

August 2015

Copyright @ 2015, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS. Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit <a href="http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit <a href="https://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit <a href="https://www.oracle.com/pls/topic/loo

Copyright © 2015, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf stipulation expresse de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique:

U.S. GOVERNMENT END USERS. Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée d'The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers, sauf mention contraire stipulée dans un contrat entre vous et Oracle. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation, sauf mention contraire stipulée dans un contrat entre vous et Oracle.

Accessibilité de la documentation

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité à la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Accès au support électronique

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info ou le site http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info ou le site <a href="http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info ou le site <a href="http://www.oracle.com/pls/

.

Contents

Using This Documentation6			
47. ACL		9	
47.1 aclcm	nd	10	
47.1.1	ip access-list		
47.1.2	mac access-list extended	13	
47.1.3	ipv6 access-list extended	14	
47.1.4	permit	15	
47.1.5	deny	16	
47.1.6	permit- ip/ospf/pim/protocol type	17	
47.1.7	deny - ip/ospf/pim/protocol type	21	
47.1.8	permit tcp	25	
47.1.9	deny tcp	30	
47.1.10	permit udp	35	
47.1.11	deny udp	40	
47.1.12	permit icmp	45	
47.1.13	deny icmp	48	
47.1.14	ip access-group	51	
47.1.15	mac access-group	52	
47.1.16	ipv6 access-group	53	
47.1.17	permit - MAC	54	
47.1.18	deny - MAC	57	
47.1.19	show access-lists	60	
47.1.20	permit- ospf/pim/protocol type – ipv6	65	
47.1.21	deny- ospf/pim/protocol type- ipv6	67	
47.1.22	permit tcp- ipv6	69	
47.1.23	deny- tcp- ipv6	72	
47.1.24	permit udp- ipv6	75	
47.1.25	deny udp- ipv6	78	
47.1.26	permit icmp- ipv6	81	
47.1.27	deny icmp– ipv6	84	
47.2 aclm	et	87	
47.2.1	ip access-list	88	
47.2.2	mac access-list extended	90	
47.2.3	permit - standard mode	91	
47 2 4	deny - standard mode	92	

	47.2	2.5	permit- ip/ospf/pim/protocol type	93
	47.2	2.6	deny - ip/ospf/pim/protocol type	96
	47.2	2.7	permit tcp	99
	47.2	2.8	deny tcp	103
	47.2	2.9	permit udp	107
	47.2	2.10	deny udp	111
	47.2	2.11	permit icmp	115
	47.2	2.12	deny icmp	118
	47.2	2.13	ip access-group	121
	47.2	2.14	mac access-group	122
	47.2	2.15	permit	123
	47.2	2.16	deny	126
	47.2	2.17	show access-lists	129
48	3. QoSX			133
	48.1	shutdo	own qos	134
	48.2	gos		135
	48.3 p	oriority	y-map	136
	48.4	-class	map	137
	48.6 p	oolicy-	-map	139
	48.7	queue	p-type	140
	48.8	shape	-template	141
		•	uler	
		•	map	
			-hierarchy	
			terface	
		•		
		•	access-group	
			ass	
			-type	
			licy	
			eter	
			go-type	
			m-detect dp	
			qos global info	
			priority-map	
	-10.∠0 3	31 10 VV	ριοιτή παρ	170

10 01	show along man	171
	show class-map	
48.25	show class-to-priority-map	172
48.26	show meter	173
48.27	show policy-map	175
48.28	show queue-template	176
48.29	show shape-template	178
48.30	show scheduler	179
48.31	show queue	180
48.32	show queue-map	182
48.33	show sched-hierarchy	184
48.34	show qos pbit-preference-over-Dscp	185
48.35	show qos def-user-priority	186
48.36	show qos meter-stats	188
48.37	show qos queue-stats	189
48.38	debug qos	191
48.39	qos pbit-preference	192
48.40	cpu rate limit queue	193
48.41	show cpu rate limit	194
48.42	mls qos	195
48.43	mls qos aggregate-policer	196

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:

- ip access-list
- mac access-list extended
- ipv6 access-list extended
- permit
- deny
- permit- ip/ospf/pim/protocol type
- deny ip/ospf/pim/protocol type
- permit tcp
- deny tcp
- permit udp
- deny udp
- permit icmp
- deny icmp
- ip access-group
- mac access-group
- ipv6 access-group
- permit MAC
- deny MAC
- show access-lists
- permit- ospf/pim/protocol type ipv6
- deny- ospf/pim/protocol type- ipv6
- permit tcp- ipv6
- deny- tcp- ipv6
- permit udp– ipv6
- deny udp– ipv6
- permit icmp— ipv6
- deny icmp- ipv6

