S-Series® CLI Reference

Firmware Version 8.31

Published September 2014

9034733-03

Copyright © 2014 Extreme Networks, Inc. All Rights Reserved.

Legal Notices

Extreme Networks, Inc., on behalf of or through its wholly-owned subsidiary, Enterasys Networks, Inc., reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information about Extreme Networks trademarks, go to:
www.extremenetworks.com/company/legal/trademarks/

Support

For product support, including documentation, visit:
http://support.extremenetworks.com/

Contact

Extreme Networks, Inc.
145 Rio Robles
San Jose, CA 19534
Tel: +1 408-579-2800

Toll-free: +1 888-257-3000

Enterasys Networks, Inc. Firmware License Agreement

BEFORE OPENING OR UTILIZING THE ENCLOSED PRODUCT, CAREFULLY READ THIS LICENSE AGREEMENT.

This document is an agreement ("Agreement") between the end user ("You") and Enterasys Networks, Inc., a wholly-owned subsidiary of Extreme Networks, Inc., on behalf of itself and its Affiliates (as hereinafter defined) ("Enterasys"), that sets forth Your rights and obligations with respect to the Enterasys software program/firmware (including any accompanying documentation, hardware or media) (collectively, the "Program") in the package and prevails over any additional, conflicting or inconsistent terms and conditions appearing on any purchase order or other document submitted by You. "Affiliate" means any person, partnership, corporation, limited liability company, other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified.

This Agreement constitutes the entire understanding between the parties, with respect to the subject matter of this Agreement. The Program may be contained in firmware, chips or other media.

BY INSTALLING OR OTHERWISE USING THE PROGRAM, YOU REPRESENT THAT YOU ARE AUTHORIZED TO ACCEPT THESE TERMS ON BEHALF OF THE END USER (IF THE END USER IS AN ENTITY ON WHOSE BEHALF YOU ARE AUTHORIZED TO ACT, “YOU” AND “YOUR” SHALL BE DEEMED TO REFER TO SUCH ENTITY) AND THAT YOU AGREE THAT YOU ARE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES, AMONG OTHER PROVISIONS, THE LICENSE, THE DISCLAIMER OF WARRANTY AND THE LIMITATION OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT OR ARE NOT AUTHORIZED TO ENTER INTO THIS AGREEMENT, ENTERASYS IS UNWILLING TO LICENSE THE PROGRAM TO YOU AND YOU AGREE TO RETURN THE UNOPENED PRODUCT TO ENTERASYS OR YOUR DEALER, IF ANY, WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A FULL REFUND.

IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT EXTREME NETWORKS, LEGAL DEPARTMENT AT (408) 579-2800.

You and Enterasys agree as follows:

1. LICENSE. You are granted a revocable, non-exclusive and non-transferable right to use only one (1) copy of the Program provided in this package subject to the terms and conditions of this Agreement.
2. RESTRICTIONS. Except as otherwise authorized in writing by Enterasys, You may not, nor may You permit any third party to:
   (a) Reverse engineer, decompile, disassemble or modify the Program, in whole or in part, including for reasons of error correction or interoperability, except to the extent expressly permitted by applicable law and to the extent the parties shall not be permitted by that applicable law, such rights are expressly excluded. Information necessary to achieve interoperability or correct errors is available from Enterasys upon request and payment of Enterasys’ applicable fee.
   (b) Incorporate the Program in whole or in part, in any other product or create derivative works based on the Program, in whole or in part.
   (c) Publish, disclose, copy reproduce or transmit the Program, in whole or in part.
   (d) Assign, sell, license, sublicense, rent, lease, encumber by way of security interest, pledge or otherwise transfer the Program, in whole or in part.
   (e) Remove any copyright, trademark, proprietary rights, disclaimer or warning notice included on or embedded in any part of the Program.

3. APPLICABLE LAW. This Agreement shall be interpreted and governed under the laws and in the state and federal courts of the State of California without regard to its conflicts of laws provisions. You accept the personal jurisdiction and venue of the Superior Court of California in Santa Clara County or the United States District Court for the Northern District of California in San Jose, California. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.
4. EXPORT RESTRICTIONS. You acknowledge and agree that the Program and its accompanying materials/documentation are subject to the export control laws and regulations of the United States, including but not limited to the Export Administration Regulations (EAR), the International Traffic in Arms Regulations (ITAR), and the sanction regimes of the U.S. Department of Treasury, Office of Foreign Assets Control's Foreign Assets Control Regulations (FACR). You agree that You will comply with these laws and regulations.

   You agree that You will not, without prior U.S. Government authorization, export, reexport, or transfer the Program, either directly or indirectly, to any country subject to a U.S. trade embargo or sanction (e.g. Cuba, N. Korea, Iran, Syria, Sudan) or to any resident or national of said countries, or to any person, organization, or entity on any of the restricted parties lists maintained by the U.S. Departments of State, Treasury, or Commerce. In addition, You agree that You will not export, reexport or transfer the Program to any end-user engaged in activities, or for any end-use, directly or indirectly related to the design, development, production, use, or stockpiling of weapons of mass destruction, e.g. nuclear, chemical, or biological weapons, and the missile technology to deliver them.
5. UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The enclosed Program (i) was developed solely at private expense; (ii) contains "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Enterasys, its Affiliates and/or its suppliers. For Department of Defense units, the Program is considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth herein.
6. DISCLAIMER OF WARRANTY. EXCEPT FOR THOSE WARRANTIES EXPRESSLY PROVIDED TO YOU IN WRITING BY ENTERASYS, ENTERASYS DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT WITH RESPECT TO THE PROGRAM. IF THE IMPLIED WARRANTIES MAY NOT BE DISCLAIMED BY APPLICABLE LAW, THEN ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO THIRTY (30) DAYS AFTER DELIVERY OF THE PROGRAM TO YOU.
7. LIMITATION OF LIABILITY. IN NO EVENT SHALL ENTERASYS OR ITS AFFILIATES AND SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM, EVEN IF ENTERASYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS FOREGOING LIMITATION SHALL APPLY REGARDLESS OF THE CAUSE OF ACTION UNDER WHICH DAMAGES ARE SOUGHT.

NOTWITHSTANDING THE FOREGOING, THE CUMULATIVE LIABILITY OF ENTERASYS TO YOU FOR ALL CLAIMS RELATING TO THE PROGRAM, IN CONTRACT,

TORT OR OTHERWISE, SHALL NOT EXCEED THE TOTAL AMOUNT OF FEES PAID TO ENTERASYS BY YOU FOR THE RIGHTS GRANTED HEREIN.

