on the interface. This value ranges from 1 to 1024. • **in** - Configures the packets as Inbound packets. • **out** - Configures the packets as Outbound packets.
Mode	Interface Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Note:	• IP access list must be created. • Following are the limitations for this command to be applicable to Layer 2 interfaces: ▪ The `out` keyword is not supported by Layer 2 interfaces. ▪ An IP ACL applied to a Layer 2 interface filters only the IP packets. MAC access group interface configuration command with MAC-extended ACLs must be used to filter non-IP packets.
Example	**SEFOS (config-if)# ip access-group 1 in**
Related Command(s)	• **ip access-list -** Creates IP ACLs and enters the IP access list configuration mode. • **show access-lists -** Displays the access list configuration.

47.1.15 mac access-group

Command Objective	This command configures a MAC access control list (ACL) to a Layer 2 interface. The no form of this command removes the MAC ACLs from the interface.
Syntax	**mac access-group <access-list-number (1-1024)> in** **no mac access-group <access-list-number (1-1024)> in**
Parameter Description	• **<access-list-number (1-1024)>**– Configures the MAC access control list number on the interface. This value ranges from 1 to 1024. • **in** - Configures the packets as Inbound packets.
Mode	Interface Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Note:	MAC access list must have been created.
Example	**SEFOS (config-if)# mac access-group 5 in**
Related Command(s)	• **mac access-list extended -** Creates Layer 2 MAC ACLs and returns the MAC access list configuration mode to the user. • **permit - MAC** - Specifies the packets to be forwarded based on the MAC address and the associated parameters. • **deny - MAC** - Specifies the packets to be rejected based on the MAC address and the associated parameters. • **show access-lists -** Displays the access list statistics.

47.1.16 ipv6 access-group

Command Objective	This command enables access control for the IPv6 packets on the interface. It controls access to a Layer 2 or Layer 3 interface. The no form of this command removes all access groups or the specified access group from the interface. The direction of filtering is specified using the token in or out.
Syntax	**ipv6 access-group <access-list-number (11-1024)> in** **no ipv6 access-group <access-list-number (11-1024)> in**
Parameter Description	• **<access-list-number (11-1024)>**– Configures the IPv6 access control list number on the interface. This value ranges from 11 to 1024. • **in** - Configures the packets as Inbound packets.
Mode	Interface Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Note:	IPv6 access list must have been created.
Example	**SEFOS (config-if)# ipv6 access-group 15 in**
Related Command(s)	• **ipv6 access-list extended** - Creates IPv6 access list and enters the IPv6 access list configuration mode. • **show access-lists –** Displays the access list statistics.

47.1.17 permit - MAC

Command Objective	This command specifies the packets to be forwarded based on the MAC address and the associated parameters. That is, this command allows non-IP traffic to be forwarded if the conditions are matched.
Syntax	**permit { any | host <src-mac-address>}{ any | host <dest-mac-address> }[aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000|etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-id | <protocol (0-65535)> [Vlan <vlan-id (1-4094)>][user-priority <value (0-7)>] [priority value (1-7)>]**
Parameter Description	• **any|host <src-mac-address>** - Allows packets to be forwarded based on the source MAC address. The source MAC address can be: ▪ **any** - Permits all packets from any source MAC address. ▪ **host <src-mac-address>** - Permits all packets with the specified host source MAC address. • **any|host <dest-mac-address>** - Allows packets to be forwarded based on the destination MAC address. The destination MAC address can be: ▪ **any** - Permits all packets from any destination MAC address. ▪ **host <dest-mac-address>** - Permits all packets with the specified host destination MAC address. • **aarp** - Configures the non-IP protocol type as Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address. • **amber** - Configures the non-IP protocol type as EtherType DEC-Amber. • **dec-spanning** - Configures the non-IP protocol type as EtherType Digital Equipment Corporation (DEC) spanning tree. • **decnet-iv –** Configures the non-IP protocol type as EtherType DECnet Phase IV protocol. • **diagnostic** - Configures the non-IP protocol type as EtherType DEC-Diagnostic • **dsm** - Configures the non-IP protocol type as EtherType DEC-DSM/DDP. • **etype-6000** - Configures the non-IP protocol type as EtherType 0x6000. • **etype-8042** - Configures the non-IP protocol type as EtherType 0x8042.

- **lat** - Configures the non-IP protocol type as EtherType DEC-LAT.
- **lavc-sca** - Configures the non-IP protocol type as EtherType DEC-LAVC-SCA.
- **mop-console** - Configures the non-IP protocol type as EtherType DEC-MOP Remote Console.
- **mop-dump** - Configures the non-IP protocol type as EtherType DEC-MOP Dump.
- **msdos** - Configures the non-IP protocol type as EtherType DEC-MSDOS.
- **mumps** - Configures the non-IP protocol type as EtherType DEC-MUMPS.
- **netbios** - Configures the non-IP protocol type as EtherType DEC-Network Basic Input/Output System (NETBIOS).
- **vines-echo** - Configures the non-IP protocol type as EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
- **vines-ip** - Configures the non-IP protocol type as EtherType VINES IP
- **xns-id** - Configures the non-IP protocol type as EtherType Xerox Network Systems (XNS) protocol suite.
- **<protocol (0-65535)>** - Configures the non-IP protocol type to be filtered. This value ranges from 0 to 65535. The value 0 represents that filter is applicable for all protocols.
- **vlan <vlan-id (1-4094)>** - Specifies the VLAN ID to be filtered. This value ranges from 1 to 4094.
- **user-priority <value (0-7)> -** Configures the user priority value of the L3 filter. This value ranges from 0 to 7.
- **priority< value(1-7)>** - Configures the priority of the filter to decide in which order the filter rule is applicable when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 7.

Mode ACL MAC Configuration Mode

Package Workgroup, Enterprise, Metro_E, and Metro

Defaults

- Protocol value - 0

Note:

- MAC access list must have been created.

Example

```
SEFOS (config-ext-macl)# permit any host 00:11:22:33:44:55
vlan 1 user-priority 0 priority 0
```

Related Command(s)

- **`mac access-list extended –`** Creates Layer 2 MAC ACLs and returns the MAC access list configuration mode to the user.
- **`user-defined access-list`** - Creates the user defined access list.
- **`mac access-group –`** Applies a MAC access control list (ACL) to a Layer 2 interface.
- **`deny – MAC`** - Specifies the packets to be rejected based on the MAC address and the associated parameters.
- **`show access-lists –`** Displays the access list statistics.

47.1.18 deny - MAC

Command Objective	This command denies the packets to be rejected based on the MAC address and the associated parameters.
Syntax	**deny { any | host <src-mac-address>}{ any | host <dest-mac-address> }[aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000|etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-id | <protocol (0-65535)> [Vlan <vlan-id (1-4094)>][user-priority <value (0-7)>] [priority value (1-7)>]**
Parameter Description	• **any|host <src-mac-address>** - Denies packets to be forwarded based on the source MAC address. The source MAC address can be: ▪ **any** - Denies all packets from any source MAC address. ▪ **host <src-mac-address>** - Denies all packets with the specified host source MAC address. • **any|host <dest-mac-address>** - Denies packets to be forwarded based on the destination MAC address. The destination MAC address can be: ▪ **any** - Denies all packets from any destination MAC address. ▪ **host <dest-mac-address>** - Denies all packets with the specified host destination MAC address. • **aarp** - Configures the non-IP protocol type as Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address. • **amber** - Configures the non-IP protocol type as EtherType DEC-Amber. • **dec-spanning** - Configures the non-IP protocol type as EtherType Digital Equipment Corporation (DEC) spanning tree. • **decent-iv** - Configures the non-IP protocol type as EtherType DECnet Phase IV protocol. • **diagnostic** - Configures the non-IP protocol type as EtherType DEC-Diagnostic. • **dsm** - Configures the non-IP protocol type as EtherType DEC-DSM/DDP. • **etype-6000 –** Configures the non-IP protocol type as EtherType 0x6000. • **etype-8042** - Configures the non-IP protocol type as EtherType 0x8042.

- **lat –** Configures the non-IP protocol type as EtherType DEC-LAT.
- **lavc-sca** - Configures the non-IP protocol type as EtherType DEC-LAVC-SCA.
- **mop-console** - Configures the non-IP protocol type as EtherType DEC-MOP Remote Console.
- **mop-dump** - Configures the non-IP protocol type as EtherType DEC-MOP Dump.
- **msdos** - Configures the non-IP protocol type as EtherType DEC-MSDOS.
- **mumps** - Configures the non-IP protocol type as EtherType DEC-MUMPS.
- **netbios** - Configures the non-IP protocol type as EtherType DEC-Network Basic Input/Output System (NETBIOS).
- **vines-echo** - Configures the non-IP protocol type as EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
- **vines-ip** - Configures the non-IP protocol type as EtherType VINES IP.
- **xns-id** - Configures the non-IP protocol type as EtherType Xerox Network Systems (XNS) protocol suite.
- **<protocol (0-65535)>** - Configures the non-IP protocol type to be filtered. This value ranges from 0 to 65535. The value 0 represents that filter is applicable for all protocols.
- **encaptype <value (1-65535)>** - Configures the arbitrary ether type of a packet with Ethernet II or SNAP encapsulation in decimal. This value ranges from 1 to 65535.
- **vlan <vlan-id (1-4094)>** - Specifies the VLAN ID to be filtered. This value ranges from 1 to 4094.
- **user-priority <value (0-7)> –** Configures the user priority value of the L3 filter. This value ranges from 0 to 7.
- **priority <(1-7)>–** Configures the priority value of the L3 filter to be used when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 7.

Mode ACL MAC Configuration Mode

Package Workgroup, Enterprise, Metro_E, and Metro

Defaults

- <protocol (0-65535)> - 0
- priority - 1

Note:	MAC access list must have been created.
Example	**SEFOS (config-ext-macl)# permit any host 00:11:22:33:44:55 vlan 1 user-priority 0 priority 0**
Related Command(s)	• **mac access-list extended -** Creates Layer 2 MAC ACLs and returns the MAC access list configuration mode to the user • **user-defined access-list** - Creates the user defined access list. • **mac access-group -** Applies a MAC access control list (ACL) to a Layer 2 interface. • **permit - MAC** - Specifies the packets to be forwarded based on the MAC address and the associated parameters. • **show access-lists -** Displays the access list statistics.

47.1.19 show access-lists

Command Objective	This command displays the access list configuration.
Syntax	**show access-lists [{ip <access-list-number (1-1024)> | mac <access-list-number (1-1024)> | <access-list-number (1-1024)>}]**
Parameter Description	• **ip <access-list-number (1-1024)>** – Displays the access list configuration for the specified IP access list. This value ranges from 1 and 1024. • **mac <access-list-number (1-1024)>** - Displays the access list configuration for the specified MAC access list. This value ranges from 1 and 1024. • **< access-list-number (1-1024)>** - Displays the access list configuration for the specified user defined access list. This value ranges from 1 and 1024.
Mode	Privileged/User EXEC Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS# show access-lists** IP ACCESS LISTS ---------------- Standard IP Access List 1 --------------------------- IP address Type : IPV4 Source IP address : 0.0.0.0 Source IP address mask : 255.255.255.255 Source IP Prefix Length : 128 Destination IP address : 0.0.0.0 Destination IP address mask : 255.255.255.255 Destination IP Prefix Length : 128 Flow Identifier : 0 In Port List : Ex0/1 Out Port List : NIL Filter Action : Permit

```
 Status                              : Active

Standard IP Access List 11
---------------------------
 IP address Type                     : IPV4
 Source IP address                   : 0.0.0.0
 Source IP address mask              : 0.0.0.0
 Source IP Prefix Length             : 0
 Destination IP address              : 13.0.0.0
 Destination IP address mask         : 255.0.0.0
 Destination IP Prefix Length        : 8
 Flow Identifier                     : 0
 In Port List                        : Ex0/1
 Out Port List                       : NIL
 Filter Action                       : Deny
 Status                              : Active


Standard IP Access List 12
---------------------------
 IP address Type                     : IPV6
 Source IP address                   : 1111::2222
 Source IP Prefix Length             : 128
 Destination IP address              : 1111::3333
 Destination IP Prefix Length        : 126
 Flow Identifier                     : 1048575
 In Port List                        : NIL
Out Port List                       : NIL
 Filter Action                       : Permit
 Status                              : InActive

MAC ACCESS LISTS
-----------------

Extended MAC Access List 1
----------------------------
 Filter Priority                     : 7
```

```
 Ether Type                          : 1
 Protocol Type                       : 1
 Vlan Id                             : 1
 User-Priority                       : 0
 Destination MAC Address             : 00:11:22:33:44:55
 Source MAC Address                  : 00:00:00:00:00:00
 In Port List                        : NIL
 Filter Action                       : Deny
 Status                              : InActive
```

SEFOS# show access-lists ip 1

```
Standard IP Access List 1
---------------------------
 IP address Type                     : IPV4
 Source IP address                   : 0.0.0.0
 Source IP address mask              : 255.255.255.255
 Source IP Prefix Length             : 128
 Destination IP address              : 0.0.0.0
 Destination IP address mask         : 255.255.255.255
 Destination IP Prefix Length        : 128
 Flow Identifier                     : 0
 In Port List                        : Ex0/1
 Out Port List                       : NIL
 Filter Action                       : Permit
 Status                              : Active
```

SEFOS# show access-lists mac 1

```
Extended MAC Access List 1
----------------------------
 Filter Priority                     : 7
 Ether Type                          : 1
 Protocol Type                       : 1
 Vlan Id                             : 1
 User-Priority                       : 0
 Destination MAC Address             : 00:11:22:33:44:55
 Source MAC Address                  : 00:00:00:00:00:00
```

```
In Port List                    : NIL
Filter Action                   : Deny
Status                          : InActive
```

Related Command(s)

- **ip access-list -** Creates IP ACLs and enters the IP access list configuration mode
- **mac access-list extended -** Creates Layer 2 MAC ACLs and returns the MAC access list configuration mode to the user
- **permit- ip/ospf/pim/protocol type -** Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched.
- **permit ipv6** - Specifies IP packets to be forwarded based on protocol and associated parameters.
- **deny - ip/ospf/pim/protocol type -** Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched.
- **deny ipv6** - Specifies IPv6 packets to be rejected based on protocol and associated parameters.
- **permit tcp -** Specifies the TCP packets to be forwarded based on the associated parameters.
- **deny tcp -** Specifies the TCP packets to be rejected based on the associated parameters.
- **permit udp -** Specifies the UDP packets to be forwarded based on the associated parameters.
- **deny udp -** Specifies the UDP packets to be rejected based on the associated parameters.
- **permit icmp**- Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters.
- **deny icmp -** Specifies the ICMP packets to be rejected based on the IP address and associated parameters.
- **ip access-group**- Enables access control for the packets on the interface.
- **mac access-group -** Applies a MAC access control list (ACL) to a Layer 2 interface.
- **user-defined access-group** - Applies a user defined access list (ACL) to an interface.

- **`permit - MAC`** - Specifies the packets to be forwarded based on the MAC address and the associated parameters.
- **`deny - MAC`** - Specifies the packets to be rejected based on the MAC address and the associated parameters.

47.1.20 permit- ospf/pim/protocol type – ipv6

Command Objective	This command permits packets of a particular protocol if the conditions defined in the permit statement are matched.
Syntax	**permit [{ospf | pim | <protocol-type (0-255)>}] {any | host <src-ipv6-addr>} [/ <src-prefix-len (0-128)>] {any | host <dst-ipv6-addr>} [/ <dst-prefix-len (0-128)>] [dscp <value (0-63)>] [flow-label <value (0-1048575)>] [priority <value (1-7)>]**
Parameter Description	• **ospf** – Permits packets for OSPF protocol. • **pim** – Permits packets for PIM protocol. • **<protocol-type (1-255)> –** Permits packets for the specified protocol number. This value ranges from 1 to 255. • **any** - Permits packets of the specified protocol from all host IPv6 address. • **host <src-ipv6-addr>** - Permits packets of the specified protocol from specified host IPv6 address. • **<src-prefix-len (0-128**)> - Configures the prefix length for the source IPv6 address. This value ranges from 0 and 128. • **any** - Permits packets of the specified protocol from all destination IPv6 addresses • **host < dst-ipv6-addr>** - Permits packets of the specified protocol from specified destination IPv6 address • **<dst-prefix-len (0-128)>** - Configures the prefix length for the destination IPv6 address. This value ranges from 0 and 128. • **dscp <value (0-63)>** – Configures the Differentiated Services Code Point (DSCP) value which provides the quality of service control. This value ranges from 0 to 63. • **priority <(1-7)>**– Configures the priority value of the L3 filter to be used when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 7.
Mode	ACL Extended Access List Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro

Defaults	• protocol type - 255 • priority - 1 • dscp -1
Example	**SEFOS (config-ipv6-acl)# permit ospf host 1111::2222 / 128 any dscp 0 flow-label 104857 priority 5**
Related Command(s)	• **ipv6 access-list extended** - Creates IPv6 access list and enters the IPv6 access list configuration mode. • **show access-lists –** Displays the access list statistics.

47.1.21 deny- ospf/pim/protocol type– ipv6

Command Objective	This command discards packets of the specified protocol if the conditions defined in the permit statement are matched.
Syntax	**deny [{ospf | pim | <protocol-type (0-255)>}] {any | host <src-ipv6-addr>} [/ <src-prefix-len (0-128)>] {any | host <dst-ipv6-addr>} [/ <dst-prefix-len (0-128)>] [dscp <value (0-63)>] [flow-label <value (0-1048575)>] [priority <value (1-7)>]**
Parameter Description	• **ospf** – Discards packets for OSPF protocol. • **pim** – Discards packets for PIM protocol. • **<protocol-type (1-255)> -** Discards packets for the specified protocol number. This value ranges from 1 to 255. • **any** - Discards packets of the specified protocol from all host IPv6 addresses. • **host <src-ipv6-addr>** - Discards packets of the specified protocol from specified host IPv6 address. • **<src-prefix-len (0-128**)> - Configures the prefix length for the source IPv6 address. This value ranges from 0 and 128. • **any** - Permits packets of the specified protocol from all destination IPv6 addresses. • **host < dst-ipv6-addr>** - Discards packets of the specified protocol from specified destination IPv6 address. • **<dst-prefix-len (0-128)>** - Discards the prefix length for the destination IPv6 address. This value ranges from 0 and 128. • **dscp <value (0-63)>** – Configures the Differentiated Services Code Point (DSCP) value which provides the quality of service control. This value ranges from 0 to 63. • **priority <(1-7)>**– Configures the priority value of the L3 filter to be used when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 7.
Mode	ACL Extended Access List Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro

Defaults	• protocol type - 255 • priority - 1 • dscp - 1
Example	**SEFOS(config-ipv6-acl)# deny ospf host 1111::2222 / 128 any dscp 0 flow-label 104857 priority 5**
Related Command(s)	• **ipv6 access-list extended** - Creates IPv6 access list and enters the IPv6 access list configuration mode. • **show access-lists –** Displays the access list statistics.

47.1.22 permit tcp– ipv6

Command Objective	This command specifies the TCP packets to be forwarded based on the associated parameters.
Syntax	**permit tcp {any | host <src-ipv6-addr>} [<src-prefix-len (0-128)>] [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <start-port-range (1-65535)> <end-port-range (1-65535)>}] {any | host <dst-ipv6-addr>} [<dst-prefix-len (0-128)>] [{ gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <start-port-range (1-65535)> <end-port-range (1-65535)>}] [{ ack | rst }] [{tos {max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp <value (0-63)>}] [flow-label <value (0-1048575)>] [priority <value (1-7)>]**
Parameter Description	• **any|host < src-ipv6-addr > <integer(0-128)>** - Permits traffic with the specified source IPv6 address. The source IPv6 address can be: ▪ **any** - Permits the traffic from any source. ▪ **host < src-ipv6-addr >** - Permits packets with the specified host source IPv6 address. • **< src-prefix-len (0-128)>** - Specifies the prefix length of the source IPv6 address. This value ranges from 0 to 128. • **gt <port-number (1-65535)>** - Permits only the UDP control packets having the TCP source port numbers greater than the specified port number. This value ranges from 1 to 65535. • **lt <port-number (1-65535)>** - Permits only the UDP control packets having the UDP source port numbers lesser than the specified port number. This value ranges from 1 to 65535. • **eq <port-number (1-65535)>** - Permits only the UDP control packets having the specified UDP source port numbers. This value ranges from 1 to 65535. • **range <start-port-range (1-65535)> <end-port-range (1-65535)>** - Permits the UDP control packets having the UDP source port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values. • **any| host <dst-ipv6-addr>} –** Permits traffic with the specified destination IPv6 address. The destination IPv6 address can be: ▪ **any –** Permits packets with any destination address.