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 <code>ip access-list</code> command is used.
	The no form of the command deletes the IP access-list.
Syntax	<pre>ip access-list {standard <access-list-number (1-10)=""> extended <access-list-number (11-1024)=""> }</access-list-number></access-list-number></pre>
	no ip access-list {standard <access-list-number (1-10=""> extended <access-list-number (11-1024)=""> }</access-list-number></access-list-number>
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.</access-list-number>
	 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.</access-list-number>
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)=""></access-list-number>	
	no mac access-list extended <short (1-1024)=""></short>	
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)=""></access-list-number>	
	no ipv6 access-list extended <access-list-number (11-1024)=""></access-list-number>	
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	<pre>permit { any host <src-ip-address> <src-ip-address> <mask> } { any host <dest-ip-address> <dest-ip-address> <mask> }</mask></dest-ip-address></dest-ip-address></mask></src-ip-address></src-ip-address></pre>	
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> < src-ip-address > <mask> - Permits packets with the specified source IP address and the network mask to be used with the source IP address.</mask> </mask></src-ip-address> any host <dest-ip-address> < dest-ip-address > <mask> -</mask></dest-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	<pre>deny{ any host <src-ip-address> <src-ip-address> <mas <dest-ip-address="" any="" host="" {="" ="" }=""> <dest-ip-address> <mas pre="" }<=""></mas></dest-ip-address></mas></src-ip-address></src-ip-address></pre>	
Parameter Description	 any host <src-ip-address> < src-ip-address ><mask> -</mask></src-ip-address> 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> 	
	 < src-ip-address> <mask> - Denies packets with the specified source IP addressand the network mask to be used with the source IP address.</mask> 	
	 any host <dest-ip-address> < dest-ip-address > <mask>-</mask></dest-ip-address> 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> 	
	 < dest-ip-address> <mask> - Denies packets with the specified destination IP address and the network mask for the given destination IP address.</mask> 	
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.
- col-type (1-255)> Configures the type of protocol to be checked against the packet. It can also be a protocol number.

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
 - 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.
- - 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.

Chapter 47 ACL 19

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

> 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.

> This feature has been included to adhere to the Note: 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.

ACL Extended Access List Configuration Mode Mode Workgroup, Enterprise, Metro_E, and Metro **Package** 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. SEFOS (config-ext-nacl) # permit 255 12.0.0.1 255.0 any Example 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.

20

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 number. This value ranges from 1 to 255.

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
 - 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.
- 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.

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.

> 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 Workgroup, Enterprise, Metro_E, and Metro • 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

Lxampic

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)> | fany | host <dest-ip-address> | dest-ip-address> <dest-mask> }[{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <port-number (1-65535)> | fack | 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.
- 1t <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.
- 1t <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.

- 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.

28

Mode	ACL Extended Access List Configuration Mode	
Package	Workgroup, Enterprise, Metro_E, and Metro	
Defaults	tos-value - 0dscp - 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

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.
- 1t <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-</pre>

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.
- 1t <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
 - 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.
- - 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.

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.

> 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.

> 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.

> This feature has been included to adhere to the Note: 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.

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

ACL Extended Access List Configuration Mode

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-</pre> 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-</pre> mask> }[{ gt <port-number (1-65535)> | lt <port-number (1-</pre> 65535)>| eq <port-number (1-65535)>| range <port-number 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.
- 1t <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-</pre> 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.
- 1t <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 $\langle (1-7) \rangle$ 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.
- cedence (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	• dscp1	
	• 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

- 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.
- 1t <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.
- 1t <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.

> 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.

> This feature has been included to adhere to the Note: 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.

> 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	dscp1priority - 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	<pre>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)>]</short></short></mask></dest-ip-address></dest-ip-address></mask></src-ip-address></src-ip-address></pre>		

- 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:

moddago typed 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

	18 255	Address Mask Reply No ICMP type
	code to be matches	e-code <short (0-255)=""> - Configures the ICMP message be checked against the packet. The packet will be allowed if it the message code. This value ranges from 0 to 255. Some of the essage codes are:</short>
	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
	used who	Ly < (1-7) >— Configures the priority value of the L3 filter to be en the packet matches more than one filter rule. Higher value of prity' implies a higher priority. This value ranges from 1 to 7.
Mode	ACL Extende	ed Access List Configuration Mode
Package	Workgroup, E	Enterprise, Metro_E, and Metro
Defaults	• priority -	1
	• dscp – 1	
	• message	e-type / message code - 255
Example	SEFOS (com	nfig-ext-nacl)# permit icmp any 13.0.0.1 255.0 25 y 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	<pre>deny icmp {any host <src-ip-address> <src-ip-address></src-ip-address></src-ip-address></pre>	

- 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:

	3
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

Package Defaults	vvorkgroup,	Enterprise, Metro_E, and Metro
Mode		led Access List Configuration Mode
	used wh	ty < (1-7) >— Configures the priority value of the L3 filter to be nen the packet matches more than one filter rule. Higher value of iority' implies a higher priority. This value ranges from 1 to 7.
	255	No ICMP Code
	12	Host Unreachable TOS
	11	Network Unreachable TOS
	10	Destination Host Administratively Prohibited
	9	Destination Network Administratively Prohibited
	8	Source Host Isolated
	7	Destination Host Unknown
	6	Destination Network Unknown
	5	Source Route Fail
	4	Fragment Need
	3	Port Unreachable
	2	Protocol Unreachable
	1	Host Unreachable
	0	Network Unreachable
	Value	ICMP code
	code to matches	be checked against the packet. The packet will be denied if it is with the message code. This value ranges from 0 to 255. Some IP message codes are:
	255	No ICMP type
	18	Address Mask Reply
	17	Address Mask Request
	16	Information Reply
	15	Information Request