8. AUDIT RIGHTS. You hereby acknowledge that the intellectual property rights associated with the Program are of critical value to Enterasys and its Affiliates, and, accordingly, You hereby agree to maintain complete books, records and accounts showing: (i) license fees due and paid, and (ii) the use, copying and deployment of the Program. You also grant to Enterasys and its authorized representatives, upon reasonable notice, the right to audit and examine during Your normal business hours, Your books, records, accounts and hardware devices upon which the Program may be deployed to verify compliance with this Agreement, including the verification of the license fees due and paid to Enterasys and the use, copying and deployment of the Program. Enterasys' right of examination shall be exercised reasonably, in good faith and in a manner calculated to not unreasonably interfere with Your business. In the event such an audit discovers any non-compliance with this Agreement, including copies of the Program made, used or deployed in breach of this Agreement, You shall promptly cease such unauthorized conduct, pay to Enterasys the appropriate license fees and be subject to any other available claim from Enterasys pursuant to applicable law. Enterasys reserves the right, to be exercised in its sole discretion and without prior notice, to terminate this Agreement, including the license, effective immediately, for failure to comply with this Agreement. Upon any such termination, You shall immediately cease all use of the Program and shall return to Enterasys the Program and all copies of the Program.
9. OWNERSHIP. This is a license agreement and not an agreement for sale. You acknowledge and agree that the Program constitutes trade secrets and/or copyrighted material of Enterasys and/or its suppliers. You agree to implement reasonable security measures to protect such trade secrets and copyrighted material. All right, title and interest in and to the Program shall remain with Enterasys and/or its Affiliates and suppliers. All rights not specifically granted to You shall be reserved to Enterasys.
10. TRADEMARKS. ENTERASYS, ENTERASYS NETWORKS, ENTERASYS SECURE NETWORKS, NETSIGHT, ENTERASYS NETSIGHT, and any logos associated therewith, are trademarks or registered trademarks of Enterasys Networks, Inc., in the United States and/or other countries. Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. For more information on Enterasys and Extreme trademarks, see: www.extremenetworks.com/about-extreme/trademarks.aspx.

    All other product names mentioned in Program may be trademarks or registered trademarks of their respective companies.
11. ENFORCEMENT. You acknowledge and agree that any breach of this Agreement by You may cause Enterasys irreparable damage for which recovery of money damages would be inadequate, and that Enterasys may be entitled to seek timely injunctive relief to protect Enterasys' rights under this Agreement in addition to any and all remedies available at law.
12. ASSIGNMENT. You may not assign, transfer or sublicense this Agreement or any of Your rights or obligations under this Agreement, except that You may assign this Agreement to any person or entity that acquires substantially all of Your stock assets. Enterasys may assign this Agreement in its sole discretion to anyone or any entity without Your consent and without notice, including assigning this Agreement to its parent company, Extreme Networks, Inc. This Agreement shall be binding upon and inure to the benefit of the parties, their legal representatives, permitted transferees, successors and assigns as permitted by this Agreement. Any attempted assignment, transfer or sublicense in violation of the terms of this Agreement shall be void and a breach of this Agreement.

13. WAIVER. A waiver by Enterasys of a breach of any of the terms and conditions of this Agreement must be in writing and will not be construed as a waiver of any subsequent breach of such term or condition. Enterasys' failure to enforce a term upon Your breach of such term shall not be construed as a waiver of Your breach or prevent enforcement on any other occasion.
14. SEVERABILITY. In the event any provision of this Agreement is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of any of the remaining provisions shall not in any way be affected or impaired thereby, and that provision shall be reformed, construed and enforced to the maximum extent permissible. Any such invalidity, illegality, or unenforceability in any jurisdiction shall not invalidate or render illegal or unenforceable such provision in any other jurisdiction.
15. TERMINATION. Enterasys may terminate this Agreement immediately upon Your breach of any of the terms and conditions of this Agreement. Upon any such termination, You shall immediately cease all use of the Program and shall return to Enterasys the Program and all copies of the Program.

Contents

About This Guide

Using This Guide liii
Related Documents liii
Conventions Used in This Guide liv
CLI “Defaults” Descriptions liv
CLI Command Modes liv
Commonly Used Acronyms lv
Getting Help lv

Chapter 1: CLI Properties Commands

set prompt 1-1
set cli completion 1-2
loop 1-2
show banner 1-3
set banner 1-4
clear banner 1-5
history 1-5
show history 1-6
set history 1-6
show version 1-7
show width 1-8
show length 1-8
set width 1-9
set length 1-9
show logout 1-10
set logout 1-10
cls (clear screen) 1-11
configure 1-11
exit | quit 1-12

Chapter 2: Line Editor Commands

show line-editor 2-3
set line-editor 2-3

Chapter 3: User Management Commands

Setting User Accounts and Passwords 3-1
Commands 3-1
show system login 3-2
set system login 3-5
clear system login 3-6
show security boot-access 3-7
set security boot-access 3-7
clear security boot-access 3-8
show security fips mode 3-8
set security fips mode 3-9
clear security fips mode 3-9
show security profile 3-10
set security profile 3-10
clear security profile 3-11
set password 3-12

show system password 3-13
set system password 3-15
clear system password 3-18
show system lockout 3-19
set system lockout 3-20
clear system lockout 3-22
Setting the Authentication Login Method 3-22
show authentication login 3-22
set authentication login 3-23
clear authentication login 3-24
Setting WebView 3-24
show webview 3-24
set webview 3-25
set webview port 3-25

Chapter 4: Internet Protocol Security (IPsec) Commands

IPsec Commands 4-1
crypto ipsec enable 4-1
crypto ipsec default 4-2
crypto ipsec trap-enable 4-3
ike map 4-3
IKE Proposal Commands 4-4
crypto ike-proposal 4-4
dh_group 4-5
encryption 4-6
hash 4-7
integrity 4-7
IKE Policy Commands 4-8
crypto ike-policy 4-8
authentication psk 4-9
initial-contact 4-10
lifetime time 4-10
passive 4-11
peer 4-12
proposal 4-12
version 4-13
IKE Map Commands 4-14
crypto ike-map 4-14
dst 4-15
dst-port 4-16
encapsulation 4-16
lifetime 4-17
policy 4-18
proposal 4-19
protocol udp 4-19
request 4-20
src 4-21
src-port 4-21
Show Commands 4-22
show ike stats 4-23
show ike proposal 4-24
show ike policy 4-25
show ike map 4-26
show ike sa 4-27
show ipsec counters 4-27

show ipsec map 4-29
show ipsec sa 4-30
show ipsec flow 4-31
show ipsec instance 4-33
show ipsec interface 4-34

Chapter 5: Public-Key Infrastructure (PKI) Commands

show pki certificate 5-1
show config pki 5-4
set pki certificate 5-5
clear pki certificate 5-6
show pki oscp 5-7
set pki ocsp 5-8
set pki ocsp signature-ca-list 5-9
clear pki ocsp signature-ca-list 5-10
set pki ocsp nonce 5-10
set pki ocsp responder 5-11
clear pki ocsp responder 5-12
show pki authorization 5-12
set pki authorization username 5-13
set pki authorization username attribute 5-14
clear pki authorization 5-15