- **host <dst-ipv6-addr>**- Permits packets with the specified host destination IPv6 address.

- **<dst-prefix-len (0-128)> -** Specifies the prefix length of the destination IPv6 address. This value ranges from 0 to 128.

- **gt <port-number (1-65535)>** - Permits the UDP control packets having the TCP source port numbers greater than the specified port number. This value ranges from 1 to 65535.

- **lt <port-number (1-65535)>** - Permits the UDP control packets having the UDP source port numbers lesser than the specified port number. This value ranges from 1 to 65535.

- **eq <port-number (1-65535)>** - Permits the UDP control packets having the specified UDP source port numbers. This value ranges from 1 to 65535.

- **range <start-port-range (1-65535)> <end-port-range (1-65535)>** - Permits the UDP control packets having the UDP source port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values.

- **ack** - Configures the TCP ACK bit to be checked against the packet.

- **rst** - Configures the TCP RST bit to be checked against the packet.

- **tos** - Permits the protocol packets based on the following Type Of Service configurations:
  - **max-reliability** - Permits the protocol packets having TOS field set as high reliability.
  - **max-throughput** - Permits the protocol packets having TOS field set as high throughput.
  - **min-delay –** Permits the protocol packets having TOS field set as low delay.
  - **normal** - Permits all protocol packets. Does not check for the TOS field in the packets.
  - **<value (0-7)>** - Permits the protocol packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS.
    - **0** - Permits all protocol packets. Does not check for the TOS field in the packets.
    - **1** - Permits the protocol packets having TOS field set as high reliability.
    - **2** - Permits the protocol packets having TOS field set as high throughput.
    - **3** - Permits the protocol packets having TOS field set either as high reliability or high throughput.

	▪ **4** - Permits the protocol packets having TOS field set as low delay. ▪ **5** - Permits the protocol packets having TOS field set either as low delay or high reliability. ▪ **6** - Permits the protocol packets having TOS field set either as low delay or high throughput. ▪ **7** - Permits the protocol packets having TOS field set either as low delay, high reliability, or high throughput. • **dscp <value (0-63)>** - Configures the Differentiated Services Code Point value to be checked against the packet. This value provides the quality of service control. This value ranges from 0 to 63. • **flow-label <value (0-1048575)>** - Configures the flow label value. This value ranges from 0 to 1048575. • **priority <(1-7)>**– Configures the priority value of the L3 filter to be used when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 7.
Mode	ACL Extended Access List Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	• priority - 1 • dscp - 1
Example	**SEFOS(config-ipv6-acl)# permit tcp host 1111::2222 128 gt 1 any lt 1** **SEFOS (config-ipv6-acl)# permit tcp host 1111::2222 128 gt 1 any lt 1 rst dscp 1 flow-label 1048575 priority 7**
Related Command(s)	• **ipv6 access-list extended** - Creates IPv6 access list and enters the IPv6 access list configuration mode. • **show access-lists –** Displays the access list statistics.

47.1.23 deny- tcp– ipv6

Command Objective	This command specifies the TCP packets to be rejected based on the associated parameters.
Syntax	**deny tcp {any | host <src-ipv6-addr>} [<src-prefix-len (0-128)>] [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <start-port-range (1-65535)> <end-port-range (1-65535)>}] {any | host <dst-ipv6-addr>} [<dst-prefix-len (0-128)>] [{ gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <start-port-range (1-65535)> <end-port-range (1-65535)>}] [{ ack | rst }] [{tos {max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp <value (0-63)>}] [flow-label <value (0-1048575)>] [priority <value (1-7)>]**
Parameter Description	• **any|host < src-ipv6-addr > <integer(0-128)>** - Denies traffic with the specified source IPv6 address. The source IPv6 address can be: ▪ **any** - Denies the traffic from any source. ▪ **host < src-ipv6-addr >** - Denies packets with the specified host source IPv6 address • **< src-prefix-len (0-128)>** - Specifies the prefix length of the source IPv6 address. This value ranges from 0 to 128. • **gt <port-number (1-65535)>** - Denies only the TCP control packets having the TCP source port numbers greater than the specified port number. This value ranges from 1 to 65535. • **lt <port-number (1-65535)>** - Denies only the TCP control packets having the UDP source port numbers lesser than the specified port number. This value ranges from 1 to 65535. • **eq <port-number (1-65535)>** - Denies only the TCP control packets having the specified UDP source port numbers. This value ranges from 1 to 65535. • **range <start-port-range (1-65535)> <end-port-range (1-65535)>** - Denies only the UDP control packets having the TCP source port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values. • **any| host <dst-ipv6-addr>} -** Denies traffic with the specified destination IPv6 address. The destination IPv6 address can be: ▪ **any -** Denies packets with any destination address.

- **host <dst-ipv6-addr>**- Denies packets with the specified host destination IPv6 address.

- **<dst-prefix-len (0-128)> -** Specifies the prefix length of the destination IPv6 address. This value ranges from 0 to 128.

- **gt <port-number (1-65535)>** - Denies the UDP control packets having the TCP source port numbers greater than the specified port number. This value ranges from 1 to 65535.

- **lt <port-number (1-65535)>** - Denies the UDP control packets having the TCP source port numbers lesser than the specified port number. This value ranges from 1 to 65535.

- **eq <port-number (1-65535)>** - Denies the UDP control packets having the specified TCP source port numbers. This value ranges from 1 to 65535.

- **range <start-port-range (1-65535)> <end-port-range (1-65535)>** - Denies the TCP control packets having the UDP source port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values.

- **ack** - Configures the TCP ACK bit to be checked against the packet.

- **rst** - Configures the TCP RST bit to be checked against the packet.

- **tos** - Denies the protocol packets based on the following Type Of Service configurations:
  - **max-reliability** - Denies the protocol packets having TOS field set as high reliability.
  - **max-throughput** - Denies the protocol packets having TOS field set as high throughput.
  - **min-delay –** Denies the protocol packets having TOS field set as low delay.
  - **normal** - Denies all protocol packets. Does not check for the TOS field in the packets.
  - **<value (0-7)>** - Denies the protocol packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS.
    - **0** - Denies all protocol packets. Does not check for the TOS field in the packets.
    - **1** - Denies the protocol packets having TOS field set as high reliability.
    - **2** - Denies the protocol packets having TOS field set as high throughput.
    - **3** - Denies the protocol packets having TOS field set either as high reliability or high throughput.

	▪ **4** - Denies the protocol packets having TOS field set as low delay. ▪ **5** - Denies the protocol packets having TOS field set either as low delay or high reliability. ▪ **6** - Denies the protocol packets having TOS field set either as low delay or high throughput. ▪ **7** - Denies the protocol packets having TOS field set either as low delay, high reliability, or high throughput. • **dscp <value (0-63)>** - Configures the Differentiated Services Code Point value to be checked against the packet. This value provides the quality of service control. This value ranges from 0 to 63. • **flow-label <value (0-1048575)>** - Configures the flow label value. This value ranges from 0 to 1048575. • **priority <(1-7)>**– Configures the priority value of the L3 filter to be used when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 7.
Mode	ACL Extended Access List Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	• priority - 1 • dscp - 1
Example	**SEFOS(config-ipv6-acl)# deny tcp host 1111::2222 128 gt 1 any lt 1** **SEFOS (config-ipv6-acl)# deny tcp host 1111::2222 128 gt 1 any lt 1 rst dscp 1 flow-label 1048575 priority 7**
Related Command(s)	• **ipv6 access-list extended** - Creates IPv6 access list and enters the IPv6 access list configuration mode. • **show access-lists –** Displays the access list statistics.

47.1.24 permit udp– ipv6

Command Objective	This command specifies the UDP packets to be forwarded based on the associated parameters.
Syntax	**permit udp {any | host <src-ipv6-addr>} [<src-prefix-len (0-128)>] [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <start-port-range (1-65535)> <end-port-range (1-65535)>}] {any | host <dst-ipv6-addr>} [<dst-prefix-len (0-128)>] [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <start-port-range (1-65535)> <end-port-range (1-65535)>}] [dscp <value (0-63)>] [flow-label <value (0-1048575)>] [priority <value (1-7)>]**
Parameter Description	• **any|host < src-ipv6-addr > <integer(0-128)>** - Permits traffic with the specified source IPv6 address. The source IPv6 address can be: ▪ **any** - Permits the traffic from any source. ▪ **host < src-ipv6-addr >** - Permits packets with the specified host source IPv6 address. • **< src-prefix-len (0-128)>** - Specifies the prefix length of the source IPv6 address. This value ranges from 0 to 128. • **gt <port-number (1-65535)>** - Permits only the UDP control packets having the TCP source port numbers greater than the specified port number. This value ranges from 1 to 65535. • **lt <port-number (1-65535)>** - Permits only the UDP control packets having the UDP source port numbers lesser than the specified port number. This value ranges from 1 to 65535. • **eq <port-number (1-65535)>** - Permits only the UDP control packets having the specified UDP source port numbers. This value ranges from 1 to 65535. • **range <start-port-range (1-65535)> <end-port-range (1-65535)>** - Permits the UDP control packets having the UDP source port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values. • **any| host <dst-ipv6-addr>} –** Permits traffic with the specified destination IPv6 address. The destination IPv6 address can be: ▪ **any –** Permits packets with any destination address. ▪ **host <dst-ipv6-addr>**- Permits packets with the specified host destination IPv6 address.

- **<dst-prefix-len (0-128)> –** Specifies the prefix length of the destination IPv6 address. This value ranges from 0 to 128.
- **gt <port-number (1-65535)>** - Permits the UDP control packets having the TCP source port numbers greater than the specified port number. This value ranges from 1 to 65535.
- **lt <port-number (1-65535)>** - Permits the UDP control packets having the UDP source port numbers lesser than the specified port number. This value ranges from 1 to 65535.
- **eq <port-number (1-65535)>** - Permits the UDP control packets having the specified UDP source port numbers. This value ranges from 1 to 65535.
- **range <start-port-range (1-65535)> <end-port-range (1-65535)>** - Permits the UDP control packets having the UDP source port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values.
- **ack** - Configures the TCP ACK bit to be checked against the packet.
- **rst** - Configures the TCP RST bit to be checked against the packet.
- **tos** - Permits the protocol packets based on the following Type Of Service configurations:
  - **max-reliability** - Permits the protocol packets having TOS field set as high reliability.
  - **max-throughput** - Permits the protocol packets having TOS field set as high throughput.
  - **min-delay –** Permits the protocol packets having TOS field set as low delay.
  - **normal** - Permits all protocol packets. Does not check for the TOS field in the packets.
  - **<value (0-7)>** - Permits the protocol packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS.
    - **0** - Permits all protocol packets. Does not check for the TOS field in the packets.
    - **1** - Permits the protocol packets having TOS field set as high reliability.
    - **2** - Permits the protocol packets having TOS field set as high throughput.
    - **3** - Permits the protocol packets having TOS field set either as high reliability or high throughput.
    - **4** - Permits the protocol packets having TOS field set as low delay.
    - **5** - Permits the protocol packets having TOS field set either as low

	delay or high reliability. ▪ **6** - Permits the protocol packets having TOS field set either as low delay or high throughput. ▪ **7** - Permits the protocol packets having TOS field set either as low delay, high reliability, or high throughput. • **dscp <value (0-63)>** - Configures the Differentiated Services Code Point value to be checked against the packet. This value provides the quality of service control. This value ranges from 0 to 63. • **flow-label <value (0-1048575)>** - Configures the flow label value. This value ranges from 0 to 1048575. • **priority <(1-7)>**– Configures the priority value of the L3 filter to be used when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 7.
Mode	ACL Extended Access List Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	• priority - 1 • dscp - 1
Example	**SEFOS(config-ipv6-acl)# permit udp host 1111::2222 128 gt 1 any lt 1 dscp 6 flow-label 1048575 priority 7**
Related Command(s)	• **ipv6 access-list extended** - Creates IPv6 access list and enters the IPv6 access list configuration mode. • **show access-lists –** Displays the access list statistics.

47.1.25 deny udp– ipv6

Command Objective	This command specifies the UDP packets to be rejected based on the associated parameters.
Syntax	**deny udp {any | host <src-ipv6-addr>} [<src-prefix-len (0-128)>] [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <start-port-range (1-65535)> <end-port-range (1-65535)>}] {any | host <dst-ipv6-addr>} [<dst-prefix-len (0-128)>] [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <start-port-range (1-65535)> <end-port-range (1-65535)>}] [dscp <value (0-63)>] [flow-label <value (0-1048575)>] [priority <value (1-7)>]**
Parameter Description	• **any|host < src-ipv6-addr > <integer(0-128)>** - Denies traffic with the specified source IPv6 address. The source IPv6 address can be: ▪ **any** - Denies the traffic from any source. ▪ **host < src-ipv6-addr >** - Denies packets with the specified host source IPv6 address • **< src-prefix-len (0-128)>** - Specifies the prefix length of the source IPv6 address. This value ranges from 0 to 128. • **gt <port-number (1-65535)>** - Denies only the TCP control packets having the TCP source port numbers greater than the specified port number. This value ranges from 1 to 65535. • **lt <port-number (1-65535)>** - Denies only the TCP control packets having the UDP source port numbers lesser than the specified port number. This value ranges from 1 to 65535. • **eq <port-number (1-65535)>** - Denies only the TCP control packets having the specified UDP source port numbers. This value ranges from 1 to 65535. • **range <start-port-range (1-65535)> <end-port-range (1-65535)>** - Denies only the UDP control packets having the TCP source port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values. • **any| host <dst-ipv6-addr>} -** Denies traffic with the specified destination IPv6 address. The destination IPv6 address can be: ▪ **any -** Denies packets with any destination address. ▪ **host <dst-ipv6-addr>** - Denies packets with the specified host destination IPv6 address.

- **<dst-prefix-len (0-128)> –** Specifies the prefix length of the destination IPv6 address. This value ranges from 0 to 128.
- **gt <port-number (1-65535)>** - Denies the UDP control packets having the TCP source port numbers greater than the specified port number. This value ranges from 1 to 65535.
- **lt <port-number (1-65535)>** - Denies the UDP control packets having the TCP source port numbers lesser than the specified port number. This value ranges from 1 to 65535.
- **eq <port-number (1-65535)>** - Denies the UDP control packets having the specified TCP source port numbers. This value ranges from 1 to 65535.
- **range <start-port-range (1-65535)> <end-port-range (1-65535)>** - Denies the TCP control packets having the UDP source port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values.
- **ack** - Configures the TCP ACK bit to be checked against the packet.
- **rst** - Configures the TCP RST bit to be checked against the packet.
- **tos** - Denies the protocol packets based on the following Type Of Service configurations:
  - **max-reliability** - Denies the protocol packets having TOS field set as high reliability.
  - **max-throughput** - Denies the protocol packets having TOS field set as high throughput.
  - **min-delay –** Denies the protocol packets having TOS field set as low delay.
  - **normal** - Denies all protocol packets. Does not check for the TOS field in the packets.
  - **<value (0-7)>** - Denies the protocol packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS.
    - **0** - Denies all protocol packets. Does not check for the TOS field in the packets.
    - **1** - Denies the protocol packets having TOS field set as high reliability.
    - **2** - Denies the protocol packets having TOS field set as high throughput.
    - **3** - Denies the protocol packets having TOS field set either as high reliability or high throughput.
    - **4** - Denies the protocol packets having TOS field set as low delay.
    - **5** - Denies the protocol packets having TOS field set either as low

	delay or high reliability. ▪ **6** - Denies the protocol packets having TOS field set either as low delay or high throughput. ▪ **7** - Denies the protocol packets having TOS field set either as low delay, high reliability, or high throughput. • **dscp <value (0-63)>** - Configures the Differentiated Services Code Point value to be checked against the packet. This value provides the quality of service control. This value ranges from 0 to 63. • **flow-label <value (0-1048575)>** - Configures the flow label value. This value ranges from 0 to 1048575. • **priority <(1-7)>** – Configures the priority value of the L3 filter to be used when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 7.
Mode	ACL Extended Access List Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	• priority - 1 • dscp - 1
Example	**SEFOS(config-ipv6-acl)# deny udp host 1111::2222 128 gt 1 any lt 1 dscp 6 flow-label 1048575 priority 7**
Related Command(s)	• **ipv6 access-list extended** - Creates IPv6 access list and enters the IPv6 access list configuration mode. • **show access-lists –** Displays the access list statistics.

47.1.26 permit icmp– ipv6

Command Objective	This command specifies the ICMP packets to be forwarded based on the IP address and the associated parameters.
Syntax	**permit icmp {any | host <src-ipv6-addr>} [/ <src-prefix-len (0-128)>] {any | host <dst-ipv6-addr>} [/<dst-prefix-len (0-128)>]** [message-type <message-type (0-255)> message-code <message-code (0-255)>] **[dscp <value (0-63)>] [flow-label <value (0-1048575)>] [priority <value (1-7)>]**
Parameter Description	• **any | host <src-ipv6-addr>** - Permits the ICMPv6 packet with the specified source IPv6 address. The sources are: ▪ **any -** Permits ICMPv6 packets from any source. ▪ **host <src-ipv6-addr>** - Permits ICMPv6 packets with the specified host source IPv6 address. • **/ <src-prefix-len (0-128)> -** Specifies the prefix length of the source IPv6 address. This value ranges from 0 to 128. • **any | host <dst-ipv6-addr>** - Permits the ICMPv6 packet with the specified source IPv6 address. The sources are: ▪ **any -** Permits ICMPv6 packets from any destination. ▪ **host < dst-ipv6-addr >** - Permits ICMPv6 packets with the specified host destination IPv6 address. • **/<dst-prefix-len (0-128)> -** Specifies the prefix length of the destination IPv6 address. This value ranges from 0 to 128. • **message-type <message-type (0-255)> -** Configures the ICMPv6 message type to be checked against the packet. The packet will be allowed if it matches the message type. This value ranges from 0 to 255. Some of the ICMPv6 message types are:

Value	ICMP Message type
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo Request
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request

16	Information Reply
17	Address Mask Request
18	Address Mask Reply
255	No ICMP type

- **message-code <message-code (0-255)>-** Configures the ICMPv6 message code to be checked against the packet. The packet is allowed if it matches the message code. This value ranges from 0 to 255. Some of the ICMPv6 message codes are:

Value	ICMP code
0	Network Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
4	Fragment Need
5	Source Route Fail
6	Destination Network Unknown
7	Destination Host Unknown
8	Source Host Isolated
9	Destination Network Administratively Prohibited
10	Destination Host Administratively Prohibited
11	Network Unreachable TOS
12	Host Unreachable TOS
255	No ICMP Code

- **dscp <value (0-63)> –** Configures the Differentiated Services Code Point value to be checked against the packet. This value provides the quality of service control. This value ranges from 0 to 63.

- **flow-label <value(0-1048575)>** - Configures the flow identifier in the IPv6 header. This value ranges from 0 to 1048575.

- **priority < value(1-7)>** - Configures the priority of the L3 filter to decide in which order the filter rule is applicable when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 7.

Mode ACL Extended Access List Configuration Mode

Package Workgroup, Enterprise, Metro_E, and Metro

Defaults

- priority - 1
- dscp – 1
- message-type / message code - 255

Example	**SEFOS(config-ipv6-acl)# permit icmp host 1111::2222 / 128 host 1111::3333 / 126 256 255 dscp 63 flow-label 1048575 priority 7**
Related Command(s)	• **ipv6 access-list extended** - Creates IPv6 access list and enters the IPv6 access list configuration mode. • **show access-lists -** Displays the access list statistics.