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}</access-list-number>	
	no ip access-group <access-list-number (1-1024)=""> {in out}</access-list-number>	
Parameter Description	• <access-list-number (1-1024)="">— Configures the IP access control list number on the interface. This value ranges from 1 to 1024.</access-list-number>	
	• 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</access-list-number>	
	no mac access-group <access-list-number (1-1024)=""> in</access-list-number>	
Parameter Description	 <access-list-number (1-1024)="">— Configures the MAC access control list number on the interface. This value ranges from 1 to 1024.</access-list-number> 	
	• 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</access-list-number>
	no ipv6 access-group <access-list-number (11-1024)=""> in</access-list-number>
Parameter Description	 <access-list-number (11-1024)="">— Configures the IPv6 access control list number on the interface. This value ranges from 11 to 1024.</access-list-number>
	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 <destmac-address> }[aarp | amber | dec-spanning | decnet-iv |
diagnostic | dsm | etype-6000|etype-8042 | lat | lavc-sca |
mop-console | mop-dump | msdos | mumps | netbios | vinesecho | vines-ip | xns-id | <protocol (0-65535)> [Vlan
<vlan-id (1-4094)>][user-priority <value (0-7)>] [priority
value (1-7)>]

- 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.

- 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.
- cool (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)>]

- 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	• <pre>- <pre>- <pre>protocol (0-65535)> - 0</pre></pre></pre>
	priority - 1

Note:	MAC access list must have been created.	
Example	SEFOS (config-ext-macl)# permit any host 00:11:22:33:44:5 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 conf	iguration.
Syntax	show access-lists [{ip <access-l (1-1024)="" <access-list-number=""> 1024)>}]</access-l>	
Parameter Description	• ip <access-list-number (1-102="" 1024.<="" access="" configuration="" for="" ip="" specified="" th="" the=""><th></th></access-list-number>	
	 mac <access-list-number (1-10<br="">configuration for the specified MAC acce and 1024.</access-list-number> 	• •
	 < access-list-number (1-1024) configuration for the specified user defined 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

: 7 Filter Priority

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

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

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	<pre>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)="">]</value></value></value></dst-prefix-len></dst-ipv6-addr></src-prefix-len></src-ipv6-addr></protocol-type></pre>
Parameter Description	ospf – Permits packets for OSPF protocol. prime Permits packets for PIM 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.</protocol-type>
	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-ipv6-addr>
	 <src-prefix-len (0-128)=""> - Configures the prefix length for the source IPv6 address. This value ranges from 0 and 128.</src-prefix-len>
	 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.</dst-prefix-len>
	 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.</value>
	 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	<pre>deny [{ospf pim <protocol-type (0-255)="">}] {any host</protocol-type></pre>	
Parameter Description	ospf – Discards packets for OSPF protocol.	
	• pim – Discards packets for PIM protocol.	
	 <pre>protocol-type (1-255)> - Discards packets for the specified protocol number. This value ranges from 1 to 255.</pre> 	
	 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-ipv6-addr> 	
	 <src-prefix-len (0-128)=""> - Configures the prefix length for the source IPv6 address. This value ranges from 0 and 128.</src-prefix-len> 	
	 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.</dst-prefix-len> 	
	 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.</value> 	
	 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</pre> (0-128)>] [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <startport-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-</pre> 65535)> <end-port-range (1-65535)>}] [{ ack | rst }] [{tos {max-reliability | max-throughput | min-delay | normal $|\langle value (0-7)\rangle | dscp \langle value (0-63)\rangle | [flow-label]$ <value (0-1048575)>] [priority <value (1-7)>]

- 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.
- 1t <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 (0128)>] [{gt <port-number (1-65535)> | lt <port-number (165535)> | eq <port-number (1-65535)> | range <start-portrange (1-65535)> <end-port-range (1-65535)>}] {any | host
<dst-ipv6-addr>} [<dst-prefix-len (0-128)>] [{ gt <portnumber (1-65535)> | lt <port-number (1-65535)> | eq <portnumber (1-65535)> | range <start-port-range (1-65535)>
<end-port-range (1-65535)>}] [{ ack | rst }] [{tos {maxreliability | max-throughput | min-delay | normal | <value
(0-7)>} | dscp <value (0-63)>}] [flow-label <value (01048575)>] [priority <value (1-7)>]

- 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.
- 1t <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.
- 1t <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</pre> (0-128)>] [{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> | range <startport-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-</pre> 65535)> <end-port-range (1-65535)>}] [dscp <value (0-63)>] [flow-label $\langle value\ (0-1048575) \rangle$] [priority $\langle value\ (1-7) \rangle$]

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.
- 1t <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-</pre> 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.
- 1t <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)> | range <start-port-range (1-65535)> | eq <port-number (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)> | cend-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.
- 1t <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.
- 1t <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		nd specifies the ICMP packets to be forwarded based on the IP the associated parameters.
Syntax	len (0-128 len (0-128 message-co	<pre>ap {any host <src-ipv6-addr>} [/ <src-prefix- 3)>] {any host <dst-ipv6-addr>} [/<dst-prefix- 3)>] [message-type <message-type (0-255)=""> ode <message-code (0-255)="">] [dscp <value (0-63)="">] ol <value (0-1048575)="">] [priority <value (1-7)="">]</value></value></value></message-code></message-type></dst-prefix- </dst-ipv6-addr></src-prefix- </src-ipv6-addr></pre>
Parameter Description	specified	nost <src-ipv6-addr> - Permits the ICMPv6 packet with the source IPv6 address. The sources are: - Permits ICMPv6 packets from any source.</src-ipv6-addr>
		t <src-ipv6-addr> - Permits ICMPv6 packets with the cified host source IPv6 address.</src-ipv6-addr>
		-prefix-len (0-128)> - Specifies the prefix length of the Pv6 address. This value ranges from 0 to 128.
		nost <dst-ipv6-addr> - Permits the ICMPv6 packet with the source IPv6 address. The sources are:</dst-ipv6-addr>
	• any	- Permits ICMPv6 packets from any destination.
		t < dst-ipv6-addr > - Permits ICMPv6 packets with the cified host destination IPv6 address.
		prefix-len (0-128)> - Specifies the prefix length of the on IPv6 address. This value ranges from 0 to 128.
	message if it match	e-type <message-type (0-255)=""> - Configures the ICMPv6 type to be checked against the packet. The packet will be allowenes the message type. This value ranges from 0 to 255. Some of Pv6 message types are:</message-type>
	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