Chapter 6: Management Authentication Notification MIB Commands

show mgmt-auth-notify 6-1
set mgmt-auth-notify 6-2
clear mgmt-auth-notify 6-3

Chapter 7: System Properties Commands

show chassis compatibility-mode 7-2
set chassis compatibility-mode 7-3
clear chassis compatibility-mode 7-5
set ip interface 7-5
clear ip interface 7-6
set ip address 7-6
clear ip address 7-7
show system 7-8
show system hardware 7-9
show system utilization 7-11
set system utilization threshold 7-13
clear system utilization 7-13
show time 7-14
set time 7-14
show summertime 7-15
set summertime 7-15
set summertime date 7-16
set summertime recurring 7-17
clear summertime 7-18
set system name 7-18
set system location 7-19
set system contact 7-19
show mtu 7-20
set mtu 7-20
clear mtu 7-21
show reset 7-21

reset 7-22
reset nemcpu 7-22
reset at 7-23
reset in 7-24
clear config 7-24
show support 7-25
show physical alias 7-26
set physical alias 7-27
clear physical alias 7-28
show physical assetid 7-29
set physical assetid 7-30
clear physical assetid 7-30

Chapter 8: MAC Address Commands

show port mac 8-1
show mac 8-2
show mac agetime 8-4
set mac 8-5
clear mac 8-6
show newaddrtrap 8-7
set newaddrtrap 8-7
show movedaddrtrap 8-8
set movedaddrtrap 8-9

Chapter 9: Telnet Commands

show telnet 9-1
set telnet 9-2
telnet 9-2

Chapter 10: Secure Shell (SSH) Commands

show ssh state 10-1
set ssh 10-3
set ssh ciphers 10-3
clear ssh ciphers 10-4
set ssh client alive-interval 10-5
set ssh client alive-count 10-5
clear ssh client 10-6
set ssh hostkey 10-7
set ssh macs 10-7
clear ssh macs 10-8
set ssh reinitialize 10-9
set ssh server allowed-auth 10-9
show ssh authkey 10-10
set ssh server authkey 10-11
clear ssh server authkey 10-12
set ssh server pki trusted-ca-list 10-12
set ssh server pki authorized-cert-list 10-13
ssh 10-14

Chapter 11: Domain Name Server (DNS) Commands

set ip dns 11-1
set ip dns domain 11-2
clear ip dns domain 11-3
set ip dns server 11-3

clear ip dns server 11-4
set ip dns zone 11-4
clear ip dns zone 11-5
set ip dns port-number 11-6
clear ip dns port-number 11-6
set ip dns timeout 11-7
clear ip dns timeout 11-7
set ip dns query-retries 11-8
clear ip dns query-retries 11-9
clear ip dns all 11-9
clear ip dns status 11-10
show ip dns 11-10

Chapter 12: Node Alias Commands

show nodealias 12-1
show nodealias mac 12-3
show nodealias protocol 12-4
show nodealias config 12-5
set nodealias 12-6
set nodealias maxentries 12-8
clear nodealias 12-8
clear nodealias config 12-9

Chapter 13: SNTP Commands

show sntp 13-2
set sntp authentication mode 13-3
set sntp authentication key 13-4
set sntp authentication trust 13-5
clear sntp authentication 13-6
set sntp client 13-6
clear sntp client 13-7
set sntp server 13-7
clear sntp server 13-8
set sntp broadcastdelay 13-8
clear sntp broadcast delay 13-9
set sntp poll-interval 13-9
clear sntp poll-interval 13-10
set sntp poll-retry 13-10
clear sntp poll-retry 13-11
set sntp poll-timeout 13-11
clear sntp poll-timeout 13-12
show timezone 13-12
set timezone 13-13
clear timezone 13-13

Chapter 14: DHCP Commands

ip dhcp server 14-2
ipv6 dhcp server 14-3
ipv6 dhcp relay source-interface 14-3
ipv6 dhcp relay destination 14-4
show ip local pool 14-5
ip local pool 14-6
exclude 14-6
ip dhcp ping packets 14-7
ip dhcp ping timeout 14-8

ip dhcp pool 14-8
ipv6 dhcp pool 14-9
ip dhcp relay information option vpn 14-9
ip dhcp send-all-options 14-10
domain-name 14-11
dns-server 14-12
nis-domain-name 14-13
nis-server 14-13
nisp-domain-name 14-14
nisp-server 14-15
sip-domain-name 14-15
sip-server 14-16
sntp-server 14-17
unicast-server 14-17
information-refresh 14-18
netbios-name-server 14-19
netbios-node-type 14-20
default-router 14-20
bootfile 14-21
next-server 14-22
option 14-22
lease 14-23
host 14-24
client-class 14-24
client-identifier 14-25
client-name 14-26
hardware-address 14-26
show ip dhcp binding 14-27
clear ip dhcp binding 14-28
show ip dhcp server statistics 14-28
clear ip dhcp server statistics 14-29

Chapter 15: License Commands

set license 15-1
show license 15-2
clear license 15-3

Chapter 16: Power over Ethernet (PoE) Commands

show inlinepower 16-2
set inlinepower mode 16-3
clear inlinepower mode 16-3
set inlinepower available 16-4
clear inlinepower available 16-4
set inlinepower powertrap 16-5
clear inlinepower powertrap 16-5
set inlinepower assigned 16-6
clear inlinepower assigned 16-6
set inlinepower threshold 16-7
clear inlinepower threshold 16-7
set inlinepower management 16-8
clear inlinepower management 16-8
set inlinepower psetrap 16-9
clear inlinepower psetrap 16-10
show port inlinepower 16-10
set port inlinepower 16-11

clear port inlinepower 16-12

Chapter 17: Configuration and Image File Management Commands

General Configuration and Image File Management Commands 17-1
dir 17-2
show boot system 17-5
set boot system 17-6
show boot high-availability 17-8
set boot high-availability group 17-11
clear boot high-availability group 17-12
set boot high-availability delay 17-13
clear boot high-availability delay 17-13
set boot high-availability default-mode 17-14
clear boot high-availability default-mode 17-15
set boot high-availability force-complete 17-15
show file 17-16
show config 17-18
configure 17-20
copy 17-21
delete 17-22
script 17-23
Restore Point Commands 17-24
set config restore-point 17-24
show config restore-point 17-25
clear config restore-point 17-26
configure restore-point 17-26

Chapter 18: Virtual Switch Bonding Commands

show bonding 18-1
set bonding chassis 18-4
clear bonding chassis 18-5
set bonding enable 18-5
set bonding disable 18-6
set bonding lfr 18-7
clear bonding lfr 18-8
set bonding port enable 18-8
set bonding port disable 18-9
set bonding mac 18-10
clear bonding mac 18-11
set bonding mode 18-11
clear bonding mode 18-12
show lacp outportLocalPreference 18-13
set lacp outportLocalPreference 18-13
clear lacp outportLocalPreference 18-14
set license vsb 18-15