47.1.27 deny icmp– ipv6

Command Objective	This command specifies the ICMP packets to be rejected based on the IP address and associated parameters.
Syntax	**deny icmp {any | host <src-ipv6-addr>} [/<src-prefix-len (0-128)>] {any | host <dst-ipv6-addr>} [/<dst-prefix-len (0-128)>]** [message-type <message-type (0-255)> message-code <message-code (0-255)>] **[dscp <value (0-63)>] [flow-label <value (0-1048575)>] [priority <value (1-7)>]**
Parameter Description	• **any | host <src-ipv6-addr>** - Denies the ICMPv6 packet with the specified source IPv6 address. The sources are: ▪ **any -** Denies ICMPv6 packets from any source. ▪ **host <src-ipv6-addr>** - Denies ICMPv6 packets with the specified host source IPv6 address. • **/ <src-prefix-len (0-128)> -** Denies the prefix length of the source IPv6 address. This value ranges from 0 to 128. • **any | host <dst-ipv6-addr>** - Denies the ICMPv6 packet with the specified source IPv6 address. The sources are: ▪ **any -** Denies ICMPv6 packets from any destination. ▪ **host < dst-ipv6-addr >** - Denies ICMPv6 packets with the specified host destination IPv6 address . • **/<dst-prefix-len (0-128)> -** Specifies the prefix length of the destination IPv6 address. This value ranges from 0 to 128. • **message-type <message-type (0-255)>** - Configures the ICMPv6 message type to be checked against the packet. The packet will be allowed if it matches the message type. This value ranges from 0 to 255. Some of the ICMPv6 message types are:

Value	ICMP Message type
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo Request
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request

16	Information Reply
17	Address Mask Request
18	Address Mask Reply
255	No ICMP type

- **message-code <message-code (0-255)>** - Configures the ICMPv6 message code to be checked against the packet. The packet is allowed if it matches the message code. This value ranges from 0 to 255. Some of the ICMPv6 message codes are:

Value	ICMP code
0	Network Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
4	Fragment Need
5	Source Route Fail
6	Destination Network Unknown
7	Destination Host Unknown
8	Source Host Isolated
9	Destination Network Administratively Prohibited
10	Destination Host Administratively Prohibited
11	Network Unreachable TOS
12	Host Unreachable TOS
255	No ICMP Code

- **dscp <value (0-63)> –** Configures the Differentiated Services Code Point value to be checked against the packet. This value provides the quality of service control. This value ranges from 0 to 63.

- **flow-label <value(0-1048575)>** - Configures the flow identifier in the IPv6 header. This value ranges from 0 to 1048575.

- **priority < value(1-7)>** - Configures the priority of the L3 filter to decide in which order the filter rule is applicable when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 7.

Mode ACL Extended Access List Configuration Mode

Package Workgroup, Enterprise, Metro_E, and Metro

Defaults

- priority - 1
- dscp – 1
- message-type / message code - 255

Example	**SEFOS(config-ipv6-acl)# deny icmp host 1111::2222 / 128 host 1111::3333 / 126 255 255 dscp 63 flow-label 1048575 priority 7**
Related Command(s)	• **ipv6 access-list extended** - Creates IPv6 access list and enters the IPv6 access list configuration mode. • **show access-lists -** Displays the access list statistics.

47.2 aclmet

CLI commands in this Fulcrum sub-category are listed below:

47.2.1 ip access-list

Command Objective	This command creates IP access list and enters the IP access list configuration mode. ACLs on the system perform both access control and Layer 3 field classification. To define Layer 3 fields' access lists the `ip access-list` command is used. The no form of the command deletes the IP access list.
Syntax	**`ip access-list {standard <access-list-number (1-1000)> | extended <access-list-number (1001-65535)> }`** **`no ip access-list {standard <access-list-number (1-1000)> | extended <access-list-number (1001-65535)> }`**
Parameter Description	• **`standard <access-list-number (1-1000)>`** - Configures the standard access list number. Standard access lists create filters based on IP address and network mask (L3 filters). This value ranges from 1 to 1000. • **`extended <access-list-number (1001-65535)>`** - Configures the extended access list number. Extended access lists enable specification of filters based on the type of protocol, range of TCP or UDP ports, as well as the IP address and network mask (Layer 4 filters). This value ranges from 1001 to 65535.
Mode	Global Configuration Mode
Package	Metro_E and Metro
Example	**`SEFOS (config)# ip access-list standard 1`**
Related Command(s)	• **`permit - standard mode -`** Specifies the packets to be forwarded depending upon the associated parameters. • **`deny - standard mode -`** Denies traffic if the conditions defined in the deny statement are matched. • **`permit- ip/ospf/pim/protocol type -`** Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched. • **`deny - ip/ospf/pim/protocol type`** - Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched. • **`copy-to-cpu - ip / ospf / pim / protocol-type`** - Copies the IP control packets of all type of protocols to control plane CPU, with or without the switching of packets based on the configured parameters.

- **`permit tcp -`** Specifies the TCP packets to be forwarded based on the associated parameters.
- **`deny tcp -`** Specifies the TCP packets to be rejected based on the associated parameters.
- **`permit udp -`** Specifies the UDP packets to be forwarded based on the associated parameters.
- **`deny udp -`** Specifies the UDP packets to be rejected based on the associated parameters.
- **`permit icmp -`** Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters.
- **`deny icmp -`** Specifies the ICMP packets to be rejected based on the IP address and associated parameters.
- **`ip access-group -`** Enables access control for the packets on the interface.
- **`show access-lists -`** Displays the access list configuration.

47.2.2 mac access-list extended

Command Objective	This command creates Layer 2 MAC ACLs, that is, this command creates a MAC access list and returns the MAC access list configuration mode to the user. This value ranges between 1 and 65535. The no form of the command deletes the MAC access list.
Syntax	**mac access-list extended <access-list-number (1-65535)>** **no mac access-list extended <short (1-65535)>**
Mode	Global Configuration Mode
Package	Metro_E and Metro
Example	**SEFOS (config)# mac access-list extended 5**
Related Command(s)	• **mac access-group –** Applies a MAC access control list (ACL) to a Layer 2 interface. • **permit – MAC** - Specifies the packets to be forwarded based on the MAC address and the associated parameters. • **deny – MAC** - Specifies the packets to be rejected based on the MAC address and the associated parameters. • **show access-lists –** Displays the access lists' configuration.

47.2.3 permit - standard mode

Command Objective	This command permits the packets to be forwarded depending upon the associated parameters. Standard IP access lists use source addresses for matching operations.
Syntax	**permit { any | host <src-ip-address> | <network-src-ip> <mask> } [{ any | host <dest-ip-address> | <network-dest-ip> <mask> }]**
Parameter Description	• **any|host <src-ip-address>| < src-ip-address> <mask>** - Permits traffic with the specified source address. The sources are: ▪ **any –** Permits packets from any source. ▪ **host <src-ip-address>** - Permits packets with the specified host source IPv4 address. ▪ **<network-src-ip> <mask>** - Permits packets with the specified source IP address and the network mask to be used with the source IP address. • **any|host <dest-ip-address>| < dest-ip-address > <mask>** - Permits traffic with the specified destination address. The destination can be: ▪ **any –** Permits the packets with any destination. ▪ **host <dest-ip-address>** - Permits packets with the specified host destination IPv4 address. ▪ **<network-dest-ip> <mask>** - Permits packets with the specified destination IP address and the network mask for the given destination IP address.
Mode	IP ACL Configuration (standard)
Package	Metro_E and Metro
Example	**SEFOS(config-std-nacl)# permit host 100.0.0.10 host 10.0.0.1**
Related Command(s)	• **ip access-list –** Creates IP ACLs and enters the IP access list configuration mode. • **deny - standard mode –** Denies traffic if the conditions defined in the deny statement are matched. • **show access-lists –** Displays the access list configuration.

47.2.4 deny - standard mode

Command Objective	This command denies packets if the conditions defined in the deny statement are matched.
Syntax	**deny{ any | host <src-ip-address> | <network-src-ip> <mask> } [{ any | host <dest-ip-address> | <network-dest-ip> <mask> }]**
Parameter Description	• **any|host <src-ip-address>| <network-src-ip><mask>** - Denies traffic with the specified source address. The sources are: ▪ **any –** Denies packets from any source. ▪ **host <src-ip-address>** - Denies packets with the specified host source IPv4 address. ▪ **<network-src-ip> <mask>** - Denies packets with the specified source IP address and the network mask to be used with the source IP address. • **any|host <dest-ip-address>| <network-dest-ip> <mask>** - Denies traffic with the specified destination address. The destination can be: ▪ **any –** Denies the packets with any destination. ▪ **host <dest-ip-address>** - Denies packets with the specified host destination IPv4 address. ▪ **<network-dest-ip> <mask>** - Denies packets with the specified destination IP address and the network mask for the given destination IP address.
Mode	IP ACL Configuration (standard)
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS(config-std-nacl)# deny host 100.0.0.10 any**
Related Command(s)	• **ip access-list –** Creates IP ACLs and enters the IP access list configuration mode. • **permit – standard mode –** Specifies the packets to be forwarded depending upon the associated parameters. • **show access-lists –** Displays the access list configuration.

47.2.5 permit- ip/ospf/pim/protocol type

Command Objective	This command allows traffic for the specified protocol packet if the conditions defined in the permit statement are matched.
Syntax	**permit { ip | ospf | pim | <protocol-type (1-255)>} { any | host <src-ip-address> | <src-ip-address> <mask>} { any | host <dest-ip-address> | <dest-ip-address> <mask> } [{tos{max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp <value (0-63)>}] [priority <value (1-255)>] [svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [cvlan-id <vlan-id (1-4094)>] [cvlan-priority <value (0-7)>] [{ single-tag | double-tag }]**
Parameter Description	• **ip** - Allows IP protocol packets. • **ospf** - Allows OSPF protocol packets. • **pim** - Allows PIM protocol packets. • **<protocol-type (1-255)>** - Configures the type of protocol to be checked against the packet. It can also be a protocol number. Note: Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed. • **any|host <src-ip-address>| < src-ip-address> <mask>** - Permits traffic with the specified source address. The sources are: ▪ **any –** Permits packets from any source. ▪ **host <src-ip-address>** - Permits packets with the specified host source IPv4 address. ▪ **<src-ip-address> <mask>** - Permits packets with the specified source IP address and the network mask to be used with the source IP address. • **any|host <dest-ip-address>| < dest-ip-address > <mask>** - Permits traffic with the specified destination address. The destination can be: ▪ **any –** Permits the packets with any destination. ▪ **host <dest-ip-address>** - Permits packets with the specified host destination IPv4 address. ▪ **<dest-ip-address> <mask>** - Permits packets with the specified destination IP address and the network mask for the given destination IP address. • **tos** - Allows the protocol packets based on the following Type Of Service

configurations:

- **max-reliability** - Allows the protocol packets having TOS field set as high reliability.
- **max-throughput** - Allows the protocol packets having TOS field set as high throughput.
- **min-delay –** Allows the protocol packets having TOS field set as low delay.
- **normal** - Allows all protocol packets. Does not check for the TOS field in the packets.
- **<value (0-7)>** - Allows the protocol packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS.
  - **0** - Allows all protocol packets. Does not check for the TOS field in the packets.
  - **1** - Allows the protocol packets having TOS field set as high reliability.
  - **2** - Allows the protocol packets having TOS field set as high throughput.
  - **3** - Allows the protocol packets having TOS field set either as high reliability or high throughput.
  - **4** - Allows the protocol packets having TOS field set as low delay.
  - **5** - Allows the protocol packets having TOS field set either as low delay or high reliability.
  - **6** - Allows the protocol packets having TOS field set either as low delay or high throughput.
  - **7** - Allows the protocol packets having TOS field set either as low delay, high reliability, or high throughput.

- **dscp <value (0-63)>** - Configures the Differentiated Services Code Point value to be checked against the packet. This value provides the quality of service control. This value ranges from 0 to 63.

- **priority <value (1-255)>** - Configures the priority of the L3 filter to decide in which order the filter rule is applicable when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 255.

- **svlan-id <vlan-id (1-4094)>**- Configures the Service VLAN value to match against incoming packets. This value ranges from 1 to 4094.

- **svlan-priority <value (0-7)>**- Configures the Service VLAN priority value to match against incoming packets. This value ranges from 0 to 7.

- **cvlan-id <vlan-id (1-4094)>**- Configures Customer VLAN value to match against incoming packets. This value ranges from 1 to 4094.

- **cvlan-priority <value (0-7)>**- Configures Customer VLAN priority value to match against incoming packets. This value ranges from 0 to 7.

	• **single-tag** - Specifies that the filter is to be applied on single VLAN tagged packets. • **double-tag** - Specifies that the filter is to be applied on double VLAN tagged packets.
Mode	ACL Extended Access List Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	• protocol-type - 255 • priority - 1 • dscp - -1 • svlan-id - 0 • svlan-priority - -1 • cvlan-id - 0 • cvlan-priority - -1 • single-tag | double-tag - Single tag • precedence - 1
Note:	• Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed. • Service VLAN, Service VLAN Priority, Customer VLAN, and Customer VLAN Priority options are applicable only for Metro Solution, when the bridge mode is “Provider Bridge”.
Example	**SEFOS (config-ext-nacl)# permit 200 host 100.0.0.10 any tos 6 load balance src-ip**
Related Command(s)	• **ip access-list –** Creates IP ACLs and enters the IP access list configuration mode. • **deny – ip/ospf/pim/protocol type –** Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched. • **show access-lists –** Displays the access list configuration.

47.2.6 deny - ip/ospf/pim/protocol type

Command Objective	This command denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched.
Syntax	**deny { ip | ospf | pim | <protocol-type (1-255)>} { any | host <src-ip-address> | <src-ip-address> <mask> } { any | host <dest-ip-addresq> | <dest-ip-address> <mask> } [{tos{max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp <value (0-63)>}] [priority <value (1-255)>] [svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [cvlan-id <vlan-id (1-4094)>] [cvlan-priority <value (0-7)>] [{ single-tag | double-tag }]**
Parameter Description	• **ip** - Denies P protocol packets. • **ospf** - Denies OSPF protocol packets. • **pim** - Denies PIM protocol packets. • **<protocol-type (1-255)>** - Denies the packets for the specified protocol number. This value ranges from 1 to 255. Note: Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed. • **any|host <src-ip-address>| < src-ip-address> <mask>** - Denies traffic with the specified source address. The sources are: ▪ **any –** Denies packets from any source. ▪ **host <src-ip-address>** - Denies packets with the specified host source IPv4 address. ▪ **<src-ip-address> <mask>** - Denies packets with the specified source IP address and the network mask to be used with the source IP address. • **any|host <dest-ip-address>| < dest-ip-address > <mask>** - Denies traffic with the specified destination address. The destination can be: ▪ **any –** Denies the packets with any destination. ▪ **host <dest-ip-address>** - Denies packets with the specified host destination IPv4 address. ▪ **<dest-ip-address> <mask>** - Denies packets with the specified destination IP address and the network mask for the given destination IP address. • **tos** - Denies the protocol packets based on the following Type Of Service

configurations:

- **max-reliability** - Denies the protocol packets having TOS field set as high reliability.
- **max-throughput** - Denies the protocol packets having TOS field set as high throughput.
- **min-delay –** Denies the protocol packets having TOS field set as low delay.
- **normal** - Denies all protocol packets. Does not check for the TOS field in the packets.
- **<value (0-7)>** - Denies the protocol packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS.
  - **0** - Denies all protocol packets. Does not check for the TOS field in the packets.
  - **1** - Denies the protocol packets having TOS field set as high reliability.
  - **2** - Denies the protocol packets having TOS field set as high throughput.
  - **3** - Denies the protocol packets having TOS field set either as high reliability or high throughput.
  - **4** - Denies the protocol packets having TOS field set as low delay.
  - **5** - Denies the protocol packets having TOS field set either as low delay or high reliability.
  - **6** - Denies the protocol packets having TOS field set either as low delay or high throughput.
  - **7** - Denies the protocol packets having TOS field set either as low delay, high reliability, or high throughput..

- **dscp <value (0-63)>** - Configures the Differentiated Services Code Point value to be checked against the packet. This value provides the quality of service control. This value ranges from 0 to 63.

- **priority <value (1-255)>** - Configures the priority of the L3 filter to decide in which order the filter rule is applicable when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 255.

- **svlan-id <vlan-id (1-4094)>** - Configures the Service VLAN value to match against incoming packets. This value ranges from 1 to 4094.

- **svlan-priority <value (0-7)>** - Configures the Service VLAN priority value to match against incoming packets. This value ranges from 0 to 7.

- **cvlan-id <vlan-id (1-4094)>** - Configures Customer VLAN value to match against incoming packets. This value ranges from 1 to 4094.

- **cvlan-priority <value (0-7)>** - Configures Customer VLAN priority value to match against incoming packets. This value ranges from 0 to 7.

	• **single-tag** - Specifies that the filter is to be applied on single VLAN tagged packets. • **double-tag** - Specifies that the filter is to be applied on double VLAN tagged packets.
Mode	ACL Extended Access List Configuration Mode
Package	Metro_E and Metro
Defaults	• protocol type - 255 • priority - 1 • svlan-id - 0 • svlan-priority - -1 • cvlan-id - 0 • cvlan-priority - -1 • single-tag | double-tag - Single tag
Example	**SEFOS(config-ext-nacl)# deny ospf any host 10.0.0.1 tos max-throughput**
Note:	• Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed. • Service VLAN, Service VLAN Priority, Customer VLAN and Customer VLAN Priority options are applicable only for Metro Solution, when the bridge mode is “Provider Bridge”.
Related Command(s)	• **ip access-list –** Creates IP ACLs and enters the IP access list configuration mode • **permit- ip/ospf/pim/protocol type –** Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched. • **show access-lists –** Displays the access list configuration

47.2.7 permit tcp

Command Objective	This command specifies the TCP packets to be forwarded based on the associated parameters.
Syntax	**permit tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> } [{gt <port-number (1-65535)> | lt <port-number (1-65535)> |eq <port-number (1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host <dest-ip-address> | <dest-ip-address> <dest-mask> } [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] [{ ack | rst }] [{tos{max-reliability|max-throughput|min-delay|normal|<tos-value(0-7)>}|dscp <value (0-63)>}] [priority <value (1-255)>] [svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [cvlan-id <vlan-id (1-4094)>] [cvlan-priority <value (0-7)>] [{ single-tag | double-tag }]**
Parameter Description	• **any|host <src-ip-address>| < src-ip-address> < src-mask>** - Permits traffic with the specified source address. The sources are: ▪ **any –** Permits TCP packets from any source. ▪ **host <src-ip-address>** - Permits TCP packets from the specified host source IPv4 address. ▪ **<src-ip-address> <src-mask>** - Permits TCP packets from the specified source IP addressand the network mask to be used with the source IP address. • **gt <port-number (1-65535)>** - Allows only the TCP control packets having the TCP source port numbers greater than the specified port number. This value ranges from 1 to 65535. • **lt <port-number (1-65535)>** - Allows only the TCP control packets having the TCP source port numbers lesser than the specified port number. This value ranges from 1 to 65535. • **eq <port-number (1-65535)>** - Allows only the TCP control packets having the specified TCP source port numbers. This value ranges from 1 to 65535. • **range <port-number (1-65535)> <port-number (1-65535)>**- Allows only the TCP control packets having the TCP source port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values. • **any|host <dest-ip-address>| < dest-ip-address > < dest-mask>** - Permits the TCP packets with the specified destination address.

The destination can be:

- **any –** Permits TCP packets with any destination.
- **host <dest-ip-address>** - Permits TCP packets with specified host destination IPv4 address.
- **<dest-ip-address> < dest-mask>** - Permits TCP packets with the specified destination IP address and the network mask for the given destination IP address.

- **gt <port-number (1-65535)>** - Allows only the TCP control packets having the TCP destination port numbers greater than the specified port number. This value ranges from 1 to 65535.

- **lt <port-number (1-65535)>** - Allows only the TCP control packets having the TCP destination port numbers lesser than the specified port number. This value ranges from 1 to 65535.

- **eq <port-number (1-65535)>** - Allows only the TCP control packets having the specified TCP destination port numbers. This value ranges from 1 to 65535.

- **range <port-number (1-65535)> <port-number (1-65535)>** - Allows only the TCP control packets having the TCP destination port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values.

- **ack** - Configures the TCP ACK bit to be checked against the packet.

- **rst** - Configures the TCP RST bit to be checked against the packet.

- **tos** - Allows the protocol packets based on the following Type Of Service configurations:
  - **max-reliability** - Allows the protocol packets having TOS field set as high reliability.
  - **max-throughput** - Allows the protocol packets having TOS field set as high throughput.
  - **min-delay –** Allows the protocol packets having TOS field set as low delay.
  - **normal** - Allows all protocol packets. Does not check for the TOS field in the packets.
  - **<value (0-7)>** - Allows the protocol packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS.
    - **0** - Allows all protocol packets. Does not check for the TOS field in the packets.
    - **1** - Allows the protocol packets having TOS field set as high reliability.
    - **2** - Allows the protocol packets having TOS field set as high throughput.

- **3** - Allows the protocol packets having TOS field set either as high reliability or high throughput.
- **4** - Allows the protocol packets having TOS field set as low delay.
- **5** - Allows the protocol packets having TOS field set either as low delay or high reliability.
- **6** - Allows the protocol packets having TOS field set either as low delay or high throughput.
- **7** - Allows the protocol packets having TOS field set either as low delay, high reliability, or high throughput.