Information Request

15

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	<pre>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)="">]</value></value></value></message-code></message-type></dst-prefix-len></dst-ipv6-addr></src-prefix-len></src-ipv6-addr></pre>

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:

	, eee a.g, p ee a.e.
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:

- ip access-list
- mac access-list extended
- permit standard mode
- deny standard mode
- permit- ip/ospf/pim/protocol type
- deny ip/ospf/pim/protocol type
- permit tcp
- deny tcp
- permit udp
- deny udp
- permit icmp
- deny icmp
- ip access-group
- mac access-group
- permit
- deny
- show access-lists

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.
	The no form of the command deletes the IP access list.
Syntax	<pre>ip access-list {standard <access-list-number (1-1000)=""> extended <access-list-number (1001-65535)=""> }</access-list-number></access-list-number></pre>
	no ip access-list {standard <access-list-number (1-1000)=""> extended <access-list-number (1001-65535)=""> }</access-list-number></access-list-number>
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.</access-list-number>
	 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.</access-list-number>
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)=""></access-list-number>
	no mac access-list extended <short (1-65535)=""></short>
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	<pre>permit { any host <src-ip-address> <network-src-ip> <mask> } [{ any host <dest-ip-address> <network-dest-ip> <mask> }]</mask></network-dest-ip></dest-ip-address></mask></network-src-ip></src-ip-address></pre>
Parameter Description	 any host <src-ip-address> < src-ip-address> <mask> - Permits traffic with the specified source address. The sources are:</mask></src-ip-address> any - Permits packets from any source.
	 host <src-ip-address> - Permits packets with the specified host source IPv4 address.</src-ip-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.</mask></network-src-ip>
	 any host <dest-ip-address> < dest-ip-address > <mask>-</mask></dest-ip-address> 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>
	<network-dest-ip> <mask> - Permits packets with the specified destination IP address and the network mask for the given destination IP address.</mask></network-dest-ip>
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	<pre>deny{ any host <src-ip-address> <network-src-ip> <mask> } [{ any host <dest-ip-address> <network-dest-ip> <mask> }]</mask></network-dest-ip></dest-ip-address></mask></network-src-ip></src-ip-address></pre>
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.</src-ip-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.</mask></network-src-ip> </mask></network-src-ip></src-ip-address> any host <dest-ip-address> <network-dest-ip> <mask> -</mask></network-dest-ip></dest-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 $|\langle value\ (0-7)\rangle |\ dscp\ \langle value\ (0-63)\rangle \}$] [priority $\langle value\$ (1-255)>] [svlan-id <vlan-id (1-4094)>] [svlan-priority $\langle value\ (0-7)\rangle$ [$cvlan-id\ \langle vlan-id\ (1-4094)\rangle$ [$cvlan-id\ \langle vlan-id\ (1-4094)\rangle$] 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.
- col-type (1-255) > Configures the type of protocol to be checked against the packet. It can also be a protocol number.

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.
- $\langle value (0-7) \rangle$ 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
	• dscp1
	• svlan-id - 0
	• svlan-priority1
	• cvlan-id - 0
	• cvlan-priority1
	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-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

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.
- $\langle value (0-7) \rangle$ 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-priority1
	• cvlan-id - 0
	• cvlan-priority1
	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-</pre> 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|mindelay|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-</pre> 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.
- 1t <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-</pre> 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.
- 1t <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.

	55 1
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-priority1
	• cvlan-id - 0
	• cvlan-priority1
	single-tag double-tag - Single tag
Example	SEFOS(config-ext-nacl)# permit tcp any 10.0.0.1 255.255.255
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

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.
- 1t <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.
- 1t <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

	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-priority1

cvlan-id - 0 cvlan-priority - -1 single-tag | double-tag - Single tag SEFOS(config-ext-nacl) # deny tcp 100.0.0.10 255.255.255.0 **Example** 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-ipaddress> <src-mask>} [{gt <port-number (1-65535)> | 1t
<port-number (1-65535)> | eq <port-number (1-65535)> |
range <port-number (1-65535)> | cont-number (1-65535)> |
any | host <dest-ip-address> | <dest-ip-address> | <destmask> } [{ gt <port-number (1-65535)> | 1t <port-number
(1-65535)> | eq <port-number (1-65535)> | range <portnumber (1-65535)> | cont-number (1-65535)> | [{tos{max-reliability|max-throughput|min-delay|normal|<tos-value(07)>} | dscp <value (0-63)>}] [priority <value (1-255)>] [
svlan-id <vlan-id (1-4094)>] [svlan-priority <value (07)>] [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.
- 1t <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.
- 1t <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.

		tagged packets.
Mode		ACL Extended Access List Configuration Mode
Package		Metro_E and Metro
Defaults		• svlan-id - 0
		• svlan-priority1
		• cvlan-id - 0
		• cvlan-priority1
		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)> | 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)> | eq <port-number (1-65535)> | ftos{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.
- 1t <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.
- 1t <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.