Chapter 19: Network Diagnostics

ping 19-1
traceroute 19-3
nslookup 19-5

Chapter 20: Discovery Protocol Commands

Displaying Neighbors 20-1
show neighbors 20-1
Neighbor Warning Detection 20-4
set neighbors warning-detection 20-4
clear neighbors warning-detection 20-5
show neighbors warnings 20-6
show neighbors warning-detection 20-7
Extreme Networks Discovery Protocol 20-8
show cdp 20-8
set cdp state 20-10
set cdp auth 20-10
set cdp interval 20-11
set cdp hold-time 20-11
clear cdp 20-12
Cisco Discovery Protocol 20-13
show ciscodp 20-13
show ciscodp port info 20-14
set ciscodp status 20-15
set ciscodp timer 20-16
set ciscodp holdtime 20-16
set ciscodp port 20-17
clear ciscodp 20-18
Link Layer Discovery Protocol and LLDP-MED 20-19
show lldp 20-20
show lldp port status 20-21
show lldp port trap 20-21
show lldp port tx-tlv 20-22
show lldp port location-info 20-23
show lldp port local-info 20-24
show lldp port remote-info 20-29
show lldp port network-policy 20-32
set lldp tx-interval 20-33
set lldp tx-fast-count 20-33
set lldp tx-fast-interval 20-34
set lldp hold-multiplier 20-35
set lldp trap-interval 20-35
set lldp med-fast-repeat 20-36
set lldp port status 20-37
set lldp port trap 20-37
set lldp port med-trap 20-38
set lldp port location-info 20-38
set lldp port tx-tlv 20-39
set lldp port network-policy 20-41
clear lldp 20-43
clear lldp port status 20-43
clear lldp port trap 20-44
clear lldp port med-trap 20-44
clear lldp port location-info 20-45
clear lldp port network-policy 20-45
clear lldp port tx-tlv 20-46

Chapter 21: Data Center Bridging Commands

Application Priority 21-1
show dcb appPri 21-1
set dcb appPri 21-2
clear dcb appPri 21-3
Congestion Notification 21-4
show dcb cn global 21-4
set dcb cn global 21-5
show dcb cn priority 21-6
set dcb cn priority 21-8
set dcb cn priority status 21-9
set dcb cn priority choice 21-10
set dcb cn priority alt-priority 21-11
set dcb cn priority defense 21-12
set dcb cn priority lldp 21-14
clear dcb cn priority 21-15
clear dcb cn port-priority 21-16
show dcb cn port-priority 21-16
set dcb cn port-priority choice 21-19
set dcb cn port-priority alt-pri 21-20
set dcb cn port-priority defense 21-21
set dcb cn port-priority lldp 21-22
show dcb cn congestion-point 21-23
set dcb cn congestion-point 21-25
clear dcb cn congestion-point 21-27
show dcb cn cp-mapping 21-27
show dcb cn q-profile 21-29
set dcb cn q-profile 21-30
clear dcb cn q-profile 21-31
show dcb cn errored-ports 21-32

Chapter 22: Tracked Object Manager Commands

State Probe Commands 22-1
probe 22-2
acv close 22-3
acv reply 22-4
acv request 22-5
acv search-depth 22-5
description 22-6
dns-query type 22-7
dns-verify match 22-8
faildetect 22-8
inservice 22-9
l5-type 22-10
open 22-11
passdetect 22-11
receive 22-12
show probe 22-13
show probe session 22-16
show probe default 22-17
Timing Probe Commands 22-18
probe icmp timing 22-18
probe udp timing 22-19
description 22-19
dns-query type 22-20

inservice 22-21
interval 22-22
l5-type 22-22
packet-options 22-23
receive 22-24
Tracked Object Commands 22-24
track 22-25
delay 22-26
description 22-26
inservice 22-27
port 22-28
threshold count 22-28
show track 22-29

Chapter 23: Bidirectional Forwarding Detection Commands

show probe 23-1
probe bfd 23-1
bfd 23-2
bfd probe 23-3
control 23-3
demand-mode 23-4
description 23-5
echo-mode 23-6
echo 23-6
inservice 23-7
slow-timer 23-8

Chapter 24: Link-State Application Commands

set link-state track 24-1
clear link-state track 24-2
show link-state 24-3

Chapter 25: IP SLA Commands

sla entry 25-1
collections 25-2
destination 25-3
distribution 25-4
history 25-4
monitor 25-6
sla schedule 25-6
entry 25-7
stop-all 25-8
show sla 25-9
show sla entry detail 25-10
show sla entry distribution 25-11
show sla entry history 25-12
show sla entry summary 25-13
show sla scheduler 25-15
show limits application sla-entry-data 25-15

Chapter 26: Port Configuration Commands

show console 26-2
set console 26-3
clear console 26-5
show forcelinkdown 26-6
set forcelinkdown 26-6
clear forcelinkdown 26-7
show port 26-7
set port 26-8
show port advertise 26-8
set port advertise 26-10
clear port advertise 26-10
show port alias 26-11
set port alias 26-12
show port counters 26-13
show port duplex 26-15
set port duplex 26-15
show port energy-eff-eth 26-16
set port energy-efficient-eth 26-17
show port flowcontrol 26-18
set port flowcontrol 26-19
show port ingress-filter 26-19
set port ingress-filter 26-20
show port jumbo 26-21
set port jumbo 26-22
clear port jumbo 26-23
set port jumbo mtu 26-23
clear port jumbo mtu 26-24
show port mdix 26-25
set port mdix 26-25
clear port mdix 26-26
show port negotiation 26-26
set port negotiation 26-27
show port oam 26-27
set port oam status 26-31
set port oam mode 26-32
set port oam loopback-rx 26-32
set port oam remote-loopback 26-33
set port oam notify-retry 26-34
clear port oam 26-35
set port oam link-monitor 26-36
clear port oam link-monitor 26-38
show oam uld-config 26-40
set port oam uld mode 26-41
set port oam uld action 26-43
set port oam uld fast-timer 26-43
clear port oam uld 26-44
show port operstatuscause 26-45
clear port operstatuscause 26-47
show port speed 26-47
set port speed 26-48
show port status 26-48
show port transceiver 26-50

Chapter 27: Link Trap and Link Flap Detection Commands

show port trap 27-1
set port trap 27-2
show linkflap 27-2
set linkflap globalstate 27-4
set linkflap portstate 27-5
set linkflap interval 27-6
set linkflap action 27-6
clear linkflap action 27-7
set linkflap threshold 27-7
set linkflap downtime 27-8
clear linkflap down 27-8
clear linkflap 27-9