- **dscp <value (0-63)>** - Configures the Differentiated Services Code Point value to be checked against the packet. This value provides the quality of service control. This value ranges from 0 to 63.

- **priority <value (1-255)>** - Configures the priority of the L3 filter to decide in which order the filter rule is applicable when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 255.

- **svlan-id <vlan-id (1-4094)>** - Configures the Service VLAN value to match against incoming packets. This value ranges from 1 to 4094.

- **svlan-priority <value (0-7)>** - Configures the Service VLAN priority value to match against incoming packets. This value ranges from 0 to 7.

- **cvlan-id <vlan-id (1-4094)>** - Configures Customer VLAN value to match against incoming packets. This value ranges from 1 to 4094.

- **cvlan-priority <value (0-7)>** - Configures Customer VLAN priority value to match against incoming packets. This value ranges from 0 to 7.

- **single-tag** - Specifies that the filter is to be applied on single VLAN tagged packets.

- **double-tag** - Specifies that the filter is to be applied on double VLAN tagged packets.

Mode

ACL Extended Access List Configuration Mode

Package

Metro_E and Metro

Defaults

- tos-value - 0

- ack - 'any' (3) [indicates that the TCP ACK bit will not be checked to decide the action]

- rst - 'any' (3) [indicates that the TCP RST bit will not be checked to decide the action]

- svlan-id - 0

- svlan-priority - -1
- cvlan-id - 0
- cvlan-priority - -1
- single-tag | double-tag - Single tag

Example

```
SEFOS(config-ext-nacl)# permit tcp any 10.0.0.1
255.255.255.255
```

Note: Service VLAN, Service VLAN Priority, Customer VLAN and Customer VLAN Priority options are applicable only for Metro Solution, when the bridge mode is “Provider Bridge”.

Related Command(s)

- **`ip access-list`** – Creates IP ACLs and enters the IP access list configuration mode.
- **`show access-lists`** – Displays the access list configuration.
- **`deny tcp`** – Specifies the TCP packets to be rejected based on the associated parameters.

47.2.8 deny tcp

Command Objective	This command specifies the TCP packets to be rejected based on the associated parameters.
Syntax	**deny tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> } [{gt <port-number (1-65535)> | lt <port-number (1-65535)> |eq <port-number (1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host <dest-ip-address> | <dest-ip-address> <dest-mask> } [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] [{ ack | rst }] [{tos{max-reliability|max-throughput|min-delay|normal|<tos-value(0-7)>} | dscp <value (0-63)>}] [priority <value (1-255)>] [svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [cvlan-id <vlan-id (1-4094)>] [cvlan-priority <value (0-7)>] [{ single-tag | double-tag }]**
Parameter Description	• **any|host <src-ip-address>| < src-ip-address> < src-mask>** - Denies traffic with the specified source address. The sources are: ▪ **any -** Denies TCP packets from any source. ▪ **host <src-ip-address>** - Denies TCP packets with the specified host source IPv4 address. ▪ **<src-ip-address> < src-mask>** - Denies TCP packets with the specified source IP address from and the network mask to be used with the source IP address • **gt <port-number (1-65535)>** - Denies only the TCP control packets having the TCP source port numbers greater than the specified port number. This value ranges from 1 to 65535. • **lt <port-number (1-65535)>** - Denies only the TCP control packets having the TCP source port numbers lesser than the specified port number. This value ranges from 1 to 65535. • **eq <port-number (1-65535)>** - Denies only the TCP control packets having the specified TCP source port numbers. This value ranges from 1 to 65535. • **range <port-number (1-65535)> <port-number (1-65535)>** - Denies only the TCP control packets having the TCP source port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values. • **any|host <dest-ip-address>| < dest-ip-address > < dest-mask>** - Denies the TCP packets with the specified destination address.

The destination can be:

- **any –** Denies TCP packets with any destination.
- **host <dest-ip-address>** - Denies TCP packets with specified host destination IPv4 address .
- **<dest-ip-address> <dest-mask>** - Denies TCP packets with the specified destination IP address and the network mask for the given destination IP address.

- **gt <port-number (1-65535)>** - Denies only the TCP control packets having the TCP destination port numbers greater than the specified port number. This value ranges from 1 to 65535.
- **lt <port-number (1-65535)>** - Denies only the TCP control packets having the TCP destination port numbers lesser than the specified port number. This value ranges from 1 to 65535.
- **eq <port-number (1-65535)>** - Denies only the TCP control packets having the specified TCP destination port numbers. This value ranges from 1 to 65535.
- **range <port-number (1-65535)> <port-number (1-65535)>** - Denies only the TCP control packets having the TCP destination port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values.
- **ack** - Configures the TCP ACK bit to be checked against the packet.
- **rst** - Configures the TCP RST bit to be checked against the packet.
- **tos** - Denies the protocol packets based on the following Type Of Service configurations:
  - **max-reliability** - Denies the protocol packets having TOS field set as high reliability.
  - **max-throughput** - Denies the protocol packets having TOS field set as high throughput.
  - **min-delay** - Denies the protocol packets having TOS field set as low delay.
  - **normal** - Denies all protocol packets. Does not check for the TOS field in the packets.
  - **<value (0-7)>** - Denies the TCP packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS.
    - **0** - Denies all packets. Does not check for the TOS field in the packets.
    - **1** - Denies the packets having TOS field set as high reliability.
    - **2** - Denies the packets having TOS field set as high throughput.
    - **3** - Denies the packets having TOS field set either as high reliability or high throughput.

- **4** - Denies the packets having TOS field set as low delay.
- **5** - Denies the packets having TOS field set either as low delay or high reliability.
- **6** - Denies the packets having TOS field set either as low delay or high throughput.
- **7** - Denies the packets having TOS field set either as low delay, high reliability, or high throughput.

- **dscp <value (0-63)>** - Configures the Differentiated Services Code Point value to be checked against the packet. This value provides the quality of service control. This value ranges from 0 to 63.

- **priority <value (1-255)>** - Configures the priority of the L3 filter to decide in which order the filter rule is applicable when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 255.

- **svlan-id <vlan-id (1-4094)>** - Configures the Service VLAN value to match against incoming packets. This value ranges from 1 to 4094.

- **svlan-priority <value (0-7)>** - Configures the Service VLAN priority value to match against incoming packets. This value ranges from 0 to 7.

- **cvlan-id <vlan-id (1-4094)>** - Configures Customer VLAN value to match against incoming packets. This value ranges from 1 to 4094.

- **cvlan-priority <value (0-7)>** - Configures Customer VLAN priority value to match against incoming packets. This value ranges from 0 to 7.

- **single-tag** - Specifies that the filter is to be applied on single VLAN tagged packets.

- **double-tag** - Specifies that the filter is to be applied on double VLAN tagged packets.

Mode

ACL Extended Access List Configuration Mode

Package

Metro_E and Metro

Defaults

- tos-value - 0
- ack - 'any' (3) [indicates that TCP ACK bit will not be checked to decide the action]
- rst - 'any' (3) [indicates that TCP RST bit will not be checked to decide the action]
- svlan-id - 0
- svlan-priority - -1

- cvlan-id - 0
- cvlan-priority - -1
- single-tag | double-tag - Single tag

Example

```
SEFOS(config-ext-nacl)# deny tcp 100.0.0.10 255.255.255.0
eq 20 any
```

Note: Service VLAN, Service VLAN Priority, Customer VLAN and Customer VLAN Priority options are applicable only for Metro Solution, when the bridge mode is “Provider Bridge”.

Related Command(s)

- **`ip access-list -`** Creates IP ACLs and enters the IP access list configuration mode.
- **`show access-lists -`** Displays the access list configuration.
- **`permit tcp -`** Specifies the TCP packets to be forwarded based on the associated parameters.

47.2.9 permit udp

Command Objective	This command specifies the UDP packets to be forwarded based on the associated parameters.
Syntax	**permit udp { any | host <src-ip-address> | <src-ip-address> <src-mask>} [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host <dest-ip-address> | <dest-ip-address> <dest-mask> } [{ gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] [{tos{max-reliability|max-throughput|min-delay|normal|<tos-value(0-7)>} | dscp <value (0-63)>}] [priority <value (1-255)>] [svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [cvlan-id <vlan-id (1-4094)>] [cvlan-priority <value (0-7)>] [{ single-tag | double-tag }]**
Parameter Description	• **any|host <src-ip-address>| < src-ip-address> <src-mask>** - Permits traffic with the specified source address. The sources are: ▪ **any –** Permits UDP packets from any source. ▪ **host <src-ip-address>** - Permits UDP packets from the specified host source IPv4 address. ▪ **<src-ip-address> <src-mask>** - Permits UDP packets from the specified source IP address from and the network mask to be used with the source IP address. • **gt <port-number (1-65535)>** - Allows only the UDP control packets having the TCP source port numbers greater than the specified port number. This value ranges from 1 to 65535. • **lt <port-number (1-65535)>** - Allows only the UDP control packets having the UDP source port numbers lesser than the specified port number. This value ranges from 1 to 65535. • **eq <port-number (1-65535)>** - Allows only the UDP control packets having the specified UDP source port numbers. This value ranges from 1 to 65535. • **range <port-number (1-65535)> <port-number (1-65535)>**- Allows only the UDP control packets having the UDP source port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values. • **any|host <dest-ip-address>| < dest-ip-address > <dest-mask>** - Permits traffic with the specified destination address. The destination can be:

- **any –** Permits UDP packets with any destination.
- **host <dest-ip-address>** - Permits UDP packets with specified host destination IPv4 address.
- **<dest-ip-address> <dest-mask>** - Permits UDP packets with the specified destination IP address and the network mask for the given source IP address.

- **gt <port-number (1-65535)>** - Allows only the UDP control packets having the UDP destination port numbers greater than the specified port number. This value ranges from 1 to 65535.

- **lt <port-number (1-65535)>** - Allows only the UDP control packets having the UDP destination port numbers lesser than the specified port number. This value ranges from 1 to 65535.

- **eq <port-number (1-65535)>** - Allows only the UDP control packets having the specified UDP destination port numbers. This value ranges from 1 to 65535.

- **range <port-number (1-65535)> <port-number (1-65535)>** - Allows only the UDP control packets having the UDP destination port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values.

- **tos** - Allows the protocol packets based on the following Type Of Service configurations:
  - **max-reliability** - Allows the protocol packets having TOS field set as high reliability.
  - **max-throughput** - Allows the protocol packets having TOS field set as high throughput.
  - **min-delay –** Allows the protocol packets having TOS field set as low delay.
  - **normal** - Allows all protocol packets. Does not check for the TOS field in the packets.
  - **<value (0-7)>** - Allows the protocol packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS.
    - **0** - Allows all protocol packets. Does not check for the TOS field in the packets.
    - **1** - Allows the protocol packets having TOS field set as high reliability.
    - **2** - Allows the protocol packets having TOS field set as high throughput.
    - **3** - Allows the protocol packets having TOS field set either as high reliability or high throughput.
    - **4** - Allows the protocol packets having TOS field set as low delay.
    - **5** - Allows the protocol packets having TOS field set either as low delay or high reliability.

- **6** - Allows the protocol packets having TOS field set either as low delay or high throughput.
- **7** - Allows the protocol packets having TOS field set either as low delay, high reliability, or high throughput.

- **dscp <value (0-63)>** - Configures the Differentiated Services Code Point value to be checked against the packet. This value provides the quality of service control. This value ranges from 0 to 63.
- **priority <value (1-255)>** - Configures the priority of the L3 filter to decide in which order the filter rule is applicable when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 255.
- **svlan-id <vlan-id (1-4094)>** - Configures the Service VLAN value to match against incoming packets. This value ranges from 1 to 4094.
- **svlan-priority <value (0-7)>** - Configures the Service VLAN priority value to match against incoming packets. This value ranges from 0 to 7.
- **cvlan-id <vlan-id (1-4094)>** - Configures Customer VLAN value to match against incoming packets. This value ranges from 1 to 4094.
- **cvlan-priority <value (0-7)>** - Configures Customer VLAN priority value to match against incoming packets. This value ranges from 0 to 7.
- **single-tag** - Specifies that the filter is to be applied on single VLAN tagged packets.
- **double-tag** - Specifies that the filter is to be applied on double VLAN tagged packets.

Mode ACL Extended Access List Configuration Mode

Package Metro_E and Metro

Defaults

- svlan-id - 0
- svlan-priority - -1
- cvlan-id - 0
- cvlan-priority - -1
- single-tag | double-tag - Single tag

Example

```
SEFOS(config-ext-nacl)# permit udp any gt 65000 any dcsp 1
```

Note: Service VLAN, Service VLAN Priority, Customer VLAN and Customer VLAN Priority options are applicable only for Metro Solution, when the bridge mode is "Provider Bridge".

Related Command(s)	• **`ip access-list -`** Creates IP ACLs and enters the IP access list configuration mode. • **`show access-lists -`** Displays the access list configuration. • **`deny udp -`** Specifies the UDP packets to be rejected based on the associated parameters.

47.2.10 deny udp

Command Objective	This command specifies the UDP packets to be rejected based on the associated parameters.
Syntax	**deny udp { any | host <src-ip-address> | <src-ip-address> <src-mask>} [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] { any | host <dest-ip-address> | <dest-ip-address> <dest-mask> } [{ gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}] [{tos{max-reliability|max-throughput|min-delay|normal|<tos-value(0-7)>} | dscp <value (0-63)>}] [priority <value (1-255)>] [svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [cvlan-id <vlan-id (1-4094)>] [cvlan-priority <value (0-7)>] [{ single-tag | double-tag }]**
Parameter Description	• **any|host <src-ip-address>| < src-ip-address><src-mask>** - Denies the UDP packets with the specified source address. The sources are: ▪ **any** – Denies UDP packets from any source. ▪ **host <src-ip-address>** - Denies UDP packets with the specified host source IPv4 address. ▪ **<src-ip-address> <src-mask>** - Denies UDP packets with the specified source IP addressfrom and the network mask to be used with the source IP address. • **gt <port-number (1-65535)>** - Denies only the UDP control packets having the TCP source port numbers greater than the specified port number. This value ranges from 1 to 65535. • **lt <port-number (1-65535)>** - Denies only the UDP control packets having the UDP source port numbers lesser than the specified port number. This value ranges from 1 to 65535. • **eq <port-number (1-65535)>** - Denies only the UDP control packets having the specified UDP source port numbers. This value ranges from 1 to 65535. • **range <port-number (1-65535)> <port-number (1-65535)>** - Denies only the UDP control packets having the UDP source port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values. • **any|host <dest-ip-address>| < dest-ip-address > <dest-mask>** - Denies the UDP packets with the specified destination address.

The destination can be:

- **any –** Denies UDP packets with any destination.
- **host <dest-ip-address>** - Denies UDP packets with specified host destination IPv4 address.
- **<dest-ip-address> <dest-mask>** - Denies UDP packets with the specified destination IP address and the network mask for the given source IP address.

- **gt <port-number (1-65535)>** - Denies only the UDP control packets having the UDP destination port numbers greater than the specified port number. This value ranges from 1 to 65535.

- **lt <port-number (1-65535)>** - Denies only the UDP control packets having the UDP destination port numbers lesser than the specified port number. This value ranges from 1 to 65535.

- **eq <port-number (1-65535)>** - Denies only the UDP control packets having the specified UDP destination port numbers. This value ranges from 1 to 65535.

- **range <port-number (1-65535)> <port-number (1-65535)>** - Denies only the UDP control packets having the UDP destination port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values.

- **tos** - Denies the protocol packets based on the following Type Of Service configurations:
  - **max-reliability** - Denies the protocol packets having TOS field set as high reliability.
  - **max-throughput** - Denies the protocol packets having TOS field set as high throughput.
  - **min-delay –** Denies the protocol packets having TOS field set as low delay.
  - **normal** - Denies all protocol packets. Does not check for the TOS field in the packets.
  - **<value (0-7)>** - Denies the protocol packets based on the TOS value set. This value ranges from 0 to 7. This value represents different combination of TOS.
    - **0** - Denies all protocol packets. Does not check for the TOS field in the packets.
    - **1** - Denies the protocol packets having TOS field set as high reliability.
    - **2** - Denies the protocol packets having TOS field set as high throughput.
    - **3** - Denies the protocol packets having TOS field set either as high reliability or high throughput.
    - **4** - Denies the protocol packets having TOS field set as low delay.
    - **5** - Denies the protocol packets having TOS field set either as low

delay or high reliability.

- **6** - Denies the protocol packets having TOS field set either as low delay or high throughput.
- **7** - Denies the protocol packets having TOS field set either as low delay, high reliability, or high throughput.

- **dscp <value (0-63)>** - Configures the Differentiated Services Code Point value to be checked against the packet. This value provides the quality of service control. This value ranges from 0 to 63.
- **priority <value (1-255)>** - Configures the priority of the L3 filter to decide in which order the filter rule is applicable when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 255.
- **svlan-id <vlan-id (1-4094)>** - Configures the Service VLAN value to match against incoming packets. This value ranges from 1 to 4094.
- **svlan-priority <value (0-7)>** - Configures the Service VLAN priority value to match against incoming packets. This value ranges from 0 to 7.
- **cvlan-id <vlan-id (1-4094)>** - Configures Customer VLAN value to match against incoming packets. This value ranges from 1 to 4094.
- **cvlan-priority <value (0-7)>** - Configures Customer VLAN priority value to match against incoming packets. This value ranges from 0 to 7.
- **single-tag** - Specifies that the filter is to be applied on single VLAN tagged packets.
- **double-tag** - Specifies that the filter is to be applied on double VLAN tagged packets.

Mode

ACL Extended Access List Configuration Mode

Defaults

- svlan-id - 0
- svlan-priority - -1
- cvlan-id - 0
- cvlan-priority - -1
- single-tag | double-tag - Single tag

Package

Metro_E and Metro

Example

```
SEFOS(config-ext-nacl)# deny udp host 10.0.0.1 any eq 20
```

Note: Service VLAN, Service VLAN Priority, Customer VLAN and Customer VLAN Priority options are applicable only for Metro Solution, when the bridge mode is

	“Provider Bridge”.
Related Command(s)	• **`ip access-list -`** Creates IP ACLs and enters the IP access list configuration mode. • **`show access-lists -`** Displays the access list configuration. • **`permit udp -`** Specifies the UDP packets to be forwarded based on the associated parameters.

47.2.11 permit icmp

Command Objective	This command specifies the ICMP packets to be forwarded based on the IP address and the associated parameters.
Syntax	**permit icmp {any |host <src-ip-address>|<src-ip-address> <mask>} {any | host <dest-ip-address> | <dest-ip-address> <mask> } [<message-type (0-255)>] [<message-code (0-255)>] [priority <value (1-255)>] [svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [cvlan-id <vlan-id (1-4094)>] [cvlan-priority <value (0-7)>] [{ single-tag | double-tag }]**
Parameter Description	• **any|host <src-ip-address>| < src-ip-address> <mask>** - Permits the ICMP packet with the specified source address. The sources are: ▪ **any –** Permits ICMP packets from any source. ▪ **host <src-ip-address>** - Permits ICMP packets from the specified host source IPv4 address. ▪ **<src-ip-address> <mask>** - Permits ICMP packets from the specified source IP address and the network mask to be used with the source IP address. • **any|host <dest-ip-address>| < dest-ip-address > <mask>** - Permits the ICMP packets with the specified destination address. The destination can be: ▪ **any –** Permits ICMP packets with any destination. ▪ **host <dest-ip-address>** - Permits ICMP packets with specified host destination IPv4 address. ▪ **<dest-ip-address> <mask>** - Permits ICMP packets with the specified destination IP address and the network mask for the given destination IP address. • **<message-type (0-255)>**- Configures the ICMP message type to be checked against the packet. The packet will be allowed if it matches the message type. This value ranges from 0 to 255. Some of the ICMP message types are:

Value	ICMP Message type
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo Request
11	Time Exceeded

12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
255	No ICMP type

- **<message-code (0-255)>**- Configures the ICMP message code to be checked against the packet. The packet will be allowed if it matches the message code. This value ranges from 0 to 255. Some of the ICMP message codes are:

Value	ICMP code
0	Network Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
4	Fragment Need
5	Source Route Fail
6	Destination Network Unknown
7	Destination Host Unknown
8	Source Host Isolated
9	Destination Network Administratively Prohibited
10	Destination Host Administratively Prohibited
11	Network Unreachable TOS
12	Host Unreachable TOS
255	No ICMP Code

- **priority <value (1-255)>** - Configures the priority of the L3 filter to decide in which order the filter rule is applicable when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 255.