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

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:

"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	<pre>permit icmp {any host <src-ip-address> <src-ip-address></src-ip-address></src-ip-address></pre>

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:

ICMP code
Network Unreachable
Host Unreachable
Protocol Unreachable
Port Unreachable
Fragment Need
Source Route Fail
Destination Network Unknown
Destination Host Unknown
Source Host Isolated
Destination Network Administratively Prohibited
Destination Host Administratively Prohibited
Network Unreachable TOS
Host Unreachable TOS
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

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-priority1
	• cvlan-id - 0
	• cvlan-priority1
	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
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

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.
ip access-group <access-list-number (1-65535)=""> {in out}</access-list-number>
<pre>no ip access-group [<access-list-number (1-65535)="">] {in out}</access-list-number></pre>
 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.
Interface Configuration Mode
Metro_E and Metro
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.
SEFOS (config-if)# ip access-group 1 in
ip access-list - Creates IP ACLs and enters the IP access list
configuration mode.

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}</access-list-number>
	<pre>no mac access-group [<access-list-number (1-65535)="">] {in out}</access-list-number></pre>
Parameter Description	 <access-list-number (1-65535)="">— Configures the MAC access control list number on the interface. This value ranges from 1 to 65535.</access-list-number>
	• 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 <destmac-address> } [{ aarp | amber | dec-spanning | decnetiv | 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)>] [{ singletag | double-tag }]

Parameter Description

- anylhost <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 datalink 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 <destmac-address> } [{ aarp | amber | dec-spanning | decnetiv | 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</pre> (1-4094)>] [cvlan-priority <priority (0-7)>] [svlanpriority <value (0-7)>] [{ single-tag | double-tag }] Parameter any | host <src-mac-address > - Source MAC address to be Description 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 datalink 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 - 0priority - 1
	outerEtherType - 0
	• svlan-id - 0
	• cvlan-priority1

	• svlan-priority1
	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' co	ກາເເງພາສແບກ.
Syntax	<pre>show access-lists [[{ip mac}] 65535)>]</pre>	<pre><access-list-number (1-<="" pre=""></access-list-number></pre>
Parameter Description	• ip – Displays the access list configura	tion for the specified IP access list.
	 mac - Displays the access list configuration. 	ation for the specified MAC access
	 < access-list-number (1-65535) access list configuration for the specific 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	
	Destination IP address mask	
	Destination IP Prefix Length	: 0
	Flow Identifier	: 0
	In Port List	: NIL
	Out Port List	: NIL
		: NIL : Deny
	Out Port List	: NIL

: 1 Filter Priority Filter Protocol Type : ANY IP address Type : IPV4 Source IP address : 0.0.0.0 Source IP address mask : 0.0.0.0 : 0 Source IP Prefix Length 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 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)></priority-map-id(1-65535)>
	no priority-map <pri>priority-map-Id(1-65535)></pri>
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)></class-map-id(1-65535)>
	no class-map <class-map-id(1-65535)></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)></meter-id(1-65535)>
	no meter <meter-id(1-65535)></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)></policy-map-id(1-65535)>
	no policy-map <policy-map-id(1-65535)></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)></q-template-id(1-65535)>
	no queue-type <q-template-id(1-65535)></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)>]</integer(0-10485760)></integer(0-10485760)></integer(0-10485760)></integer(1-10485760)></integer(1-65535)>
	no shape-template <shape-template-id(1-65535)></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.</integer(1-65535)>
	 cir<integer(1-10485760) -="" committed="" configures="" information="" rate<br="" the="">for packets through the queue. This value ranges from 1 to 10485760. cir should be less than eir.</integer(1-10485760)>
	 cbs<integer (0-10485760)=""> - Configures the committed burst size for packets through the queue. This value ranges from 0 to 10485760.</integer>
	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.</integer(0-10485760)>
	 ebs<integer(0-10485760)> - Configures the excess burst size for packets through the hierarchy. This value ranges from 0 to 10485760.</integer(0-10485760)>
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.</integer(0-65535)>
	 hierarchy-level<integer(0-10)> - Depth of the queue or scheduler hierarchy. This value ranges from 0 to 10.</integer(0-10)>
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	<pre>queue <integer(1-65535)> interface <iftype> <ifnum> [qtype</ifnum></iftype></integer(1-65535)></pre>
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.</integer> 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.</integer> scheduler<integer (1-65535)=""> - Scheduler identifier that manages the specified queue. This value ranges from 1 to 65535.</integer> 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. </integer> priority<integer (0-15)=""> - User assigned priority for the CoS queue. This value ranges from 0 to 15.</integer> shaper<integer (0-65535)=""> - Shaper identifier that specifies the bandwidth requirements for the queue. This value ranges from 0 to 65535.</integer> unicast - Unicast queue to store known unicast packets. multicast - Multicast queue to store DLF, multicast, broadcast, and
Mode	mirrored packets. 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 gueue 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.