Chapter 28: Port Priority Configuration

Configuring Port Priority 28-1
show port priority 28-1
set port priority 28-2
clear port priority 28-3
Configuring Priority to Transmit Queue Mapping 28-3
show port priority-queue 28-3
set port priority-queue 28-4
clear port priority-queue 28-5

Chapter 29: Broadcast Suppression Commands

show port broadcast 29-1
set port broadcast 29-2
clear port broadcast 29-3

Chapter 30: Port Mirroring Commands

Physical Port Mirroring 30-1
show port mirroring 30-1
set port mirroring 30-2
show port mirroring enhanced 30-3
set port mirroring enhanced 30-4
set port mirroring orl 30-5
clear port mirroring 30-6
clear port mirroring orl 30-6
Policy Mirror Destinations 30-7
set mirror create 30-8
set mirror enable 30-8
set mirror disable 30-9
set mirror mirrorN 30-9
set mirror ports 30-10
set mirror 30-10
clear mirror ports 30-11
clear mirror 30-11
show mirror 30-12

Chapter 31: LACP Commands

show lacp 31-2
set lacp 31-3
clear lacp state 31-4
set lacp asyspri 31-4

set lacp aadminkey 31-5
clear lacp 31-5
set lacp static 31-6
clear lacp static 31-7
show lacp singleportlag 31-7
set singleportlag 31-8
clear singleportlag 31-8
show port lacp 31-9
set port lacp 31-10
clear port lacp 31-12
show lacp flowRegeneration 31-13
set lacp flowRegeneration 31-13
clear lacp flowRegeneration 31-14
show lacp outportAlgorithm 31-14
set lacp outportAlgorithm 31-15
clear lacp outportAlgorithm 31-15

Chapter 32: SNMP User, Group, and Community Commands

Configuring SNMP Users, Groups, and Communities 32-1
show snmp user 32-2
set snmp user 32-3
clear snmp user 32-4
set snmp engineid 32-5
clear snmp engineid 32-5
show snmp group 32-6
set snmp group 32-7
clear snmp group 32-8
show snmp community 32-8
set snmp community 32-9
clear snmp community 32-10
Configuring SNMP Access Rights 32-10
show snmp access 32-11
set snmp access 32-12
clear snmp access 32-14

Chapter 33: SNMP MIB View Commands

show snmp view 33-1
show snmp context 33-2
set snmp view 33-3
clear snmp view 33-4

Chapter 34: SNMP Parameter and Review Commands

Configuring SNMP Target Parameters 34-1
show snmp targetparams 34-1
set snmp targetparams 34-3
clear snmp targetparams 34-4
Configuring SNMP Target Addresses 34-4
show snmp targetaddr 34-5
set snmp targetaddr 34-6
clear snmp targetaddr 34-7
Configuring SNMP Notification Parameters 34-7
About SNMP Notify Filters 34-8
show snmp notify 34-8
set snmp notify 34-9
clear snmp notify 34-10

show snmp notifyfilter 34-11
set snmp notifyfilter 34-11
clear snmp notifyfilter 34-12
show snmp notifyprofile 34-13
set snmp notifyprofile 34-13
clear snmp notifyprofile 34-14
Configuring SNMP MIB Walk Behavior 34-14
set snmp timefilter break 34-15
clear snmp timefilter break 34-15
show snmp timefilter 34-16
Reviewing SNMP Statistics 34-16
show snmp engineid 34-16
show snmp counters 34-17

Chapter 35: Spanning Tree Bridge Commands

show spantree stats 35-3
show spantree version 35-6
set spantree version 35-7
clear spantree version 35-7
show spantree stpmode 35-8
set spantree stpmode 35-8
clear spantree stpmode 35-9
show spantree maxconfigurablestps 35-9
set spantree maxconfigurablestps 35-10
clear spantree maxconfigurablestps 35-10
show spantree mstilist 35-11
set spantree msti 35-11
clear spantree msti 35-12
show spantree mstmap 35-12
set spantree mstmap 35-13
clear spantree mstmap 35-13
show spantree vlanlist 35-14
show spantree mstcfgid 35-14
set spantree mstcfgid 35-15
clear spantree mstcfgid 35-16
show spantree bridgeprioritymode 35-16
set spantree bridgeprioritymode 35-17
clear spantree bridgeprioritymode 35-17
show spantree priority 35-18
set spantree priority 35-18
clear spantree priority 35-19
show spantree bridgehellomode 35-20
set spantree bridgehellomode 35-20
clear spantree bridgehellomode 35-21
show spantree hello 35-21
set spantree hello 35-22
clear spantree hello 35-22
show spantree maxage 35-23
set spantree maxage 35-23
clear spantree maxage 35-24
show spantree fwddelay 35-24
set spantree fwddelay 35-25
clear spantree fwddelay 35-25
show spantree autoedge 35-26
set spantree autoedge 35-26

clear spantree autoedge 35-27
show spantree legacypathcost 35-27
set spantree legacypathcost 35-28
clear spantree legacypathcost 35-28
show spantree tctrapsuppress 35-29
set spantree tctrapsuppress 35-29
clear spantree tctrapsuppress 35-30
show spantree txholdcount 35-30
set spantree txholdcount 35-31
clear spantree txholdcount 35-31
show spantree maxhops 35-32
set spantree maxhops 35-32
clear spantree maxhops 35-33
show spantree spanguard 35-33
set spantree spanguard 35-34
clear spantree spanguard 35-34
show spantree spanguardtimeout 35-35
set spantree spanguardtimeout 35-35
clear spantree spanguardtimeout 35-36
show spantree spanguardlock 35-36
clear / set spantree spanguardlock 35-37
show spantree spanguardtrapenable 35-37
set spantree spanguardtrapenable 35-38
clear spantree spanguardtrap enable 35-38
show spantree backuproot 35-39
set spantree backuproot 35-39
clear spantree backuproot 35-40
show spantree backuproottrapendable 35-40
set spantree backuproottrapenable 35-41
clear spantree backuproottrapenable 35-41
show spantree newroottrapendable 35-42
set spantree newroottrapenable 35-42
clear spantree newroottrapenable 35-43
clear spantree default 35-43
show spantree debug 35-44
clear spantree debug 35-46

Chapter 36: Spanning Tree Port Commands

show spantree portenable 36-2
set spantree portenable 36-2
clear spantree portenable 36-3
show spantree portadmin 36-3
set spantree portadmin 36-4
clear spantree portadmin 36-5
set spantree protomigration 36-5
show spantree portstate 36-6
show spantree blockedports 36-6
show spantree portpri 36-7
set spantree portpri 36-8
clear spantree portpri 36-8
set spantree porthello 36-9
clear spantree porthello 36-9
show spantree portcost 36-10
show spantree adminpathcost 36-10
set spantree adminpathcost 36-11

clear spantree adminpathcost 36-12
show spantree adminedge 36-12
set spantree adminedge 36-13
clear spantree adminedge 36-13
show spantree operedge 36-14
show spantree adminpoint 36-14
show spantree operpoint 36-15
set spantree adminpoint 36-16
clear spantree adminpoint 36-16
show spantree restrictedtcn 36-17
set spantree restrictedtcn 36-17
clear spantree restrictedtcn 36-18
show spantree restrictedrole 36-19
set spantree restrictedrole 36-19
clear spantree restrictedrole 36-20