- **svlan-id <vlan-id (1-4094)>** - Configures the Service VLAN value to match against incoming packets. This value ranges from 1 to 4094.

- **svlan-priority <value (0-7)>** - Configures the Service VLAN priority value to match against incoming packets. This value ranges from 0 to 7.

- **cvlan-id <vlan-id (1-4094)>** - Configures Customer VLAN value to match against incoming packets. This value ranges from 1 to 4094.

- **cvlan-priority <value (0-7)>** - Configures Customer VLAN priority value to match against incoming packets. This value ranges from 0 to 7.

	• **single-tag** - Specifies that the filter is to be applied on single VLAN tagged packets. • **double-tag** - Specifies that the filter is to be applied on double VLAN tagged packets.
Mode	ACL Extended Access List Configuration Mode
Package	Metro_E and Metro
Defaults	• priority - 1 • dscp – 1 • message-type / message code - 255
Note:	Service VLAN, Service VLAN Priority, Customer VLAN and Customer VLAN Priority options are applicable only for Metro Solution, when the bridge mode is “Provider Bridge”.
Example	**SEFOS(config-ext-nacl)# permit icmp any any**
Related Command(s)	• **ip access-list –** Creates IP ACLs and enters the IP access list configuration mode. • **show access-lists –** Displays the access list configuration. • **deny icmp –** Specifies the ICMP packets to be rejected based on the IP address and associated parameters.

47.2.12 deny icmp

Command Objective	This command specifies the ICMP packets to be rejected based on the IP address and associated parameters.
Syntax	**deny icmp {any |host <src-ip-address>|<src-ip-address> <mask>} {any | host <dest-ip-address> | <dest-ip-address> <mask> } [<message-type (0-255)>] [<message-code (0-255)>] [priority <value (1-255)>] [svlan-id <vlan-id (1-4094)>] [svlan-priority <value (0-7)>] [cvlan-id <vlan-id (1-4094)>] [cvlan-priority <value (0-7)>] [{ single-tag | double-tag }]**
Parameter Description	• **any|host <src-ip-address>| < src-ip-address> <mask>** - Denies the ICMP packet with the specified source address. The sources are: ▪ **any –** Denies ICMP packets from any source. ▪ **host <src-ip-address>** - Denies ICMP packets from the specified host source IPv4 address. ▪ **<src-ip-address> <mask>** - Denies ICMP packets from the specified source IP address and the network mask to be used with the source IP address. • **any|host <dest-ip-address>| < dest-ip-address > <mask>** - Denies the ICMP packets with the specified destination address. The destination can be: ▪ **any –** Denies ICMP packets with any destination. ▪ **host <dest-ip-address>** - Denies ICMP packets with specified host destination IPv4 address. ▪ **<dest-ip-address> <mask>** - Denies ICMP packets with the specified destination IP address and the network mask for the given destination IP address. • **<message-type (0-255)>**- Configures the ICMP message type to be checked against the packet. The packet will be denied if it matches with the message type. This value ranges from 0 to 255. Some of the ICMP message types are:

Value	ICMP Message type
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo Request
11	Time Exceeded
12	Parameter Problem

13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
255	No ICMP type

- **<message-code (0-255)>**- Configures the ICMP message code to be checked against the packet. The packet will be denied if it matches with the message code. This value ranges from 0 to 255. Some of the ICMP message codes are:

Value	ICMP code
0	Network Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
4	Fragment Need
5	Source Route Fail
6	Destination Network Unknown
7	Destination Host Unknown
8	Source Host Isolated
9	Destination Network Administratively Prohibited
10	Destination Host Administratively Prohibited
11	Network Unreachable TOS
12	Host Unreachable TOS
255	No ICMP Code

- **priority <value (1-255)>** - Configures the priority of the L3 filter to decide in which order the filter rule is applicable when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority. This value ranges from 1 to 255.

- **svlan-id <vlan-id (1-4094)>** - Configures the Service VLAN value to match against incoming packets. This value ranges from 1 to 4094.

- **svlan-priority <value (0-7)>** - Configures the Service VLAN priority value to match against incoming packets. This value ranges from 0 to 7.

- **cvlan-id <vlan-id (1-4094)>** - Configures Customer VLAN value to match against incoming packets. This value ranges from 1 to 4094.

- **cvlan-priority <value (0-7)>** - Configures Customer VLAN priority value to match against incoming packets. This value ranges from 0 to 7.

- **single-tag** - Specifies that the filter is to be applied on single VLAN

	tagged packets. • **double-tag** - Specifies that the filter is to be applied on double VLAN tagged packets.
Mode	ACL Extended Access List Configuration Mode
Package	Metro_E and Metro
Defaults	• message-type/message code - 255 • svlan-id - 0 • svlan-priority - -1 • cvlan-id - 0 • cvlan-priority - -1 • single-tag | double-tag - Single tag
Note:	Service VLAN, Service VLAN Priority, Customer VLAN and Customer VLAN Priority options are applicable only for Metro Solution, when the bridge mode is “Provider Bridge”.Service VLAN, Service VLAN Priority, Customer VLAN and Customer VLAN Priority options are applicable only for Metro Solution, when the bridge mode is “Provider Bridge”.
Example	**SEFOS(config-ext-nacl)# deny icmp host 100.0.0.10 10.0.0.1 255.255.255.255**
Related Command(s)	• **ip access-list –** Creates IP ACLs and enters the IP access list configuration mode. • **show access-lists –** Displays the access list configuration. • **permit icmp –** Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters.

47.2.13 ip access-group

Command Objective	This command enables access control for the packets on the interface. It controls access to a Layer 2 or Layer 3 interface. The no form of this command removes all access groups or the specified access group from the interface. The direction of filtering is specified using the token in or out.
Syntax	**ip access-group <access-list-number (1-65535)> {in | out}** **no ip access-group [<access-list-number (1-65535)>] {in | out}**
Parameter Description	• **access-list-number (1-65535)>**– Configures the IP access control list number on the interface. This value ranges from 1 to 65535. • **in** - Configures the packets as Inbound packets. • **out** - Configures the packets as Outbound packets.
Mode	Interface Configuration Mode
Package	Metro_E and Metro
Note:	• IP access list must have been created. • Following are the limitations for this command to be applicable to Layer 2 interfaces: ▪ The `out` keyword is not supported by Layer 2 interfaces. ▪ An IP ACL applied to a Layer 2 interface filters only the IP packets. MAC access group interface configuration command with MAC-extended ACLs must be used to filter non-IP packets.
Example	**SEFOS (config-if)# ip access-group 1 in**
Related Command(s)	• **ip access-list -** Creates IP ACLs and enters the IP access list configuration mode. • **show access-lists -** Displays the access list configuration.

47.2.14 mac access-group

Command Objective	This command applies a MAC access control list (ACL) to a Layer 2 interface. The no form of this command can be used to remove the MAC ACLs from the interface.
Syntax	**mac access-group <access-list-number (1-65535)> {in | out}** **no mac access-group [<access-list-number (1-65535)>] {in | out}**
Parameter Description	• **<access-list-number (1-65535)>**– Configures the MAC access control list number on the interface. This value ranges from 1 to 65535. • **in** - Configures the packets as Inbound packets. • **out** - Configures the packets as Outbound packets.
Mode	Interface Configuration Mode
Package	Metro_E and Metro
Note:	MAC access list must have been created.
Example	**SEFOS (config-if)# mac access-group 5 in**
Related Command(s)	• **mac access-list extended -** Creates Layer 2 MAC ACLs and returns the MAC access list configuration mode to the user. • **permit - MAC** - Specifies the packets to be forwarded based on the MAC address and the associated parameters. • **deny - MAC** - Specifies the packets to be rejected based on the MAC address and the associated parameters. • **show access-lists -** Displays the access list statistics.

47.2.15 permit

Command Objective	This command specifies the packets to be forwarded based on the MAC address and the associated parameters. That is, this command allows non-IP traffic to be forwarded if the conditions are matched.
Syntax	**permit { any | host <src-mac-address> } { any | host <dest-mac-address> } [{ aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-id | <short (0-65535)> }] [encaptype <integer (1-65535)>] [vlan <vlan-id (1-4094)>] [priority <short (1-255)>] [outerEtherType < integer (1-65535)>] [svlan-id <vlan-id (1-4094)>] [cvlan-priority <value (0-7)>] [svlan-priority <value (0-7)>] [{ single-tag | double-tag }]**
Parameter Description	• **any|host <src-mac-address > –** - Permits traffic with the specified source MAC address. The sources are: ▪ **any –** Permits packets from any source. ▪ **host <src-mac-address >** - Permits packets with the specified host source MAC address. • **any | host <dest-mac-address >** - Destination MAC address to be matched with the packet. • **any | host <dest-mac-address > –** - Permits traffic with the specified source MAC address. The sources are: ▪ **any –** Permits packets from any destination. ▪ **host <dest-mac-address >** - Permits packets with the specified host destination MAC address. • **aarp** - Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address. • **amber** - EtherType DEC-Amber. • **dec-spanning** - EtherType Digital Equipment Corporation (DEC) spanning tree. • **decnet-iv** - EtherType DECnet Phase IV protocol. • **diagnostic** - EtherType DEC-Diagnostic. • **dsm** - EtherType DEC-DSM/DDP. • **etype-6000** - EtherType 0x6000.

- **etype-8042** - EtherType 0x8042.
- **lat** - EtherType DEC-LAT.
- **lavc-sca** - EtherType DEC-LAVC-SCA.
- **mop-console** - EtherType DEC-MOP Remote Console.
- **mop-dump** - EtherType DEC-MOP Dump.
- **msdos** - EtherType DEC-MSDOS.
- **mumps** - EtherType DEC-MUMPS.
- **netbios** - EtherType DEC- Network Basic Input/Output System (NETBIOS).
- **vines-echo** - EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
- **vines-ip** - EtherType VINES IP.
- **xns-id** - EtherType Xerox Network Systems (XNS) protocol suite.
- **encaptype –** Encapsulation type.
- **outerEtherType** - EtherType value to match on Service VLAN tag.
- **svlan-id** - Service VLAN value to match against incoming packets.
- **cvlan-priority** - Customer VLAN priority value to match against incoming packets.
- **svlan-priority** - Service VLAN priority value to match against incoming packets.
- **single-tag** - Filter to be applied on single VLAN tagged packets.
- **double-tag** - Filter to be applied on double VLAN tagged packets.

Mode	ACL MAC Configuration Mode
Package	Metro_E and Metro
Defaults	• vlan-id - 0 • priority - 1 • outerEtherType - 0

- svlan-id - 0
- cvlan-priority - -1
- svlan-priority - -1
- single-tag | double-tag - Single tag

Example

```
SEFOS(config-ext-macl)# permit host 00:11:22:33:44:55 any
load-balance src-ip sub-action modify lan 526
```

Note:

- MAC access list must have been created.
- OuterEtherType, Service VLAN, Service VLAN Priority, and Customer VLAN Priority options are applicable only for Metro Solution, when the bridge mode is “Provider Bridge”.

Related Command(s)

- **`mac access-list extended`** – Creates Layer 2 MAC ACLs and returns the MAC access list configuration mode to the user.
- **`mac access-group`** – Applies a MAC access control list (ACL) to a Layer 2 interface.
- **`deny`** – Specifies the packets to be rejected based on the MAC address and the associated parameters.
- **`show access-lists`** – Displays the access list statistics.
- **`user-defined access-list`** - Creates user defined access list.

47.2.16 deny

Command Objective	This command specifies the packets to be rejected based on the MAC address and the associated parameters.
Syntax	**deny { any | host <src-mac-address> } { any | host <dest-mac-address> } [{ aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-id | <short (0-65535)> }] [encaptype <integer (1-65535)>] [vlan <vlan-id (1-4094)>] [priority <short (1-255)>] [outerEtherType < integer (1-65535)>] [svlan-id <vlan-id (1-4094)>] [cvlan-priority <priority (0-7)>] [svlan-priority <value (0-7)>] [{ single-tag | double-tag }]**
Parameter Description	• **any | host <src-mac-address >** - Source MAC address to be matched with the packet. • **any | host <dest-mac-address >** - Destination MAC address to be matched with the packet. • **aarp** - Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address. • **amber** - EtherType DEC-Amber. • **dec-spanning –** EtherType Digital Equipment Corporation (DEC) spanning tree. • **decent-iv** - EtherType DECnet Phase IV protocol. • **diagnostic** - EtherType DEC-Diagnostic. • **dsm** - EtherType DEC-DSM/DDP. • **etype-6000** - EtherType 0x6000. • **etype-8042** - EtherType 0x8042. • **lat** - EtherType DEC-LAT. • **lavc-sca** - EtherType DEC-LAVC-SCA. • **mop-console** - EtherType DEC-MOP Remote Console. • **mop-dump** - EtherType DEC-MOP Dump.

- **msdos** - EtherType DEC-MSDOS.
- **mumps** - EtherType DEC-MUMPS.
- **netbios** - EtherType DEC- Network Basic Input/Output System (NETBIOS).
- **vines-echo** - EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
- **vines-ip** - EtherType VINES IP.
- **xns-id** - EtherType Xerox Network Systems (XNS) protocol suite.
- **encaptype** - Encapsulation type.
- **vlan** - VLAN ID to be filtered.
- **priority** - The priority of the L2 filter is used to decide which filter rule is applicable when the packet matches more than one filter rule. Higher value of 'filter priority' implies a higher priority.
- **outerEtherType** - EtherType value to match on Service VLAN tag.
- **svlan-id –** Service VLAN value to match against incoming packets.
- **cvlan-priority** - Customer VLAN priority value to match against incoming packets.
- **svlan-priority** - Service VLAN priority value to match against incoming packets.
- **single-tag** - Filter to be applied on single VLAN tagged packets.
- **double-tag** - Filter to be applied on double VLAN tagged packets.

Mode ACL MAC Configuration Mode

Package Metro_E and Metro

Defaults

- vlan-id - 0
- priority - 1
- outerEtherType - 0
- svlan-id - 0
- cvlan-priority - -1

- svlan-priority - -1
- single-tag | double-tag - Single tag

Example

```
SEFOS(config-ext-macl)# deny any host 00:11:22:33:44:55
priority 200
```

Note:

- MAC access list must have been created.
- OuterEtherType, Service VLAN, Service VLAN Priority, and Customer VLAN Priority options are applicable only for Metro Solution, when the bridge mode is “Provider Bridge”.

Related Command(s)

- **`mac access-list extended`** – Creates Layer 2 MAC ACLs and returns the MAC access list configuration mode to the user.
- **`mac access-group`** – Applies a MAC access control list (ACL) to a Layer 2 interface.
- **`Permit`** – Specifies the packets to be forwarded based on the MAC address and the associated parameters.
- **`show access-lists`** – Displays the access list statistics.
- **`user-defined access-list`** - Creates user defined access list.

47.2.17 show access-lists

Command Objective	This command displays the access lists' configuration.
Syntax	**show access-lists [[{ip | mac}] <access-list-number (1-65535)>]**
Parameter Description	• **ip** – Displays the access list configuration for the specified IP access list. • **mac** - Displays the access list configuration for the specified MAC access list. • **< access-list-number (1-65535)> -** Displays the MAC, IP, or user access list configuration for the specified access list number. This value ranges from 1 and 65535.
Mode	Privileged/User EXEC Mode
Package	Metro_E and Metro
Example	**SEFOS# show access-lists** EIP ACCESS LISTS ---------- Standard IP Access List 34 ---------- IP address Type : IPV4 Source IP address : 172.30.3.134 Source IP address mask : 255.255.255.255 Source IP Prefix Length : 32 Destination IP address : 0.0.0.0 Destination IP address mask : 0.0.0.0 Destination IP Prefix Length : 0 Flow Identifier : 0 In Port List : NIL Out Port List : NIL Filter Action : Deny Status : InActive Extended IP Access List 1002 ----------

```
 Filter Priority                  : 1
 Filter Protocol Type             : ANY
 IP address Type                  : IPV4
 Source IP address                : 0.0.0.0
 Source IP address mask           : 0.0.0.0
 Source IP Prefix Length          : 0
 Destination IP address           : 0.0.0.0
 Destination IP address mask      : 0.0.0.0
 Destination IP Prefix Length     : 0
 Flow Identifier                  : 0
 In Port List                     : NIL
 Out Port List                    : NIL
 Filter TOS                       : Invalid combination
 Filter DSCP                      : NIL
 Filter Action                    : Permit
 Status                           : InActive
Extended IP Access List 10022
-----------------------------
 Filter Priority                  : 1
 Filter Protocol Type             : ANY
 IP address Type                  : IPV4
 Source IP address                : 0.0.0.0
 Source IP address mask           : 0.0.0.0
 Source IP Prefix Length          : 0
 Destination IP address           : 0.0.0.0
 Destination IP address mask      : 0.0.0.0
 Destination IP Prefix Length     : 0
 Flow Identifier                  : 0
 In Port List                     : NIL
 Out Port List                    : NIL
 Filter TOS                       : Invalid combination
 Filter DSCP                      : NIL
 Filter Action                    : Permit
 Status                           : InActive
MAC ACCESS LISTS
-----------------
 No MAC Access Lists have been configured
```

Note: OuterEtherType, Service VLAN, Service VLAN Priority, innerEtherType, Customer VLAN, and Customer VLAN Priority options are applicable only with Metro Ethernet Feature and bridge mode is provider.

Related Command(s)

- **`ip access-list -`** Creates IP ACLs and enters the IP access list configuration mode.
- **`mac access-list extended -`** Creates Layer 2 MAC ACLs and returns the MAC access list configuration mode to the user.
- **`permit - standard mode -`** Specifies the packets to be forwarded depending upon the associated parameters.
- **`deny - standard mode -`** Denies traffic if the conditions defined in the deny statement are matched.
- **`permit- ip/ospf/pim/protocol type -`** Allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched.
- **`deny - ip/ospf/pim/protocol type -`** Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched.
- **`permit tcp -`** Specifies the TCP packets to be forwarded based on the associated parameters.
- **`deny tcp -`** Specifies the TCP packets to be rejected based on the associated parameters.
- **`permit udp -`** Specifies the UDP packets to be forwarded based on the associated parameters.
- **`deny udp -`** Specifies the UDP packets to be rejected based on the associated parameters.
- **`permit icmp -`** Specifies the ICMP packets to be forwarded based on the IP address and the associated parameters.
- **`deny icmp -`** Specifies the ICMP packets to be rejected based on the IP address and associated parameters.
- **`ip access-group -`** Enables access control for the packets on the interface.
- **`mac access-group -`** Applies a MAC access control list (ACL) to a Layer 2 interface.
- **`permit -`** Specifies the packets to be forwarded based on the MAC address and the associated parameters.

- **deny –** Specifies the packets to be rejected based on the MAC address and the associated parameters.

CHAPTER 48

QoSX

QoS (Quality of Service) defines the ability to provide different priorities to different applications, users, or data flows or the ability to guarantee a certain level of performance to a data flow. QoS refers to resource reservation control mechanisms rather than the achieved service quality and specifies a guaranteed throughput level.

Oracle QoS provides a complete IP Quality of Service solution across VPNs and helps in implementing service provisioning policies for applications or customers, who desire an enhanced performance for their traffic on the Internet.

48.1 shutdown qos

Command Objective	This command shuts down the QoS subsystem. The no form of the command starts the QoS subsystem.
Syntax	**shutdown qos** **no shutdown qos**
Mode	Global Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	QoS subsystem is started and enabled by default.
Note:	• Resources required by QoS subsystem are allocated and QoS subsystem starts running, when started. • All the MemPools used by the QoS subsystem will be released, when shut down.
Example	**SEFOS(config)# shutdown qos**
Related Command(s)	• **qos –** Enables or disables the QoS subsystem • **show qos global info –** Displays QoS-related global configurations.

48.2 qos

Command Objective	This command enables or disables the QoS subsystem.
Syntax	**`qos {enable | disable}`**
Parameter Description	• **`enable –`** Enables the QoS subsystem. • **`disable –`** Disables the Qos subsystem.
Mode	Global Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	Enabled
Note:	• This command executes only when QoS is started in the system. • QoS module programs the hardware and starts protocol operation, when set as enable. • QoS module stops protocol operation by deleting the hardware configuration, when set as disable.
Example	**`SEFOS(config)# qos enable`**
Related Command(s)	• **`shutdown qos`** – Shuts down the QoS subsystem. • **`show qos global info –`** Displays QoS-related global configurations.