> 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 asMPLS 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 gueue. 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-levelqueue <integer(0-65535)> | next-level-scheduler
<integer(0-65535)>} [priority <integer(0-15)>] [weight
<integer(0-1000)>]

no sched-hierarchy interface <iftype> <ifnum> hierarchylevel <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.</integer(0-1000)>
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)></integer(0-7)></ifnum></iftype>
Parameter Description	• <iftype> - Sets the type of interface for the outbound queue. The interface can be:</iftype>
	 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.</ifnum>
	 def-user-priority <integer(0-7)> - Default ingress user priority for the port.</integer(0-7)>
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.</integer(0-7)>
Mode	Priority Map Configuration Mode
Package	Workgroup, Enterprise, Metro_E, and Metro
Defaults	• vlan - 0
	in-priority-type - vlanPri
	• in-priority1
	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	<pre>match access-group { [mac-access-list <integer(0-65535)>] [ip-access-list <integer(0-65535)>] priority-map <integer(0-65535)> }</integer(0-65535)></integer(0-65535)></integer(0-65535)></pre>
Parameter Description	 mac-access-list <integer(0-65535)> - Identifier of the MAC filter.</integer(0-65535)> 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.</integer(0-65535)>
	 priority-map <integer(0-65535)> - Priority map identifier for mapping incoming priority against received packet. This value ranges from 0 to 65535.</integer(0-65535)>
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	<pre>set class <class integer(1-65535)=""> [pre-color { green yellow red none }] [regen-priority <integer(0-7)> group-name <string(31)>]</string(31)></integer(0-7)></class></pre>
	no set class <pre><class integer(1-65535)=""></class></pre>
Parameter Description	• <class integer(1-65535)=""> - Traffic CLASS to which an incoming frame pattern is classified.</class>
	 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.</integer(0-7)>
	 group-name <string(31)> - Unique identification of the group to which an input CLASS belongs.</string(31)>
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	<pre>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)>]</integer(0-65535)></integer(0-10485760)></integer(0-></integer(0-10485760)></integer(0-></short(1-10000)></pre>

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. Meter Configuration Mode 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-</pre> 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. This value can be overwritten by the meter used for the policy map. Mode Policy Map Configuration Mode Workgroup, Enterprise, Metro_E, and Metro Package Defaults class - 0 SEFOS(config-ply-map)# set policy class 1 interface Example 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 { costransmit-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-exptransmit <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-</pre> de-set <short(0-1)> | set-inner-vlan-pri <short(0-7)> setinner-vlan-de <short(0-1)> | set-mpls-exp-transmit <short(0-7)> | set-ip-prec-transmit <short(0-7)> | set-ipdscp-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)> | innervlan-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-ipdscp-transmit <short(0-63)> }] [set-conform-newclass <integer(0-65535)>] [set-exceed-newclass <integer(0-</pre> 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 costransmit-set 5 exceed-action cos-transmit-set 5 set-conform-newclass 100 set-exceed-newclass 100 set-violatenewclass 10
Related Command(s)	Show policy-map - Displays the policy map entry.

48.20 set algo-type

Command Objective Syntax	This command configures Q template entry parameters. set algo-type { tailDrop headDrop red wred } [queue-limit <integer(1-12582720)>] [queue-drop-algo {enable disable }]</integer(1-12582720)>
Syntax	<pre>limit <integer(1-12582720)>] [queue-drop-algo {enable </integer(1-12582720)></pre>
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.</integer>
	• 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(112582720)>] [max-threshold <integer(1-12582720)>] [maxpkt-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 gueue 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.

	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. show qos global info Privileged EXEC Mode		
Syntax			
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

Syntax	Privileged EXEC Mode.		
Parameter Description			
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 RegenPriority	: 1 : 5	
	InnerRegenPriority	: 7	
Note:			
11010.	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

Syntax	show class-map [<class-map-id(1-65535)>]</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.</class-map-id(1-65535)>		
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.		

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)></group-name(31)>		
Parameter Description	 <group-name(31)> - Displays the details of the unique identification of the group to which an input CLASS belongs.</group-name(31)> Privileged EXEC Mode. 		
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

_	Privileged EXEC Mode.		
Syntax			
Parameter Description			
_	Workgroup, Enterprise, Metro_E, and Metro		
Example	SEFOS# show meter		
	QoS Meter Entries		
	MeterId	: 1	
	Туре	: 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 avacuted without the action	al 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

Syntax	show policy-map [<meter-id(1-65535)>]</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.</meter-id(1-65535)> Privileged EXEC Mode. Workgroup, Enterprise, Metro_E, and Metro 		
Mode			
Package			
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)	lated Command(s) • set policy – Sets CLASS for policy.		
Related Command(s)		-	

48.28 show queue-template

Command Objective	This command displays the Q Template and Random Detect configurations.		
Syntax	<pre>show queue-template [<queue-template-id(1-65535)>] • <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.</queue-template-id(1-65535)></queue-template-id(1-65535)></pre>		
Parameter Description			
Mode	Privileged EXEC Mode.		
Package	Workgroup, Enterprise, Metro_E, and Metro		
Example	SEFOS# show queue-tem	plate	
	Queue Template Entrie	s	
		-	
	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 ExpWeight 0, Gain 1,	40, MaxPktSize 1000, MaxDropProb 10, 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	