Chapter 37: Spanning Tree Loop Protect Commands

set spantree lp 37-2
show spantree lp 37-3
clear spantree lp 37-3
show spantree lplock 37-4
clear spantree lplock 37-5
set spantree lpcapablepartner 37-5
show spantree lpcapablepartner 37-6
clear spantree lpcapablepartner 37-7
set spantree lpthreshold 37-7
show spantree lpthreshold 37-8
clear spantree lpthreshold 37-8
set spantree lpwindow 37-9
show spantree lpwindow 37-9
clear spantree lpwindow 37-10
set spantree lptrapenable 37-10
show spantree lptrapenable 37-11
clear spantree lptrapenable 37-11
set spantree disputedbpduthreshold 37-12
show spantree disputedbpduthreshold 37-12
clear spantree disputedbpduthreshold 37-13
show spantree nonforwardingreason 37-13

Chapter 38: Shortest Path Bridging (SPB) Commands

show spb 38-1
set spb status 38-2
show spb basevid 38-3
show spb dynamic-ect-alg 38-4
set spb basevid 38-5
clear spb basevid 38-6
show spb port 38-6
set spb port status 38-7
clear spb port 38-8
set spb system 38-8
clear spb system 38-9
show spb neighbors 38-10
set spantree version spt 38-10
clear spantree version 38-11

Chapter 39: Routing as a Service (RaaS) Commands

show raas 39-1
raas 39-2
vrrp fabric-route-mode helper-router 39-3

Chapter 40: 802.1Q VLAN Commands

Reviewing Existing VLANs 40-1
show vlan 40-2
Creating and Naming Static VLANs 40-3
set vlan 40-3
set vlan name 40-4
clear vlan 40-4
clear vlan name 40-5
Assigning Port VLAN IDs (PVIDs) and Ingress Filtering 40-5
show port vlan 40-6
show vlan portinfo 40-7
set port vlan 40-8
clear port vlan 40-9
show vlan interface 40-9
set vlan interface 40-11
clear vlan interface 40-12
show port ingress filter 40-12
set port ingress filter 40-13
show vlan constraint 40-14
set vlan constraint 40-15
clear vlan constraint 40-16
show port discard 40-16
set port discard 40-17
clear port discard 40-17
Configuring the VLAN Egress List 40-18
show port egress 40-18
set vlan egress 40-19
clear vlan egress 40-20
show vlan dynamicegress 40-21
set vlan dynamicegress 40-21
Provider Bridging Commands 40-22
set bridge mode 40-22
show bridge mode 40-23

Chapter 41: GVRP Commands

show gvrp 41-1
show garp timer 41-2
set gvrp 41-3
clear gvrp 41-4
show gvrp vlan restricted 41-4
set gvrp vlan restricted 41-5
clear gvrp vlan restricted 41-6
set garp timer 41-6
clear garp timer 41-7

Chapter 42: MVRP Commands

show mrp timer 42-1
set mrp timer 42-2
clear mrp timer 42-3
show mvrp 42-4
set mvrp 42-5
clear mvrp 42-6
show mvrp vlan restricted 42-7
set mvrp vlan restricted 42-7
clear mvrp vlan restricted 42-8

Chapter 43: Policy Profile Commands

Policy Profile Commands 43-1
show policy profile 43-2
set policy profile 43-4
clear policy profile 43-6
show policy captive-portal 43-6
set policy captive-portal listening 43-7
clear policy captive-portal listening 43-8
set policy captive-portal web-redirect 43-8
clear policy captive-portal web-redirect 43-9
show policy dynamic 43-9
set policy dynamic 43-10
clear policy dynamic 43-11
show policy invalid 43-11
set policy invalid action 43-12
clear policy invalid action 43-12
set policy maptable 43-13
show policy maptable 43-14
clear policy maptable 43-15
show port tcioverwrite 43-15
set port tcioverwrite 43-16
Classification Rule Commands 43-16
show policy rule 43-17
show policy capability 43-21
set policy rule 43-23
clear policy rule 43-27
clear policy all-rules 43-29
show policy accounting 43-29
set policy accounting 43-30
clear policy accounting 43-30
set policy port 43-31
show policy allowed-type 43-31
set policy allowed-type 43-33
clear policy allowed-type 43-35
show policy dropped-notify 43-36
show policy disabled-ports 43-36
clear policy disabled-ports 43-37
clear policy usage-list 43-37
show policy autoclear 43-39
set policy autoclear 43-40
clear policy autoclear 43-40
clear policy port-hit 43-41
show policy syslog 43-42
set policy syslog 43-42

clear policy syslog 43-44

Chapter 44: System Logging Commands

show logging all 44-1
show logging server 44-4
set logging server 44-5
clear logging server 44-6
show logging default 44-7
set logging default 44-7
clear logging default 44-8
show logging application 44-9
set logging application 44-11
clear logging application 44-14
show logging local 44-14
set logging local 44-15
clear logging local 44-16
set logging here 44-16
clear logging here 44-17
show logging buffer 44-17

Chapter 45: Policy Class of Service (CoS) Commands

show cos state 45-2
set cos state 45-2
show cos port-type 45-3
show cos unit 45-4
show cos port-config 45-6
set cos port-config irl 45-7
clear cos port-config irl 45-7
set cos port-config txq 45-8
clear cos port-config txq 45-10
set cos port-config flood-ctrl 45-10
clear cos port-config flood-ctrl 45-11
show cos port-resource 45-12
set cos port-resource irl 45-12
clear cos port-resource irl 45-13
set cos port-resource txq 45-14
clear cos port-resource txq 45-15
set cos port-resource flood-ctrl 45-16
clear cos port-resource flood-ctrl 45-17
show cos reference 45-18
set cos reference irl 45-19
clear cos reference irl 45-19
set cos reference txq 45-20
clear cos reference txq 45-20
show cos settings 45-21
set cos settings 45-21
clear cos settings 45-23
show cos violation 45-23
clear cos violation 45-24
clear cos all-entries 45-25

Chapter 46: Network Monitoring Commands

show netstat 46-1
show users 46-3
tell 46-4
disconnect 46-5

Chapter 47: SMON Commands

show smon priority 47-1
set smon priority 47-2
clear smon priority 47-3
show smon vlan 47-3
set smon vlan 47-4
clear smon vlan 47-5