48.3 priority-map

Command Objective	This command adds a priority map entry. Configures the priority map index for the incoming packet received over ingress port or VLAN with specified incoming priority. This value ranges from 1 to 65535. The no form of the command deletes a priority map entry.
Syntax	**priority-map <priority-map-Id(1-65535)>** **no priority-map <priority-map-Id(1-65535)>**
Mode	Global Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Note:	This command executes only if QoS is started in the system.
Example	**SEFOS(config)# priority-map 1** **SEFOS(config-pri-map)#**
Related Command(s)	• **shutdown qos** – Shuts down the QoS subsystem. • **show priority-map –** Displays the priority map entry.

48.4 class-map

Command Objective	This command adds a class map entry. Configures an index that enumerates the MultiField Classifier table entries. This value ranges from 1 to 65535. The no form of the command deletes a class map entry.
Syntax	**`class-map <class-map-id(1-65535)>`** **`no class-map <class-map-id(1-65535)>`**
Mode	Global Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Note:	This command executes only if QoS is started in the system.
Example	**`SEFOS(config)# class-map 1`** **`SEFOS(config-cls-map)#`**
Related Command(s)	• **`shutdown qos`** – Shuts down the QoS subsystem. • **`set class -`** Sets CLASS for L2 or L3, or both filters or priority map ID, and adds a CLASS to priority map entry with regenerated priority • **`show class-map –`** Displays the class map entry.

48.5 meter

Command Objective	This command creates a meter. Configures an index that enumerates the meter entries. This value ranges from 1 to 65535. The no form of the command deletes a meter.
Syntax	**meter <meter-id(1-65535)>** **no meter <meter-id(1-65535)>**
Mode	Global Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Note:	This command executes only if QoS is started in the system.
Example	**SEFOS(config)# meter 1** **SEFOS(config-meter)#**
Related Command(s)	• **shutdown qos** – Shuts down the QoS subsystem. • **meter-type** - Sets meter parameters CIR, CBS, EIR, EBS, interval, meter type, and color awareness. • **show meter –** Displays the meter entry.

48.6 policy-map

Command Objective	This command creates a policy map. Configures an index that enumerates the policy map table entries. This value ranges from 1 to 65535. The no form of the command deletes a policy map.
Syntax	**policy-map <policy-map-id(1-65535)>** **no policy-map <policy-map-id(1-65535)>**
Mode	Global Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Note:	This command executes only if QoS is started in the system.
Example	**SEFOS(config)# policy-map 1** **SEFOS(config-ply-map)#**
Related Command(s)	• **shutdown qos** – Shuts down the QoS subsystem. • **set policy -** Sets CLASS for policy. • **show policy-map –** Displays the policy map entry.

48.7 queue-type

Command Objective	This command creates a queue template type with the specified queue template ID. This value ranges from 1 to 65535. The no form of the command deletes a queue template type.
Syntax	**queue-type <Q-Template-Id(1-65535)>** **no queue-type <Q-Template-Id(1-65535)>**
Mode	Global Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Note:	This command executes only if QoS is started in the system
Example	**SEFOS(config)# queue-type 1** **SEFOS(config-qtype)#**
Related Command(s)	• **shutdown qos** – Shuts down the QoS subsystem. • **set algo-type** - Sets Q template entry parameters. • **random-detect dp** - Sets random detect table entry parameters. • **show queue-template –** Displays the Q template and random detect configurations.

48.8 shape-template

Command Objective	This command creates a shape template. The no form of the command deletes a shape template.
Syntax	**shape-template <integer(1-65535)> [cir <integer(1-10485760)>] [cbs <integer(0-10485760)>] [eir <integer(0-10485760)>] [ebs <integer(0-10485760)>]** **no shape-template <Shape-Template-Id(1-65535)>**
Parameter Description	• **shape-template <integer(1-65535)>** - Configures the Shape Template Table index. This value ranges from 1 to 65535. • **cir<integer(1-10485760)** - Configures the committed information rate for packets through the queue. This value ranges from 1 to 10485760. `cir` should be less than `eir`. • **cbs<integer(0-10485760)>** - Configures the committed burst size for packets through the queue. This value ranges from 0 to 10485760. Note: For XCAT/LION platform committed burst size range is from 0 to 4095. • **eir<integer(0-10485760)>** - Configures the excess information rate for packets through the hierarchy. This value ranges from 0 to 10485760. • **ebs<integer(0-10485760)>** - Configures the excess burst size for packets through the hierarchy. This value ranges from 0 to 10485760.
Mode	Global Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS(config)# shape-template 1 cir 20 cbs 40 eir 50 ebs 40**
Related Command(s)	• **show shape-template –** Displays the shape template configurations.

48.9 scheduler

Command Objective

This command creates a scheduler and configures the scheduler parameters.

The no form of the command deletes a scheduler.

Syntax

```
scheduler <integer(1-65535)> interface <iftype> <ifnum>
[sched-algo {strict-priority | rr | wrr | wfq | strict-rr
| strict-wrr | strict-wfq | deficit-rr}] [shaper
<integer(0-65535)>] [hierarchy-level <integer(0-10)>]

no scheduler <Scheduler-Id(1-65535)> interface <iftype>
<ifnum>
```

Parameter Description

- **scheduler-Id<integer(1-65535)>** - Scheduler identifier that uniquely identifies the scheduler in the system or egress interface. This value ranges from 1 to 65535.

  Note: XCAT/LION platforms support maximum of 8 schedulers. An error message is displayed for any scheduler ID beyond this range.

- **iftype -** Interface type. Supports everything except port-channel.
- **ifnum -** Interface number.
- **sched-algo** - Packet scheduling algorithm for the port. The algorithms are:
  - **strict-priority** – strictPriority.
  - **rr** – roundRobin.
  - **wrr** – weightedRoundRobin.
  - **wfg** – weightedFairQueing.
  - **strict-rr** – strictRoundRobin.
  - **strict-wrr** – strictWeightedRoundRobin.
  - **strict-wfg** – strictWeightedFairQueing.
  - **deficit-rr** – deficitRoundRobin.

  Note: XCAT/LION platforms support scheduling algorithms such as Strict Priority and Shaped Deficit Weighted Round Robin (SDWRR)

  Note: For XCAT/LION platforms, configuring **rr/wrr/strict-wrr** options in the command provisions the Shaped Deficit Weighted Round Robin (SDWRR) algorithm in the hardware.

  Note: An error message is displayed if any other scheduling algorithm is configured.

	• **shaper<integer(0-65535)>** - Shaper identifier that specifies the bandwidth requirements for the scheduler. This value ranges from 0 to 65535. • **hierarchy-level<integer(0-10)>** - Depth of the queue or scheduler hierarchy. This value ranges from 0 to 10.
Mode	Global Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	• sched-algo - strict-priority • hierarchy-level - 0
Example	**SEFOS(config)# scheduler 10 interface extreme-ethernet 0/1 sched-algo rr shaper 1 hierarchy-level 1**
Note:	Shape template with the shaper ID should have been created to specify the bandwidth requirements for the scheduler.
Related Command(s)	• **show scheduler –** Displays the configured scheduler. • **sched-hierarchy –** Creates a scheduler hierarchy. • **show sched-hierarchy –** Displays the configured hierarchy scheduler. • **shape-template** – Creates a shape template.

48.10 queue

Command Objective	This command creates a queue and configures the queue parameters. The no form of the command deletes a queue.
Syntax	**queue <integer(1-65535)> interface <iftype> <ifnum> [qtype <integer(1-65535)>] [scheduler <integer(1-65535)>] [weight <integer(0-1000)>] [priority <integer(0-15)>] [shaper <integer(0-65535)>] [queue-type {unicast | multicast }]** **no queue <integer(1-65535)> interface <iftype> <ifnum>**
Parameter Description	• **queue<integer(1-65535)>** - Queue identifier that uniquely identifies the queue in the system or port. This value ranges from 1 to 65535. • **iftype –** Interface type. Supports everything except port-channel. • **ifnum –** Interface number. • **qtype<integer(1-65535)>** - Queue type identifier. This value ranges from 1 to 65535. • **scheduler<integer(1-65535)>** - Scheduler identifier that manages the specified queue. This value ranges from 1 to 65535. • **weight<integer(0-1000)>** - User assigned weight to the CoS queue. This value ranges from 0 to 1000. Note: For XCAT/LION platforms the weight ranges from 0 to 255. • **priority<integer(0-15)>** - User assigned priority for the CoS queue. This value ranges from 0 to 15. • **shaper<integer(0-65535)> –** Shaper identifier that specifies the bandwidth requirements for the queue. This value ranges from 0 to 65535. • **unicast** - Unicast queue to store known unicast packets. • **multicast** - Multicast queue to store DLF, multicast, broadcast, and mirrored packets.
Mode	Global Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	• weight - 0

- priority - 0
- Queue-type - Unicast

Example

```
SEFOS(config)# queue 1 interface giga 0/1 qtype 2
scheduler 1 weight 20 priority 10 shaper 1.
```

Note:

- Scheduler identifier is unique relative to an egress interface.
- User assigned weights are used only when scheduling algorithm is a weighted scheduling algorithm.
- User assigned priority is used only when the scheduler uses a priority based scheduling algorithm.

Related Command(s)

- **`queue-type –`** Creates a queue template type.
- **`scheduler –`** Creates a scheduler and configures the scheduler parameters.
- **`shape-template`** – Creates a shape template.
- **`show queue`** – Displays the configured queues.

48.11 queue-map

Command Objective

This command creates a map for a queue with class or regenerated priority.

The no form of the command deletes a queue map entry.

Syntax

```
queue-map { CLASS <integer(1-65535)> | regn-priority  { vlanPri <integer(0-15)> | ipTos <integer(0-7)> | ipDscp <integer(0-63)> | mplsExp <integer(0-7)> | vlanDEI <integer(0-1)> | internalPri <integer(0-15)> }} [interface <iftype> <ifnum>] queue-id <integer(1-65535)>

no queue-map { CLASS  <integer(1-65535)> | regn-priority { vlanPri | ipTos | ipDscp | mplsExp | vlanDEI | internalPri } <integer(0-63)> } [interface <iftype> <ifnum>]
```

Parameter Description

- **CLASS <integer(1-65535)>** - Configures the input CLASS (associated with an incoming packet) that needs to be mapped to an outbound queue. This value ranges from 1 to 65535.

  Note: Class needs to be created using the **set class** command to configure this parameter.

- **regn-priority** - Configures the regenerated-priority type that needs to be mapped to an outbound queue. The types are
  - **vlanPri <integer(0-15)>**– Sets the regenerated priority type as VLAN Priority. This value ranges from 0 to 15.
  - **ipTos<integer(0-7)>** – Sets the regenerated priority type as IP Type of Service. This value ranges from 0 to 7.
  - **ipDscp <integer(0-63)>**– Sets the regenerated priority type as IP Differentiated Services Code Point. This value ranges from 0 to 63.
  - **mplsExp <integer(0-7)>** – Sets the regenerated priority type as MPLS Experimental. This value ranges from 0 to 7.
  - **vlanDEI <integer(0-1)>** – Sets the regenerated priority type as VLAN Drop Eligibility Indicator. The input value for this parameter can be 0 or 1.
  - **internalPri <integer(0-15)>** - Sets the regenerated priority type as Internal Priority. The packets classified to internal priority will be associated to queue. This value ranges from 0 to 15.

- .**<iftype>** - Sets the type of interface for the outbound queue. The interface can be:
  - **fastethernet** – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Mbits/sec.
  - **extreme-ethernet** – A version of LAN standard architecture that supports data transfer up to 1 Gbit/sec.

	▪ **extreme-ethernet** – A version of Ethernet that supports data transfer up to 10 Gbits/sec. This Ethernet supports only full duplex links. ▪ **internal-lan** – Internal LAN created on a bridge per IEEE 802.1ap. • **<ifnum>** - Sets the type of interface for the outbound queue. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan id is provided, for interface type internal-lan. • **queue-id <integer(1-65535)>** - Configures the queue identifier that uniquely identifies a queue relative to an interface. This value ranges from 1 to 65535.
Mode	Global Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Note:	This command executes only if QoS is started in the system.
Example	**SEFOS(config)# queue-map regn-priority iptos 1 interface extreme-ethernet 0/1 queue-id 1**
Related Command(s)	• **shutdown qos** – Shuts down the QoS subsystem. • **set class -** Sets CLASS for L2 and/or L3 filters or priority map ID, and adds a CLASS to priority map entry with regenerated priority • **show queue-map** – Displays the configured queue map.

48.12 sched-hierarchy

Command Objective

This command creates a scheduler hierarchy.

The no form of the command deletes a scheduler hierarchy.

Syntax

```
sched-hierarchy interface <iftype> <ifnum> hierarchy-level
<integer(1-10)> sched-id <integer(1-65535)> {next-level-
queue <integer(0-65535)> | next-level-scheduler
<integer(0-65535)>} [priority <integer(0-15)>] [weight
<integer(0-1000)>]

no sched-hierarchy interface <iftype> <ifnum> hierarchy-
level <integer(1-10)> sched-id <integer(1-65535)>
```

Parameter Description

- **<iftype>** - Sets the type of interface for the outbound queue. The interface can be:
  - **fastethernet** – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Mbits/sec.
  - **XL-ethernet** – A version of LAN standard architecture that supports data transfer up to 1 Gbit/sec.
  - **extreme-ethernet** – A version of Ethernet that supports data transfer up to 10 Gbits/sec.

    Note: As of release 2.0.0.3, all interfaces are referred to as extreme-ethernet.

  - **internal-lan** – Internal LAN created on a bridge per IEEE 802.1ap.
- **<ifnum>** - Sets the type of interface for the outbound queue. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan id is provided, for interface type internal-lan.
- **hierarchy-level <integer(1-10)>** - Depth of the queue or scheduler hierarchy.
- **sched-id <integer(1-65535)>** - Scheduler identifier.
  - **next-level-queue** – Next-level queue to which the scheduler output needs to be sent.

    Note: This option is not supported.

  - **next-level-scheduler –** Next-level scheduler to which the scheduler output needs to be sent.
- **priority <integer(0-15)** - Scheduler priority.

	• **weight <integer(0-1000)>** - Scheduler weight.
Mode	Global Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	priority - 0
Example	**SEFOS(config)# sched-hierarchy interface extreme-ethernet 0/1 hierarchy-level 1 sched-id 10 next-level-scheduler 11 priority 5 weight 50**
Note:	• The priority is specified when the scheduler is connecting to any of the priorities (EF, AF, BE) of the next level strict-priority scheduler. • The weight is specified if the scheduler is connecting to a WeightedFairQueing of another scheduler.
Related Command(s)	• **show scheduler –** Displays the configured scheduler. • **sched-hierarchy –** Creates a scheduler hierarchy. • **show sched-hierarchy –** Displays the configured hierarchy scheduler.

48.13 qos interface

Command Objective	This command sets the default ingress user priority for the port.
Syntax	**qos interface <iftype> <ifnum> def-user-priority <integer(0-7)>**
Parameter Description	• **<iftype>** - Sets the type of interface for the outbound queue. The interface can be: ▪ **fastethernet** – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Mbits/sec. ▪ **XL-ethernet** – A version of LAN standard architecture that supports data transfer up to 1 Gbit/sec. ▪ **extreme-ethernet** – A version of Ethernet that supports data transfer up to 10 Gbits/sec. ▪ **internal-lan** – Internal LAN created on a bridge per IEEE 802.1ap. • **<ifnum>** - Sets the type of interface for the outbound queue. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan id is provided, for interface type internal-lan. • **def-user-priority <integer(0-7)>** - Default ingress user priority for the port.
Mode	Global Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS(config)# qos interface extreme-ethernet 0/1 def-user-priority 3**
Note:	The default ingress user priority will be used to set priority for untagged packets.
Related Command(s)	• **show qos def-user-priority** – Displays the configured default ingress user priority for a port.

48.14 map

Command Objective	This command adds a priority map entry for mapping an incoming priority to a regenerated priority. The no form of the command sets default value to the Interface, VLAN, and regenerated inner priority.
Syntax	**`map [interface <iftype> <ifnum>] [vlan <integer(1-4094)>] in-priority-type { vlanPri | ipTos | ipDscp | mplsExp | vlanDEI } in-priority <integer(0-63)> regen-priority <integer(0-63)> [regen-inner-priority <integer(0-7)>]`** **`no map { interface | vlan | regen-inner-priority }`**
Parameter Description	• **`<iftype>`** - Sets the type of interface for the outbound queue. The interface can be: ▪ **`fastethernet`** – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Mbits/sec. ▪ **`XL-ethernet`** – A version of LAN standard architecture that supports data transfer up to 1 Gbit/sec. ▪ **`extreme-ethernet`** – A version of Ethernet that supports data transfer up to 10 Gbits/sec. ▪ **`internal-lan`** – Internal LAN created on a bridge per IEEE 802.1ap. • **`<ifnum>`** - Sets the type of interface for the outbound queue. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan id is provided, for interface type internal-lan. • **`vlan <integer(1-4094)>`** - VLAN identifier. This value ranges from 1 to 4094. • **`in-priority-type`** - Type of the incoming priority. The types are: ▪ **`vlanPri`** – VLAN Priority. ▪ **`ipTos`** – IP Type of Service. ▪ **`ipDscp`** – IP Differentiated Services Code Point. ▪ **`mplsExp`** – MPLS Experimental. ▪ **`vlanDEI`** – VLAN Drop Eligibility Indicator. • **`in-priority <integer(0-63)>`** - Incoming priority value determined for the received frame. This value ranges from 0 to 63. • **`regen-priority <integer(0-63)>`** - Regenerated priority value

	determined for the received frame. This value ranges from 0 to 63. • **regen-inner-priority <integer(0-7)>** - Regenerated inner-VLAN (CVLAN) priority value determined for the received frame. This value ranges from 0 to 7.
Mode	Priority Map Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	• vlan - 0 • in-priority-type - vlanPri • in-priority - -1 • regen-priority - 0
Example	**SEFOS(config-pri-map)# map interface gig 0/1 vlan 4094 in-priority-type vlanPri in-priority 0 regen-priority 7 regen-inner-priority 1**
Note:	Priority map entry should have been created.
Related Command(s)	• **priority-map** – Adds a priority map entry. • **show priority-map –** Displays the priority map entry.

48.15 match access-group

Command Objective	This command sets class map parameters using L2 or L3 ACL or both, or priority map ID.
Syntax	**match access-group { [mac-access-list <integer(0-65535)>] [ip-access-list <integer(0-65535)>] | priority-map <integer(0-65535)> }**
Parameter Description	• **mac-access-list <integer(0-65535)>** - Identifier of the MAC filter. This value ranges from 0 to 65535. • **ip-access-list <integer(0-65535)>** - Identifier of the IP filter. This value ranges from 0 to 65535. • **priority-map <integer(0-65535)>** - Priority map identifier for mapping incoming priority against received packet. This value ranges from 0 to 65535.
Mode	Class Map Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	• mac-access-list - 0 • ip-access-list - 0 • priority-map - 0
Example	**SEFOS(config-cls-map)# match access-group priority-map 1**
Note:	• Priority map ID should have been created. • L2 or L3 ACL or both should have been created.
Related Command(s)	• **priority-map** – Adds a priority map entry. • **show class-map –** Displays the class map entry.

48.16 set class

Command Objective	This command sets CLASS for L2 or L3 filters or both, or priority map ID, and adds a CLASS to priority map entry with regenerated priority. The no form of the command deletes a CLASS to priority map table entry.
Syntax	**set class <class integer(1-65535)> [pre-color { green | yellow | red | none }] [regen-priority <integer(0-7)> group-name <string(31)>]** **no set class <class integer(1-65535)>**
Parameter Description	• **<class integer(1-65535)>** - Traffic CLASS to which an incoming frame pattern is classified. • **pre-color** - Color of the packet prior to metering. This can be any one of the following: ▪ **None** – Traffic is not pre-colored. ▪ **green** – Traffic conforms to SLAs (Service Level Agreements). ▪ **yellow** – Traffic exceeds the SLAs. ▪ **red** – Traffic violates the SLAs. • **regen-priority <integer(0-7)>** - Regenerated priority value determined for the input CLASS. This value ranges from 0 to 7. • **group-name <string(31)>** - Unique identification of the group to which an input CLASS belongs.
Mode	Class Map Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	• class - 0
Example	**SEFOS(config-cls-map)# set class 1000 pre-color none regen-priority 1 group-name CLASS**
Note:	• Class map should have created. • The default value zero provided for the class is not configurable.
Related Command(s)	• **queue-map -** Creates a map for a queue with class or regenerated priority. • **class-map** – Adds a class map entry.