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 templ	ate configu	urations.	
Syntax	show shape-template [<shape-te< th=""><th>mplate-</th><th>Id(1-6553</th><th>5)>]</th></shape-te<>	mplate-	Id(1-6553	5)>]
Parameter Description	• <shape-template-id< th=""><th>(1-65535)</th><th>> - Shape</th><th>Template T</th><th>able index.</th></shape-template-id<>	(1-65535)	> - Shape	Template T	able index.
Mode	Privileged EXEC Mode.				
Package	Workgroup, Enterprise, Metro_E, and Metro				
Example	SEFOS# show shape-tem QoS Shape Template En	-			
	ShapeTemplate Id	CIR	CBS	EIR	EBS
	1	1	1	1	1
Note:	If executed without the option available shape template info		er, this con	nmand displ	ays all the
Related Command(s)	• shape-template — Cre	eates a shap	e template	э.	

48.30 show scheduler

Command Objective	This command displays the configured scheduler.				
Syntax	show scheduler [interface <iftype> <ifnum>]</ifnum></iftype>				
Parameter Description	• <iftype> - Sets the type of interface for the outbound queue. The interface can be:</iftype>				
	 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.</ifnum>				
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>]</ifnum></iftype>				
Parameter Description	• <iftype> - Sets the type of interface for the outbound queue. The interface can be:</iftype>				
	 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.</ifnum>				
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 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 comm	and displa	ys the configured q	lueue map.	
Syntax	show que	ue-map [interface <ift< th=""><th>cype> <ifnum>]</ifnum></th><th></th></ift<>	cype> <ifnum>]</ifnum>	
Parameter Description		rpe> - Sets	the type of interfac	ce for the outbound qu	ueue. The
	is		of LAN standard are	erred to as 100BASE- chitecture that suppor	
			et – A version of L r up to 1 Gbit/sec.	AN standard architect	ture that supports
			thernet – A version 10 Gbits/sec.	on of Ethernet that su	pports data
	• ir	nternal-	lan – Internal LAN	created on a bridge p	oer IEEE 802.1ap.
	combir interfac	nation of sloce type oth	ot number and port	ecific interface. This van number separated by and port-channel. Or an.	/ a slash, for
Mode	Privileged	EXEC Mod			
Mode Package				 etro	
		, Enterpris	e, Metro_E, and Me		
Package	Workgroup	o, Enterpris	e, Metro_E, and Me		
Package	Workgroup	o, Enterpris	e, Metro_E, and Me		
Package	Workgroup SEFOS# s QoS Queu	o, Enterpris	e, Metro_E, and Me		
Package	Workgroup SEFOS# s QoS QueuIfIndex	o, Enterpris	e, Metro_E, and Me	etro	
Package	Workgroup SEFOS# s QoS QueuIfIndex	o, Enterpris	e, Metro_E, and Me	etro	
Package	Workgroup SEFOS# s QoS Queu IfIndex Queue	chow queu e Map Er CLASS	e, Metro_E, and Measure map	Priority Value	Mapped
Package	Workgroup SEFOS# s QoS Queu IfIndex Queue Ex0/1	chow queu e Map En CLASS	e, Metro_E, and Me ne-map ntries PriorityType VlanPri	Priority Value	Mapped
Package	Workgroup SEFOS# s QoS Queu IfIndex Queue Ex0/1 Ex0/1	chow queu e Map Er CLASS	e, Metro_E, and Metro_E and Me	Priority Value 0 1	Mapped 1 2
Package	Workgroup SEFOS# s QoS Queu IfIndex Queue Ex0/1 Ex0/1 Ex0/1	chow queu e Map En CLASS	e, Metro_E, and Meaneri e-map ntries PriorityType VlanPri VlanPri VlanPri	Priority Value 0 1 2	Mapped 1 2 3
Package	Workgroup SEFOS# s QoS Queu IfIndex Queue Ex0/1 Ex0/1 Ex0/1 Ex0/1	chow queu e Map En CLASS none none none none	e, Metro_E, and Merce-map ntries PriorityType VlanPri VlanPri VlanPri VlanPri VlanPri	Priority Value 0 1 2 3	Mapped 1 2 3 4
Package	Workgroup SEFOS# s QoS Queu IfIndex Queue Ex0/1 Ex0/1 Ex0/1 Ex0/1 Ex0/1	none none none none none	e, Metro_E, and Me	Priority Value 0 1 2 3 4	Mapped 1 2 3 4 5

	Ex0/1	none	IPToS	1	1
	Ex0/1	none	IPDSCP	1	1
	Ex0/1	1	none	0	1
Note:		rithout the optio	•	mmand displays all th	е
Related Command(s)	• queue-m	nap – Creates a	a map for a queue with	n 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>]</ifnum></iftype>
Parameter Description	• <iftype> - Sets the type of interface for the outbound queue. The interface can be:</iftype>
	 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.</ifnum>
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.