Chapter 48: RMON Commands

show rmon stats 48-2
set rmon stats 48-4
clear rmon stats 48-5
show rmon history 48-5
set rmon history 48-7
clear rmon history 48-8
show rmon alarm 48-9
set rmon alarm properties 48-10
set rmon alarm status 48-11
clear rmon alarm 48-12
show rmon event 48-13
set rmon event properties 48-14
set rmon event status 48-15
clear rmon event 48-15
show rmon host 48-16
set rmon host properties 48-17
set rmon host status 48-17
clear rmon host 48-18
show rmon topN 48-18
set rmon topN properties 48-20
set rmon topN status 48-20
clear rmon topN 48-21
show rmon matrix 48-21
set rmon matrix properties 48-23
set rmon matrix status 48-24
clear rmon matrix 48-24
show rmon channel 48-25
set rmon channel 48-25
clear rmon channel 48-26
show rmon filter 48-27
set rmon filter 48-28
clear rmon filter 48-28
show rmon capture 48-29
set rmon capture 48-30
clear rmon capture 48-31

Chapter 49: NetFlow Commands

show netflow 49-1
set netflow cache 49-3
clear netflow cache 49-3
set netflow export-data 49-4
clear netflow export-data 49-5
set netflow export-destination 49-5
clear netflow export-destination 49-6
set netflow export-interval 49-7
clear netflow export-interval 49-7
set netflow export-rate 49-8
clear netflow export-data 49-9
set netflow port 49-9
clear netflow port 49-10
set netflow export-version 49-10
clear netflow export-version 49-11
set netflow template 49-11
clear netflow template 49-13

Chapter 50: Connectivity Fault Management (CFM) Commands

Global Configuration Commands 50-1
cfm default-md 50-2
cfm enable 50-3
cfm logging filter 50-3
cfm md 50-4
cfm vlan-table 50-6
Default Maintenance Domain (MD) Configuration Commands 50-7
id-permission 50-7
level 50-9
mhf-creation 50-10
Maintenance Domain Configuration Commands 50-11
enable 50-11
ma 50-12
name 50-14
Maintenance Association Configuration Commands 50-15
ccm-interval 50-15
ma-comp 50-16
mep 50-17
mep-list 50-17
name 50-18
Maintenance Association Component Configuration Commands 50-19
vid 50-19
Maintenance End-Point Configuration Commands 50-20
active 50-21
alarm-defect-syslog 50-22
alarm-defect-trap 50-23
alarm-time 50-24
cci-enabled 50-25
direction 50-25
linktrace 50-26
loopback 50-28
port 50-29
priority 50-29
remote-mep active 50-30
reset-time 50-31

CFM Clear Commands 50-32
clear cfm bridge mip-ccm 50-32
clear cfm ccm-database 50-32
clear cfm counters 50-34
CFM Show Commands 50-35
show cfm all 50-35
show cfm bridge mip-ccm 50-37
show cfm default-md 50-37
show cfm md 50-38
show cfm md ma 50-40
show cfm md ma ma-comp 50-41
show cfm md ma mep 50-42
show cfm md ma mep ccm-errors 50-45
show cfm md ma mep linktrace 50-47
show cfm md ma mep-list 50-49
show cfm md ma mep remote-mep 50-50
show cfm md mip-ccm 50-52
show cfm stack-table 50-54
show cfm status 50-55

Chapter 51: Virtual Routing and Forwarding (VRF) Commands

set router vrf create 51-1
clear router vrf 51-2

Chapter 52: Global Configuration Address Family Commands

address-family 52-1
topology 52-2

Chapter 53: Router Commands

show router 53-1
show limits 53-3
set limits 53-6
clear limits 53-7
set router vrf create 53-8
clear router vrf 53-9
router 53-9
show running-config 53-10

Chapter 54: Routing Interface Commands

show interface 54-1
interface 54-2
ip forwarding 54-4
ip ecm-forwarding-algo 54-4
show ip interface 54-5
ip address 54-6
ip checkspoof 54-7
ip icmp unreachable 54-8
ip icmp redirects 54-9
ip icmp echo-reply 54-9
secondary-vlan 54-10
no shutdown 54-11

Chapter 55: IPv6 Interface Commands

show ipv6 interface 55-1
ipv6 address 55-3
ipv6 checkspoof 55-5
ipv6 forwarding 55-6
ipv6 icmp unreachable 55-6
ipv6 icmp redirects 55-7
ipv6 icmp echo-reply 55-7
ipv6 nd dad attempts 55-8
ipv6 nd managed-config-flag 55-9
ipv6 nd ns-interval 55-9
ipv6 nd other-config-flag 55-10
ipv6 nd prefix 55-11
ipv6 nd ra hoplimit suppress 55-11
ipv6 nd ra interval 55-12
ipv6 nd ra lifetime 55-13
ipv6 nd ra mtu 55-14
ipv6 nd ra suppress 55-14
ipv6 nd reachable-time 55-15

Chapter 56: IP Traffic Routes Commands

show ip route 56-1
show ipv6 route 56-4
ip route 56-5
ipv6 route 56-7
set ip route 56-9
clear ip route 56-10
ip icmp 56-10
ipv6 neighbor 56-11
ipv6 nd delay-time 56-12
ipv6 nd reachable-time 56-12
ipv6 nd retransmit-time 56-13
ipv6 nd stale-time 56-13
show ipv6 neighbors 56-14
show ipv6 general-prefix 56-16
ipv6 general-prefix 56-17

Chapter 57: Tunnel Configuration Commands

Reviewing Existing Tunnels 57-1
show tunnel 57-1
Configuring Tunnels 57-4
tunnel source 57-4
tunnel destination 57-5
tunnel any-remote enable 57-7
tunnel keepalive 57-8
tunnel keyword 57-8
tunnel mode 57-9
tunnel mode gre l2 (Virtual Private Port) 57-10
tunnel mode gre l2 (Virtual Private Ethernet Service) 57-11
tunnel mirror enable 57-12
tunnel mode gre l2 (mirrored tunnel) 57-13
tunnel probe 57-14
tunnel tos 57-15

Chapter 58: L3 VPN Commands

VRF L3 VPN Commands 58-1
mpls ip 58-2
mpls ipv6 58-2
mpls ldp-lsr-id 58-3
mpls label-protocol-ldp 58-4
mpls ldp-label-allocate 58-5
mpls ldp-label-retention-mode 58-6
mpls ip propagate-ttl 58-7
mpls label mode 58-7
rd 58-8
route-target 58-10
vpn id 58-11
show mpls interface 58-12
show mpls forwarding-table 58-13
show mpls ldp-parameters 58-14
show mpls ip-bindings 58-15
show mpls ldp-neighbor 58-16
BGP L3 VPN Commands 58-17
address-family 58-17
enable 58-19
neighbor activate 58-19
show ip bgp vpn 58-20
show ip bgp vpn vrf 58-23
show ipv6 bgp vpn 58-26
show ipv6 bgp vpn vrf 58-28