- **`set policy`** - Sets CLASS for policy.
- **`show class-to-priority-map`** – Displays the class group entry.

48.17 meter-type

Command Objective	This command sets meter parameters CIR, CBS, EIR, EBS, interval, meter type, and color awareness.
Syntax	**meter-type { simpleTokenBucket | avgRate| srTCM | trTCM | tswTCM | mefCoupled | mefDeCoupled } [color-mode { aware | blind }] [interval <short(1-10000)>] [cir <integer(0-10485760)>] [cbs <integer(0-10485760)>] [eir <integer(0-10485760)>] [ebs <integer(0-10485760)>] [next-meter <integer(0-65535)>]**
Parameter Description	• **simpleTokenBucket** - Configures the meter type as Two Parameter Token Bucket Meter. • **avgRate** - Configures the meter type as Average Rate Meter. Valid parameters supported are interval and cir. • **srTCM** - Configures the meter type as Single Rate Three Color Marker Metering as defined by RFC 2697. Valid parameters supported are cir, cbs, and ebs. • **trTCM** - Configures the meter type as Two Rate Three Color Marker Metering as defined by RFC 2698. Valid value for given meter type are CIR, CBS, EIR, and EBS. • **tswTCM** - Configures the meter type as Time Sliding Window Three Color Marker Metering as defined by RFC 2859. • **mefCoupled** - Configures the meter type where average bit rate of service frames are marked as yellow and is bounded by CIR and EIR. • **mefDeCoupled** - Configures the meter type where average bit rate of service frames are marked as yellow and is bounded by EIR. • **color-mode** - Configures the color mode of the meter. The color modes are: ▪ **aware** – The meter considers the pre-color of the packet. ▪ **blind** – The meter ignores the pre-color of the packet. • **interval <short(1-10000)>** - Configures the time interval used with the token bucket. This value ranges from 1 to 10000. • **interval <short(1-10000)>** - Configures the time interval used with the token bucket. This value ranges from 1 to 10000. • **cir <integer(0-10485760)>** - Configures the committed information rate. This value ranges from 0 to 10485760.

	• **cbs <integer(0-10485760)>** - Configures the committed burst size. This value ranges from 0 to 10485760. • **eir <integer(0-10485760)>** - Configures the excess information rate. This value ranges from 0 to 10485760. • **ebs <integer(0-10485760)** - Configures the excess burst size. This value ranges from 0 to 10485760. • **next-meter <integer(0-65535)>** - Configures the meter entry identifier used for applying the second or next level of conformance on the incoming packet. This value ranges from 0 to 65535.
Mode	Meter Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	• color-mode - blind • interval - none • type - Simple token bucket
Example	**SEFOS(config-meter)# meter-type srTCM cir 20 cbs 20 ebs 20**
Note:	Meter should have been created.
Related Command(s)	• **meter** – Creates a meter. • **show meter –** Displays the meter entry.

48.18 set policy

Command Objective	This command sets CLASS for policy. The no form of the command sets the default value for interface in this policy.
Syntax	**set policy [class<integer(0-65535)>] [interface <iftype> <ifnum>] default-priority-type { none | { vlanPri <integer(0-7)> | ipTos <integer(0-7)> | ipDscp <integer(0-63)> | mplsExp <integer(0-7)> }}** **no set policy interface**
Parameter Description	• **class <integer(0-65535)** - Specifies the Traffic CLASS for which the policy map needs to be applied. Note: In XCAT/LION platforms, maximum CLASS value is limited to 36 and an error message is displayed for any value configured beyond this range. Note: Class needs to be created using the **set class** command to configure this parameter. • **<iftype>** - Sets the type of interface for the outbound queue. The interface can be: ▪ **fastethernet** – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Mbits/sec. ▪ **XL-ethernet** – A version of LAN standard architecture that supports data transfer up to 1 Gbit/sec. ▪ **extreme-ethernet** – A version of Ethernet that supports data transfer up to 10 Gbits/sec. ▪ **internal-lan** – Internal LAN created on a bridge per IEEE 802.1ap. • **<ifnum>** - Sets the type of interface for the outbound queue. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan id is provided, for interface type internal-lan. • **default-priority-type** - Sets the Per-Hop Behavior (PHB) type to be used for filling the default PHB for the policy map entry. The types are: ▪ **none** – Sets default PHB type as none . ▪ **vlanPri<integer(0-7)>** – Sets the PHB type as VLAN Priority. This value ranges from 0 to 7. ▪ **ipTos <integer(0-7)>** – Sets the PHB type as IP Type of Service. This value ranges from 0 to 7.

	▪ **ipDscp <integer(0-63)>**– Sets the PHB type as IP Differentiated Services Code Point. This value ranges from 0 to 63. ▪ **mplsExp <integer(0-7)>** – Sets the PHB type as MPLS Experimental. This value ranges from 0 to 7. Note: This value can be overwritten by the meter used for the policy map.
Mode	Policy Map Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	class - 0
Example	**SEFOS(config-ply-map)# set policy class 1 interface extreme-ethernet 0/1 default-priority-type none**
Related Command(s)	• **set class -** Sets CLASS for L2and/or L3 filters or priority map ID, and adds a CLASS to priority map entry with regenerated priority. • **policy-map** – Creates a policy map. • **show policy-map –** Displays the policy map entry.

48.19 set meter

Command Objective

This command sets policy parameters such as meter and meter actions.

The no form of the command removes the meter from the policy and the meter actions.

Syntax

```
set meter <integer(1-65535)> [ conform-action { cos-
transmit-set <short(0-7)> | de-transmit-set <short(0-1)> |
set-cos-transmit <short(0-7)> set-de-transmit <short(0-1)>
| set-port <iftype> <ifnum> | inner-vlan-pri-set <short(0-
7)> | inner-vlan-de-set <short(0-1)> | set-inner-vlan-pri
<short(0-7)> set-inner-vlan-de <short(0-1)> |set-mpls-exp-
transmit <short(0-7)> | set-ip-prec-transmit <short(0-7)> |
set-ip-dscp-transmit <short(0-63)>}] [ exceed-action {drop
| cos-transmit-set <short(0-7)> | de-transmit-set <short(0-
1)> | set-cos-transmit <short(0-7)> set-de-transmit
<short(0-1)> | inner-vlan-pri-set <short(0-7) | inner-vlan-
de-set <short(0-1)> | set-inner-vlan-pri <short(0-7)> set-
inner-vlan-de <short(0-1)> | set-mpls-exp-transmit
<short(0-7)> | set-ip-prec-transmit <short(0-7)> | set-ip-
dscp-transmit <short(0-63)> }] [ violate-action {drop |
cos-transmit-set <short(0-7)> | de-transmit-set <short(0-
1)> | set-cos-transmit <short(0-7)> set-de-transmit
<short(0-1)> | inner-vlan-pri-set <short(0-7)> | inner-
vlan-de-set <short(0-1)> | set-inner-vlan-pri <short(0-7)>
set-inner-vlan-de <short(0-1)> | set-mpls-exp-transmit
<short(0-7)> | set-ip-prec-transmit <short(0-7)> | set-ip-
dscp-transmit <short(0-63)> }] [ set-conform-newclass
<integer(0-65535)> ] [ set-exceed-newclass <integer(0-
65535)> ] [ set-violate-newclass <integer(0-65535)> ]

no set meter
```

Parameter Description

- **<integer(1-65535)>** - Meter table identifier which is the index for the meter table.
- **conform-action** - Configures action to be performed on the packet, when the packets are found to be in profile (conform). Options are:
  - **cos-transmit-set <short(0-7)> –** Sets the VLAN priority of the outgoing packet. This value ranges from 0 and 7.
  - **de-transmit-set <short(0-1)> –** Sets the VLAN drop eligible indicator of the outgoing packet. This value ranges from 0 to 1.
  - **set-cos-transmit <short(0-7)> –** Sets the VLAN priority of the outgoing packet. This value ranges from 0 and 7.
  - **set-de-transmit <short(0-1)> –** Sets the VLAN drop eligible indicator of the outgoing packet. This value ranges from 0 to 1.
  - **set-port <iftype> <ifnum> –** Sets the new port value.

- **inner-vlan-pri-set <short(0-7)> -** Sets the inner VLAN priority of the outgoing packet. This value ranges from 0 and 7.
- **inner-vlan-de-set <short(0-1)> -** Sets the inner VLAN DE of the outgoing packet. This value ranges from 0 and 1.
- **set-inner-vlan-pri <short(0-7)> -** Sets the inner VLAN priority of the outgoing packet. This value ranges from 0 and 7
- **set-inner-vlan-de <short(0-1)> -** Sets the inner VLAN DE of the outgoing packet. This value ranges from 0 and 1.
- **set-ip-prec-transmit -** Sets the new IP Type of Service.
- **set-mpls-exp-transmit -** Sets the MPLS experimental bits of the outgoing packet.
- **set-ip-dscp-transmit <short(0-63)>** - Sets the new differentiated services code point value. This value ranges from 0 and 63.

- **exceed-action** - Action to be performed on the packet, when the packets are found to be in profile (exceed). Options are:
  - **drop** – Drops the packet.
  - **cos-transmit-set <short(0-7)> -** Sets the VLAN priority of the outgoing packet. This value ranges 0 and 7.
  - **de-transmit-set <short(0-1)> -** Sets the VLAN Drop Eligible indicator of the outgoing packet. This value ranges from 0 to 1.
  - **set-cos-transmit<short(0-7)>** – Sets the VLAN priority of the outgoing packet. This value ranges 0 and 7.
  - **set-de-transmit<short(0-1)>** – Sets the VLAN Drop Eligible indicator of the outgoing packet. This value ranges from 0 to 1.
  - **inner-vlan-pri-set <short(0-7) -** Sets the inner VLAN priority of the outgoing packet. This value ranges from 0 to 7.
  - **inner-vlan-de-set <short(0-1)> -** Sets the inner VLAN DE of the outgoing packet. This value ranges from 0 to 1.
  - **set-inner-vlan-pri<short(0-7)>** – Sets the inner VLAN priority of the outgoing packet. This value ranges from 0 to 7.
  - **set-inner-vlan-de <short(0-1)> -** Sets the inner VLAN DE of the outgoing packet. This value ranges from 0 to 1.
  - **set-mpls-exp-transmit<short(0-7)>** – Sets the MPLS Experimental bits of the outgoing packet. This value ranges from 0 to 7.
  - **set-ip-prec-transmit<short(0-7)>** – Sets the new IP TOS value. This value ranges from 0 to 7.
  - **set-ip-dscp-transmit<short(0-63)>** – Sets the new DSCP value. This value ranges from 0 to 63.

- **violate-action** - Action to be performed on the packet, when the packets are found to be out of profile. Options are:
  - **drop** – Drops the packet.
  - **cos-transmit-set <short(0-7)> -** Sets the VLAN priority of

the outgoing packet. This value ranges 0 and 7.

- **de-transmit-set <short(0-1)> -** Sets the VLAN Drop Eligible indicator of the outgoing packet. This value ranges from 0 to 1.
- **set-cos-transmit<short(0-7)>** – Sets the VLAN priority of the outgoing packet. This value ranges 0 and 7.
- **set-de-transmit<short(0-1)>** – Sets the VLAN Drop Eligible indicator of the outgoing packet. This value ranges from 0 to 1.
- **inner-vlan-pri-set <short(0-7) -** Sets the inner VLAN priority of the outgoing packet. This value ranges from 0 to 7.
- **inner-vlan-de-set <short(0-1)> -** Sets the inner VLAN DE of the outgoing packet. This value ranges from 0 to 1.
- **set-inner-vlan-pri<short(0-7)>** – Sets the inner VLAN priority of the outgoing packet. This value ranges from 0 to 7.
- **set-inner-vlan-de <short(0-1)> -** Sets the inner VLAN DE of the outgoing packet. This value ranges from 0 to 1.
- **set-mpls-exp-transmit<short(0-7)>** – Sets the MPLS Experimental bits of the outgoing packet. This value ranges from 0 to 7.
- **set-ip-prec-transmit<short(0-7)>** – Sets the new IP TOS value. This value ranges from 0 to 7.
- **set-ip-dscp-transmit<short(0-63)>** – Sets the new DSCP value. This value ranges from 0 to 63.

- **set-conform-newclass<integer(0-65535)>** - Represents the Traffic CLASS to which an incoming frame pattern is classified after metering. This value ranges from 0 to 65535.
- **set-exceed-newclass<integer(0-65535)>** - Represents the Traffic CLASS to which an incoming frame pattern is classified after metering. This value ranges from 0 to 65535.
- **set-violate-newclass<integer(0-65535)>** - Represents the Traffic CLASS to which an incoming frame pattern is classified after metering. This value ranges from 0 to 65535.

Mode Policy Map Configuration Mode

Package Workgroup, Enterprise, Metro_E, and Metro

Defaults

- set-cos-transmit - 0
- set-de-transmit - 0
- set-mpls-exp-transmit - 0
- set-inner-vlan-pri - 0

Note: VLAN priority can be set to a non-zero value only when MPLS Experimental bits is set to zero.

Example	**SEFOS(config-ply-map)# set meter 10 conform-action cos-transmit-set 5 exceed-action cos-transmit-set 5 set-conform-newclass 100 set-exceed-newclass 100 set-violate-newclass 10**
Related Command(s)	• **Show policy-map** - Displays the policy map entry.

48.20 set algo-type

Command Objective	This command configures Q template entry parameters.
Syntax	**set algo-type { tailDrop | headDrop | red | wred } [queue-limit <integer(1-12582720)>] [queue-drop-algo {enable | disable }]**
Parameter Description	• **algo-type** – Configures the type of drop algorithm used by the queue template. Options are: ▪ **tailDrop** – Sets the algorithm type as Tail Drop. With tail drop, when the queue is filled to its maximum capacity; the newly arriving packets are dropped until the queue has enough room to accept incoming traffic. ▪ **headDrop** – Sets the algorithm type as Head Drop. Packets currently at the head of the queue are dropped to make room for the new packet to be enqueued at the tail of the queue, when the current depth of the queue is at the maximum depth of the queue. ▪ **red** – Sets the algorithm type as RED (Random Early Detection) .On packet arrival, an Active Queue Management algorithm is executed which may randomly drop a packet. ▪ **wred** – Sets the algorithm type as WRED (Weighted Random Early Detection) . WRED is an enhanced RED mechanism for congestion avoidance with support for six drop profiles maintained separately for each color (green, yellow and red) TCP or NON-TCP traffic. On packet arrival, an Active Queue Management algorithm is executed which may randomly drop a packet. Note: XCAT/LION platforms support tailDrop algorithm only. • **queue-limit<integer(1-12582720)>** - Configures the queue size limit . This is depth in bytes of the queue being measured, at which a trigger is generated to the dropping algorithm. This value ranges from 1 to 12582720. • **queue-drop-algo** - Sets the option to enable or disable Drop Algorithm for congestion management. Options are: ▪ **enable** – Enables Drop Algorithm. ▪ **disable** – Disables Drop Algorithm.
Mode	Queue Template Configuration mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	• queue-drop-algo - disable • Drop-type - Taildrop

	• Queue-limit - 10000
Example	**`SEFOS(config-qtype)# set algo-type wred queue-limit 120000 queue-drop-algo enable`**
Note:	• Queue size must be greater than or equal to the minimum average threshold and less than or equal to the maximum average threshold. • Drop algorithm for congestion management can be enabled only when the Random Detect Table entry is created for the queue.
Related Command(s)	• **`queue-type -`** Creates a queue template type. • **`random-detect dp`** – Sets Random Detect Table entry parameters. • **`show queue-template –`** Displays the Q template and random detect configurations.

48.21 random-detect dp

Command Objective

This command sets Random Detect Table entry parameters.

The no form of the command deletes Random Detect Table entry.

Syntax

```
random-detect dp <short(0-5)> [min-threshold <integer(1-12582720)>] [max-threshold <integer(1-12582720)>] [max-pkt-size <short(1-65535)>] [mark-probability-denominator <short(1-100)>] [exponential-weight <integer(0-31)>] [gain <short(0-100)>] [drop-threshold-type { packets | bytes}] [ecn-threshold <short(0-65535)>] [flag {[cap-average] [mark-congestion] | none }]

no random-detect dp <short(0-5)>
```

Parameter Description

- **dp <short(0-5)> –** Configures the Drop Precedence for TCP and Non-TCP profiles. Options are:
  - 0 – Sets low drop precedence - Discards TCP Green.
  - 1 – Sets medium drop precedence - Discards TCP Yellow.
  - 2 – Sets high drop precedence - Discards TCP Red.
  - 3 – Discards NON-TCP Green
  - 4 – Discards NON-TCP Yellow
  - 5 - Discards NON-TCP Red

- **min-threshold <integer(1-12582720)>** - Configures the minimum average threshold for the random detect algorithm. Below this threshold, packets are admitted into the queue. This value ranges from 1 to 12582720 if Drop threshold type is set as bytes, and 1 to 65535 if Drop threshold type is set as packets.

  Note: This value must be less than or equal to the maximum threshold and the queue size.

  Note: The units for this is based on the Drop threshold type configured.

- **max-threshold <integer(1-12582720)>** - Configures the maximum average threshold for the random detect algorithm. Above this threshold, packets are discarded before entering the queue. This value ranges from 1 to 12582720 if Drop threshold type is set as bytes and 1 to 65535 if Drop threshold type is set as packets.

  Note: This must be greater than or equal to the minimum threshold and less than or equal to the queue size.

  Note: The units for this is based on the Drop threshold type configured.

- **max-pkt-size <short(1-65535)>** - Configures the maximum allowed packet size. The unit is in bytes. This value ranges from 1 to 65535.
- **mark-probability-denominator <short(1-100)>** - Configures the maximum probability of discarding a packet in units of percentage. This value ranges from 1 to 100.
- **exponential-weight <integer(0-31)>** - Configures the exponential weight for determining the average queue size. This value ranges from 0 to 31.
- **gain <short(0-100)> -** Configures the gain which defines an increase in drop-probability on each granular increase of buffer-occupancy due to received traffic. This value range from 0 to 100.
- **drop-threshold-type** – Sets WRED Drop threshold type to discard in bytes or packets.
  - **packets –** Sets the WRED drop type to discard packets.
  - **Bytes -** Sets the WRED drop type to discard in terms of bytes.
- **ecn-threshold <short(0-65535)> -** Configures the ECN Threshold which defines the queue depth in bytes to stop marking and start dropping ECN eligible packets. This value ranges from 0 to 65535.
- **flag -** Configure additional action flags for WRED Drop profile.
  - **cap-average -** Sets the average queue size as always less than the actual queue size.
  - **mark-congestion -** Marks ECN instead of dropping.
  - **none** - Does not configures additional action flags for WRED Drop profile.

Mode	Queue Template Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	• mark-probability-denominator - 100 • exponential-weight – 0 • drop-threshold-type – packets
Example	**SEFOS(config-qtype)# random-detect dp 5 min-threshold 20 max-threshold 30 max-pkt-size 1 mark-probability-denominator 20 exponential-weight 31 gain 10 drop-threshold-type bytes ecn-threshold 1 flag none**
Related Command(s)	• **queue-type** - Creates a queue template type. • **set algo-type** - Sets Q template entry parameters.

- **`show queue-template –`** Displays the Q template and random detect configurations.

48.22 show qos global info

Command Objective	This command displays QoS-related global configurations.
Syntax	**show qos global info**
Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS# show qos global info** QoS Global Information ---------- System Control : Start System Control : Enable Rate Unit : kbps Rate Granularity : 64 Trace Flag : 0
Related Command(s)	• **shutdown qos** – Shuts down the QoS subsystem. • **qos** – Enables or disables the QoS subsystem.

48.23 show priority-map

Command Objective	This command displays the priority map entry.
Syntax	**show priority-map [<priority-map-id(1-65535)>]**
Parameter Description	• **<priority-map-id(1-65535)>** - Displays the output for the priority map index of the incoming packet received over ingress port or VLAN with specified incoming priority. This value ranges from 1 to 65535.
Mode	Privileged EXEC Mode.
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS# show priority-map** QoS Priority Map Entries ======================== PriorityMapId : 1 IfIndex : 1 VlanId : 4094 InPriorityType : VlanPriority InPriority : 0 RegenPriority : 7 InnerRegenPriority : 1 PriorityMapId : 9 IfIndex : Ex0/5 VlanId : 2 InPriorityType : IP Protocol InPriority : 1 RegenPriority : 5 InnerRegenPriority : 7
Note:	If executed without the optional parameters, this command displays all the available priority map information.
Related Command(s)	• **priority-map** – Adds a priority map entry. • **map** - Adds a priority map entry for mapping an incoming priority to a regenerated priority.