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>]</ifnum></iftype>
Parameter Description	• <iftype> - Sets the type of interface for the outbound queue. The interface can be:</iftype>
	 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.</ifnum>
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

-	This command displays the configured default ingress user priority for a port.
Syntax	show qos def-user-priority [interface <iftype> <ifnum>]</ifnum></iftype>
Parameter Description	 <iftype> - Sets the type of interface for the outbound queue. The interface can be:</iftype>
	 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 support 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.</ifnum>
Mode	Privileged EXEC Mode.
Package	Workgroup, Enterprise, Metro_E, and Metro
Example	SEFOS# show qos def-user-priority
	Occ. Defendt Heer Drievity Branch
	QoS Default User Priority Entries
	IfIndex Default User Priority
	-
	IfIndex Default User Priority
	IfIndex Default User Priority Ex0/1 0
	IfIndex Default User Priority Ex0/1 0 Ex0/2 0
	IfIndex Default User Priority Ex0/1
	IfIndex Default User Priority Ex0/1 0 Ex0/2 0 Ex0/3 0 Ex0/4 0
	IfIndex Default User Priority Ex0/1
	IfIndex Default User Priority Ex0/1

	ut the optional parameter, this command displays the ingress user priority entries for all the interface.
Ex0/24	0
Ex0/23	0
Ex0/22	0
Ex0/21	0
Ex0/20	0
Ex0/19	0
Ex0/18	0
Ex0/17	0
Ex0/16	0
Ex0/15	0
Ex0/14	0
	0
	0
	0
	Ex0/15 Ex0/16 Ex0/17 Ex0/18 Ex0/19 Ex0/20 Ex0/21 Ex0/22 Ex0/23 Ex0/24 If executed witho

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)>]</meter-id(1-65535)>		
Parameter Description	<meter-id(1-65535)> - Index that enumerates the meter entries.</meter-id(1-65535)>		
Mode	Privileged EXEC Mode.		
Package	Workgroup, Enterprise, Metro_E, and Metro		
Example	SEFOS# show qos meter-	stats	
	QoS Meter (Policer) St	ats	
	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.		

48.37 show qos queue-stats

Command Objective	This command displays queue stati octets count, Management Algo Dro	stics for EnQ, DeQ, discarded packets and op, and Q occupancy.
Syntax	show qos queue-stats [inte	rface <iftype> <ifnum>]</ifnum></iftype>
Parameter Description	<iftype> - Sets the type of initerface can be:</iftype>	terface for the outbound queue. The
		y referred to as 100BASE-T standard. This rd architecture that supports data transfer
	 XL-ethernet – A versior data transfer up to 1 Gbit/s 	of LAN standard architecture that supports sec.
	 extreme-ethernet – A transfer up to 10 Gbits/sec 	version of Ethernet that supports data
	internal-lan – Internal	LAN created on a bridge per IEEE 802.1ap.
	unique value that represents the combination of slot number and	erface for the outbound queue. This is a e specific interface. This value is a I port number separated by a slash, for al-lan and port-channel. Only i-lan id is rnal-lan.
Mode	Privileged EXEC Mode.	
Package	Workgroup, Enterprise, Metro_E, a	nd Metro
	SEFOS# show qos queue-stat	s
Example		-
Example	QoS Queue Stats	
Example		
Example		: Ex0/1
Example	QoS Queue Stats	
Example	QoS Queue Stats Interface Index	: Ex0/1
Example	QoS Queue Stats Interface Index Queue Index	: Ex0/1 : 2
Example	QoS Queue Stats Interface Index Queue Index EnQ Packets	: Ex0/1 : 2 : 00
Example	QoS Queue Stats Interface Index Queue Index EnQ Packets EnQ Octects	: Ex0/1 : 2 : 00 : 00
Example	QoS Queue Stats Interface Index Queue Index EnQ Packets EnQ Octects DeQ Packets	: Ex0/1 : 2 : 00 : 00 : 00
Example	QoS Queue Stats Interface Index Queue Index EnQ Packets EnQ Octects DeQ Packets DeQ Octects	: Ex0/1 : 2 : 00 : 00 : 00 : 00
Example	QoS Queue Stats Interface Index Queue Index EnQ Packets EnQ Octects DeQ Packets DeQ Octects Discard Packets	: Ex0/1 : 2 : 00 : 00 : 00 : 00 : 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	<pre>debug qos {initshut mgmt ctrl dump os failall buffer}</pre>
	<pre>no debug qos {initshut mgmt ctrl dump os failall buffer}</pre>
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	<pre>cpu rate limit queue <integer(1-65535)> minrate <integer(65535)> maxrate <integer(1-65535)></integer(1-65535)></integer(65535)></integer(1-65535)></pre>			
Parameter Description	• <integer(1-65535)> - Queue identifier that uniquely identifies the queue in the system or port. This value ranges from 1 to 65535.</integer(1-65535)>			
	 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.</integer(1-65535)> 			
	 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.</integer(1-65535)> 			
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:</iftype>				
	 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				
	unique v combina interface	alue that repre tion of slot nur type other tha	be of interface for the outbound queue. This is a seents the specific interface. This value is a subset and port number separated by a slash, for an internal-lan and port-channel. Only i-lan id is 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		

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	no mls qos Global Configuration Mode
Mode Package	

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	<pre>mls qos aggregate-policer <meter-id (1-65535)=""> <bits (1-65535)="" per="" second=""> <normal (1-65535)="" burst="" bytes=""> exceed- action {drop set-ip-dscp-transmit}</normal></bits></meter-id></pre>		
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.</meter-id(1-65535)> 		
	 <bits (1-65535)="" per="" second=""> - Configures the average traffic rate in bits per second. This value ranges from 1 to 65535.</bits> 		
	 <normal (1-65535)="" burst="" bytes=""> - Configures the normal burst size in bytes. This value ranges from 1 to 65535.</normal> 		
	• 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		