48.24 show class-map

Command Objective	This command displays the class map entry.
Syntax	**show class-map [<class-map-id(1-65535)>]**
Parameter Description	• **<class-map-id(1-65535)>** - Displays the class map configurations for the specified class map entry. This value ranges from 1 to 65535.
Mode	Privileged EXEC Mode.
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS# show class-map** QoS Class Map Entries ========== ClassMapId : 1 L2FilterId : None L3FilterId : None PriorityMapId : 1 CLASS : 1000 PolicyMapId : 1 PreColor : None Status : Active
Note:	If executed without the optional parameters, this command displays all the available class map information.
Related Command(s)	• **class-map** – Adds a class map entry. • **priority-map** – Adds a priority map entry.

48.25 show class-to-priority-map

Command Objective	This command displays the class group entry.
Syntax	**show class-to-priority-map <group-name(31)>**
Parameter Description	• **<group-name(31)>** - Displays the details of the unique identification of the group to which an input CLASS belongs.
Mode	Privileged EXEC Mode.
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS# show class-to-priority-map CLASS1** QoS Class To Priority Map Entries --------------------------------- GroupName : CLASS1 Class LocalPriority --------------------------------- 2 2
Related Command(s)	• **show class-map –** Displays the class map entry. • **set class** – Sets CLASS for L2 or L3 filters or both, or priority map ID, and adds a CLASS to priority map entry with regenerated priority.

48.26 show meter

Command Objective	This command displays the meter entry.
Syntax	**show meter [<meter-id(1-65535)>]**
Parameter Description	• **<meter-id(1-65535)>** - Displays the configurations for the index that enumerates the meter entries. This value ranges from 1 to 65535.
Mode	Privileged EXEC Mode.
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS# show meter** QoS Meter Entries ---------------- MeterId : 1 Type : SRTCM Color Mode : Color Blind Interval : None CIR : 20 CBS : 20 EIR : None EBS : 20 NextMeter : None Status : Active MeterId : 2 Type : Simple Token Bucket Color Mode : Color Blind Interval : None CIR : None CBS : None EIR : None EBS : None NextMeter : None Status : InActive
Note:	If executed without the optional parameters, this command displays all the

	available meter information.
Related Command(s)	• **`meter`** – Creates a meter. • **`meter-type`** - Sets meter parameters CIR, CBS, EIR, EBS, Interval, meter type, and color awareness. • **`set meter`** – Sets policy parameters such as meter and meter actions.

48.27 show policy-map

Command Objective	This command displays the policy map entry.
Syntax	**show policy-map [<meter-id(1-65535)>]**
Parameter Description	• **<meter-id(1-65535)>** - Specifies the index that enumerates the meter entry. This value ranges from 1 to 65535.
Mode	Privileged EXEC Mode.
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS# show policy-map** QoS Policy Map Entries ========== PolicyMapId : 1 IfIndex : 0 Class : 0 DefaultPHB : None. MeterId : 1 ConNClass : 0 ExcNClass : 0 VioNClass : 0 ConfAct : Port 1 ExcAct : Drop. VioAct : Drop.
Note:	If executed without the optional parameter, this command displays all the available policy map information.
Related Command(s)	• **set policy** – Sets CLASS for policy. • **policy-map** – Creates a policy map.

48.28 show queue-template

Command Objective	This command displays the Q Template and Random Detect configurations.
Syntax	**show queue-template [<queue-template-Id(1-65535)>]**
Parameter Description	• **<queue-template-Id(1-65535)>**–Displays the Q Template and Random Detect configurations for the specified queue template table index. This value ranges from 1 to 65535.
Mode	Privileged EXEC Mode.
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS# show queue-template** Queue Template Entries ---------- Q Template Id : 1 Q Limit : 10000 Drop Type : Tail Drop Drop Algo Status : Disable DP 2, MinTH 20, MaxTH 50, MaxPktSize 1000,MaxDropProb 10, ExpWeight 0, Gain 10, ECN Threshold 0 Drop threshold type : Discard Bytes RD Cfg Flag : cap-average mark-ecn DP 5, MinTH 10, MaxTH 40, MaxPktSize 1000,MaxDropProb 10, ExpWeight 0, Gain 1, ECN Threshold 0 Drop threshold type : Discard Packets Q Template Id : 10 Q Limit : 25 Drop Type : WRED Drop Algo Status : Enable DP 4, MinTH 10000, MaxTH 50000, MaxPktSize 1000,MaxDropProb 1, ExpWeight 0, Gain 0, ECN Threshold 30 Drop threshold type : Discard Packets
Note:	• If executed without the optional parameter, this command displays all the

	available queue template information. • This show command displays the Random Detect Parameters only if the Drop Algorithm type is configured using the `set algo-type` command.
Related Command(s)	• **`queue-type –`** Creates a queue template type. • **`set algo-type`** - Sets Q template entry parameters. • **`random-detect dp`** – Sets Random Detect Table entry parameters.

48.29 show shape-template

Command Objective	This command displays the shape template configurations.
Syntax	**show shape-template [<shape-template-Id(1-65535)>]**
Parameter Description	• **<shape-template-Id(1-65535)>** - Shape Template Table index.
Mode	Privileged EXEC Mode.
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS# show shape-template** QoS Shape Template Entries -------------------------- ShapeTemplate Id CIR CBS EIR EBS ---------- --- --- --- --- 1 1 1 1 1
Note:	If executed without the optional parameter, this command displays all the available shape template information.
Related Command(s)	• **shape-template** – Creates a shape template.

48.30 show scheduler

Command Objective	This command displays the configured scheduler.
Syntax	**show scheduler [interface <iftype> <ifnum>]**
Parameter Description	• **<iftype>** - Sets the type of interface for the outbound queue. The interface can be: ▪ **fastethernet** – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Mbits/sec. ▪ **XL-ethernet** – A version of LAN standard architecture that supports data transfer up to 1 Gbit/sec. ▪ **extreme-ethernet** – A version of Ethernet that supports data transfer up to 10 Gbits/sec. ▪ **internal-lan** – Internal LAN created on a bridge per IEEE 802.1ap. • **<ifnum>** - Sets the type of interface for the outbound queue. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan id is provided, for interface type internal-lan.
Mode	Privileged EXEC Mode.
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS# show scheduler** QoS Scheduler Entries ---------- IfIndex Scheduler Index Scheduler Algo Shape Index Scheduler HL GlobalId ------- --------- ---------- ---------- ---------- --------- Ex0/1 1 strictPriority 0 0 1
Note:	If executed without the optional parameter, this command displays all the available scheduler entries.
Related Command(s)	• **scheduler –** Creates a scheduler and configures the scheduler parameters.

48.31 show queue

Command Objective	This command displays the configured queues.
Syntax	**show queue [interface <iftype> <ifnum>]**
Parameter Description	• **<iftype>** - Sets the type of interface for the outbound queue. The interface can be: ▪ **fastethernet** – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Mbits/sec. ▪ **XL-ethernet** – A version of LAN standard architecture that supports data transfer up to 1 Gbit/sec. ▪ **extreme-ethernet** – A version of Ethernet that supports data transfer up to 10 Gbits/sec. ▪ **internal-lan** – Internal LAN created on a bridge per IEEE 802.1ap. • **<ifnum>** - Sets the type of interface for the outbound queue. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan id is provided, for interface type internal-lan.
Mode	Privileged EXEC Mode.
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS# show queue** QoS Queue Entries ---------- IfIndex Queue Idx Queue Type Scheduler Idx Weight Priority Shape Idx Global Id ------- --------- ---------- ------------- ------ -------- --------- --------- Ex0/1 1 1 1 1 1 1 1
Note:	If executed without the optional parameter, this command displays all the available queue entries
Related Command(s)	• **queue** – Creates a queue and configures the queue parameters. • **queue-type –** Creates a queue template type. • **show queue-template –** Displays the Q template and random detect

configurations.

48.32 show queue-map

Command Objective	This command displays the configured queue map.
Syntax	**show queue-map [interface <iftype> <ifnum>]**
Parameter Description	• **<iftype>** - Sets the type of interface for the outbound queue. The interface can be: ▪ **fastethernet** – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Mbits/sec. ▪ **XL-ethernet** – A version of LAN standard architecture that supports data transfer up to 1 Gbit/sec. ▪ **extreme-ethernet** – A version of Ethernet that supports data transfer up to 10 Gbits/sec. ▪ **internal-lan** – Internal LAN created on a bridge per IEEE 802.1ap. • **<ifnum>** - Sets the type of interface for the outbound queue. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan id is provided, for interface type internal-lan.
Mode	Privileged EXEC Mode.
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS# show queue-map** QoS Queue Map Entries ----------

```
IfIndex  CLASS   PriorityType  Priority Value  Mapped
Queue
---------- ---------- --------------- --------------- ----
-
Ex0/1      none       VlanPri         0               1
Ex0/1      none       VlanPri         1               2
Ex0/1      none       VlanPri         2               3
Ex0/1      none       VlanPri         3               4
Ex0/1      none       VlanPri         4               5
Ex0/1      none       VlanPri         5               6
Ex0/1      none       VlanPri         6               7
Ex0/1      none       VlanPri         7               8
```

```
Ex0/1       none        IPToS           1               1
Ex0/1       none        IPDSCP          1               1
Ex0/1       1           none            0               1
```

Note: If executed without the optional parameter, this command displays all the available queue map entries.

Related Command(s)

- **`queue-map`** – Creates a map for a queue with class or regenerated priority.

48.33 show sched-hierarchy

Command Objective	This command displays the configured hierarchy scheduler.
Syntax	**show sched-hierarchy [interface <iftype> <ifnum>]**
Parameter Description	• **<iftype>** - Sets the type of interface for the outbound queue. The interface can be: ▪ **fastethernet** – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Mbits/sec. ▪ **XL-ethernet** – A version of LAN standard architecture that supports data transfer up to 1 Gbit/sec. ▪ **extreme-ethernet** – A version of Ethernet that supports data transfer up to 10 Gbits/sec. ▪ **internal-lan** – Internal LAN created on a bridge per IEEE 802.1ap. • **<ifnum>** - Sets the type of interface for the outbound queue. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan id is provided, for interface type internal-lan.
Mode	Privileged EXEC Mode.
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS# show sched-hierarchy** QoS Hierarchy Scheduler Entries ------------------------------ IfIndex Hierarchy Level Sched Index NextQueue Id NextSched Id Weight Priority ------- --------------- ----------- ------------ ---------- ------ -------- Ex0/1 1 1 0 2 1 1
Note:	If executed without the optional parameter, this command displays all the available hierarchy scheduler entries
Related Command(s)	• **scheduler –** Creates a scheduler and configures the scheduler parameters. • **sched-hierarchy –** Creates a scheduler hierarchy.

48.34 show qos pbit-preference-over-Dscp

Command Objective	This command displays configured pbit reference for the tagged ports.
Syntax	**show qos pbit-preference-over-Dscp [interface <iftype> <ifnum>]**
Parameter Description	• **<iftype>** - Sets the type of interface for the outbound queue. The interface can be: ▪ **fastethernet** – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Mbits/sec. ▪ **XL-ethernet** – A version of LAN standard architecture that supports data transfer up to 1 Gbit/sec. ▪ **extreme-ethernet** – A version of Ethernet that supports data transfer up to 10 Gbits/sec. ▪ **internal-lan** – Internal LAN created on a bridge per IEEE 802.1ap. • **<ifnum>** - Sets the type of interface for the outbound queue. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan id is provided, for interface type internal-lan.
Mode	Privileged EXEC Mode.
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS# show qos pbit-preference-over-Dscp** QoS Default Pbit Preference Entries ----------
	IfIndex Pbit preference over DSCP -------- ----------
	Ex0/1 Enabled
Note:	If executed without the optional parameter, this command displays all the available scheduler entries
Related Command(s)	• **scheduler –** Creates a scheduler and configures the scheduler parameters. • **sched-hierarchy –** Creates a scheduler hierarchy.

48.35 show qos def-user-priority

Command Objective	This command displays the configured default ingress user priority for a port.
Syntax	**show qos def-user-priority [interface <iftype> <ifnum>]**
Parameter Description	• **<iftype>** - Sets the type of interface for the outbound queue. The interface can be: ▪ **fastethernet** – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Mbits/sec. ▪ **XL-ethernet** – A version of LAN standard architecture that supports data transfer up to 1 Gbit/sec. ▪ **extreme-ethernet** – A version of Ethernet that supports data transfer up to 10 Gbits/sec. ▪ **internal-lan** – Internal LAN created on a bridge per IEEE 802.1ap. • **<ifnum>** - Sets the type of interface for the outbound queue. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan id is provided, for interface type internal-lan.
Mode	Privileged EXEC Mode.
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS# show qos def-user-priority** QoS Default User Priority Entries ----------

```
IfIndex  Default User Priority
-------- ---------------------
Ex0/1              0
Ex0/2              0
Ex0/3              0
Ex0/4              0
Ex0/5              0
Ex0/6              0
Ex0/7              0
Ex0/8              0
Ex0/9              0
```

	Ex0/10	0
	Ex0/11	0
	Ex0/12	0
	Ex0/13	0
	Ex0/14	0
	Ex0/15	0
	Ex0/16	0
	Ex0/17	0
	Ex0/18	0
	Ex0/19	0
	Ex0/20	0
	Ex0/21	0
	Ex0/22	0
	Ex0/23	0
	Ex0/24	0

Note: If executed without the optional parameter, this command displays the available default ingress user priority entries for all the interface.

Related Command(s)

- **`qos interface`** – Sets the default ingress user priority for the port.

48.36 show qos meter-stats

Command Objective	This command displays the meters statistics for conform, exceed, violate packets, and octets count.
Syntax	**show qos meter-stats [<Meter-Id(1-65535)>]**
Parameter Description	• **<Meter-Id(1-65535)>** - Index that enumerates the meter entries.
Mode	Privileged EXEC Mode.
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS# show qos meter-stats** QoS Meter (Policer) Stats ------------------------- Meter Index : 1 Conform Packets : 00 Conform Octects : 00 Exceed Packets : 00 Exceed Octects : 00 Violate Packets : 00 Violate Octects : 0
Note:	If executed without the optional parameter, this command displays the meter statistics for all the available meters.
Related Command(s)	• **show meter –** Displays the meter entry. • **set meter** – Sets policy parameters such as meter and meter actions.

48.37 show qos queue-stats

Command Objective	This command displays queue statistics for EnQ, DeQ, discarded packets and octets count, Management Algo Drop, and Q occupancy.
Syntax	**show qos queue-stats [interface <iftype> <ifnum>]**
Parameter Description	• **<iftype>** - Sets the type of interface for the outbound queue. The interface can be: ▪ **fastethernet** – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Mbits/sec. ▪ **XL-ethernet** – A version of LAN standard architecture that supports data transfer up to 1 Gbit/sec. ▪ **extreme-ethernet** – A version of Ethernet that supports data transfer up to 10 Gbits/sec. ▪ **internal-lan** – Internal LAN created on a bridge per IEEE 802.1ap. • **<ifnum>** - Sets the type of interface for the outbound queue. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan id is provided, for interface type internal-lan.
Mode	Privileged EXEC Mode.
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS# show qos queue-stats** QoS Queue Stats ------------------ Interface Index : Ex0/1 Queue Index : 2 EnQ Packets : 00 EnQ Octects : 00 DeQ Packets : 00 DeQ Octects : 00 Discard Packets : 00 Discard Octects : 00 Occupancy Octects : 00 CongMgntAlgoDrop Octects : 00

	Note: If executed without the optional parameter, this command displays the queue statistics for all the available Interfaces.
Related Command(s)	• **`show queue`** – Displays the configured queues.

48.38 debug qos

Command Objective	This command sets the debug level for QOS module. The no form of the command resets the debug level for QoS module.
Syntax	**debug qos {initshut | mgmt | ctrl | dump | os | failall | buffer}** **no debug qos {initshut | mgmt | ctrl | dump | os | failall | buffer}**
Parameter Description	• **initshut** - Generates debug statements for Init and shutdown traces. • **mgmt** - Generates debug statements for management traces. • **ctrl** - Generates debug statements for control plane traces. • **dump** - Generates debug statements for packet dump traces. • **os** - Generates debug statements for traces related to all resources except buffers. • **failall** - Generates debug statements for all failure traces. • **buffer** - Generates debug statements for buffer allocation or release traces.
Mode	Privileged EXEC Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS# debug qos initshut**

48.39 qos pbit-preference

Command Objective	This command sets pbit preference value. Setting this to enable indicates that if a frame includes both 802.1p and a DSCP field, then the pbit field takes precedence. For DSCP to take precedence, set to disable.
Syntax	`qos pbit-preference {enable | disable}`
Parameter Description	• **`enable`** – Enables the feature. • **`disable`** – Disables the feature.
Mode	Interface Configuration mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Default	Disabled
Example	`SEFOS(config-if)# qos pbit-preference enable`

48.40 cpu rate limit queue

Command Objective	This command is used to configure rates for a CPU port queues.
Syntax	**cpu rate limit queue <integer(1-65535)> minrate <integer(1-65535)> maxrate <integer(1-65535)>**
Parameter Description	• **<integer(1-65535)>** - Queue identifier that uniquely identifies the queue in the system or port. This value ranges from 1 to 65535. • **minrate <integer(1-65535)>** - Minimum transmission rate on a CPU port. This value ranges from 1 to 65535. Minimum rate must be less than or equal to maximum rate. • **maxrate <integer(1-65535)>** - Maximum transmission rate on a CPU port. This value ranges from 1 to 65535. Maximum rate must be greater than or equal to minimum rate.
Mode	Global Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	Enabled
Example	**SEFOS(config)# cpu rate limit queue 1 minrate 10 maxrate 100**
Related Command(s)	• **Show cpu rate limit** – Display the rate limiting values for CPU.

48.41 show cpu rate limit

Command Objective	This command displays the rate limiting values for CPU.
Syntax	**show cpu rate limit**
Parameter Description	• **<iftype>** - Sets the type of interface for the outbound queue. The interface can be: ▪ **fastethernet** – Officially referred to as 100BASE-T standard. This is a version of LAN standard architecture that supports data transfer up to 100 Mbits/sec. ▪ **XL-ethernet** – A version of LAN standard architecture that supports data transfer up to 1 Gbit/sec. ▪ **extreme-ethernet** – A version of Ethernet that supports data transfer up to 10 Gbits/sec. ▪ **internal-lan** – Internal LAN created on a bridge per IEEE 802.1ap. • **<ifnum>** - Sets the type of interface for the outbound queue. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface type other than internal-lan and port-channel. Only i-lan id is provided, for interface type internal-lan.
Mode	Privileged EXEC Mode.
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS# show cpu rate limit** QoS CPU Queue Rate Limit Table ------------------------------ Queue ID MinRate MaxRate -------- ------- ------- 1 1 65535 2 1 65535 3 1 65535 4 1 65535 5 1 65535 6 1 65535 7 1 65535 8 1 65535
Related Command(s)	• **cpu rate limit queue** – Configure rates for a CPU port queues.

48.42 mls qos

Command Objective	This command enables multilayer security QoS. The no form of the command disables the multilayer security QoS.
Note:	This command is a standardized implementation of the existing command **qos**. Its operation is similar to the existing command.
Syntax	**mls qos** **no mls qos**
Mode	Global Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS(config)# mls qos**

48.43 mls qos aggregate-policer

Command Objective	This command defines an aggregate policer and configures the policer parameters.
Note:	This command is a standardized implementation of the existing command **set meter**. Its operation is similar to the existing command.
Syntax	**mls qos aggregate-policer <meter-id (1-65535)> <Bits per second (1-65535)> <Normal burst bytes (1-65535)> exceed-action {drop | set-ip-dscp-transmit}**
Parameter Description	• **<meter-id(1-65535)>** - Configures the meter table identifier which is the index for the meter table. This value ranges from 1 to 65535. • **<Bits per second (1-65535)>** - Configures the average traffic rate in bits per second. This value ranges from 1 to 65535. • **<Normal burst bytes (1-65535)>** - Configures the normal burst size in bytes. This value ranges from 1 to 65535. • **exceed-action** - Configures the action to be performed on the packet, when the packets are found to be in profile (exceed). Options are: ▪ **drop** – Drops the packet. ▪ **set-ip-dscp-transmit** – Changes the DSCP of the packet to that specified in policed DSCP map.
Mode	Global Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	**SEFOS(config)# mls qos aggregate-policer 1 10 10 exceed-action drop**