Chapter 59: ARP Table Commands

show arp 59-1
set arp 59-3
clear arp 59-4
arp 59-4
arp timeout 59-5
arp retransmit-time 59-6
arp stale-entry-timeout 59-7
arp-nd-proxy-all 59-7
ip gratuitous-arp 59-8
ip gratuitous-arp-learning 59-8
ip proxy-arp 59-9
ip mac-address 59-10
ip multicast-arp-learning 59-11
clear arp-cache 59-11

Chapter 60: Broadcast Configuration Commands

ip directed-broadcast 60-1
ip forward-protocol 60-2
ip dhcp relay information option 60-3
ip dhcp relay information option vpn 60-4
ip dhcp relay information option server-override 60-5
ip dhcp relay information option remote-id 60-6
ip dhcp relay information option circuit-id 60-7
ip dhcp relay information option link-selection 60-8
ip dhcp relay source-interface 60-9
ip helper-address 60-11

Chapter 61: IP Debug

debug ip bgp 61-1
debug ip ospf 61-2
debug packet restart 61-3
debug packet show-statistics 61-3
debug packet clear-statistics 61-4
debug packet filter 61-5
debug packet control 61-6
show debugging 61-7
debug ip vrrp 61-9
debug ip vrrp show 61-9

Chapter 62: IGMP Commands

Enabling / Disabling IGMP 62-1
show igmp enable 62-1
set igmp enable 62-2
set igmp disable 62-2
Configuring IGMP 62-3
show igmp config 62-4
set igmp config 62-5
show igmp counters 62-7
clear igmp counters 62-7
set igmp delete 62-8
show igmp flows 62-8
show igmp flow-full-action 62-10
set igmp flow-full-action 62-10
show igmp groups 62-11
set igmp input-filter 62-13
show igmp input-filter 62-14
clear igmp input-filter 62-14
show igmp number-flows 62-15
show igmp portFastLeave 62-15
set igmp portFastLeave 62-16
clear igmp portFastLeave 62-16
show igmp protocols 62-17
set igmp protocols 62-18
clear igmp protocols 62-18
show igmp query 62-19
set igmp query-enable 62-20
set igmp query-disable 62-20
show igmp reporters 62-21
show igmp static 62-22
set igmp static 62-22
clear igmp static 62-23
set igmp unknown-input-action 62-25
show igmp unknown-input-action 62-25
show igmp vlan 62-26

Chapter 63: Multicast Listener Discovery (MLD) Commands

set mld enable 63-2
show mld enable 63-2
set mld disable 63-3
set mld delete 63-3
set mld config 63-4
show mld config 63-5

show mld counters 63-6
clear mld counters 63-7
set mld query-enable 63-7
set mld query-disable 63-8
show mld query 63-8
set mld flow-full-action 63-9
show mld flow-full-action 63-10
show igmp groups 63-10
set mld input-filter 63-12
show mld input-filter 63-13
clear mld input-filter 63-14
set mld static 63-14
clear mld static 63-15
set mld protocols 63-15
clear mld protocols 63-16
show mld protocols 63-17
set mld portFastLeave 63-17
clear mld portFastLeave 63-18
show mld portFastLeave 63-19
show mld number-flows 63-19
show mld vlan 63-20
show mld groups 63-20
show mld static 63-23
show mld reporters 63-23
show mld flows 63-24
set mld unknown-input-action 63-25
show mld unknown-input-action 63-26

Chapter 64: IPv4 PIM Commands

ip mroute 64-2
ip pim sparse-mode 64-4
ip pim dense-mode 64-4
ip pim ssm 64-5
ip pim anycast-rp 64-6
ip pim asm-join-filter 64-7
ip pim ssm-join-filter 64-7
ip pim bsr-candidate 64-8
ip pim bsr-border 64-9
ip pim dr-priority 64-9
ip pim graceful-restart 64-10
ip pim multipath 64-11
ip pim neighbor-filter 64-12
ip pim rp-address 64-12
ip pim rp-candidate 64-13
ip pim state-refresh origination-interval 64-14
ip pim static-rp-override 64-15
show ip mroute 64-15
show ip mcache 64-17
show ip pim 64-19
show ip pim anycast-rp 64-20
show ip pim bsr 64-21
show ip pim interface 64-23
show ip pim mrt 64-24
show ip pim mrt type 64-26
show ip pim neighbor 64-28

show ip pim rp 64-30
show ip pim rp-hash 64-32
show ip pim statistics 64-32
clear ip mroute 64-33
clear ip pim statistics 64-34

Chapter 65: IPv6 PIM Commands

ipv6 mroute 65-2
ipv6 pim sparse mode 65-3
ipv6 pim dense-mode 65-4
ipv6 pim ssm 65-5
ipv6 pim static-rp-override 65-5
ipv6 pim state-refresh origination-interval 65-6
ipv6 pim asm-join-filter 65-7
ipv6 pim ssm-join-filter 65-7
ipv6 pim bsr candidate bsr 65-8
ipv6 pim bsr candidate rp 65-9
ipv6 pim dr-priority 65-10
ipv6 pim rp-address 65-10
ipv6 pim anycast-rp 65-11
ipv6 pim graceful-restart 65-12
ipv6 pim multipath 65-13
ipv6 pim neighbor-filter 65-14
clear ipv6 mroute 65-15
clear ipv6 pim statistics 65-15
show ipv6 mcache 65-16
show ipv6 mroute 65-17
show ipv6 pim 65-19
show ipv6 pim anycast-rp 65-20
show ipv6 pim bsr 65-20
show ipv6 pim interface 65-22
show ipv6 pim mrt 65-24
show ipv6 pim mrt type 65-26
show ipv6 pim neighbor 65-27
show ipv6 pim rp 65-29
show ipv6 pim rp-hash 65-30
show ipv6 pim statistics 65-30

Chapter 66: MSDP Commands

show ip msdp peer 66-1
ip msdp peer 66-2
clear ip msdp peer 66-3
ip msdp shutdown 66-3
ip msdp originator-id 66-4
show ip msdp sa-cache 66-5
clear ip msdp sa-cache 66-5
ip msdp sa-filter in 66-6
ip msdp sa-filter out 66-6
ip msdp mesh-group 66-7
show ip msdp summary 66-8
clear ip msdp peer statistics 66-8

Chapter 67: DVMRP Commands

ip dvmrp 67-1
ip dvmrp metric 67-2
show ip dvmrp route 67-3
show ip dvmrp 67-4
show ip dvmrp interface 67-5
show ip dvmrp neighbor 67-5

Chapter 68: Network Address Translation (NAT) Commands

ip nat pool 68-2
ipv6 nat pool 68-3
ip nat inside 68-4
ipv6 nat inside 68-4
ip nat outside 68-5
ipv6 nat outside 68-6
ip nat inside source list 68-6
ipv6 nat inside source list 68-8
ip nat inside source static (NAT) 68-10
ipv6 nat inside source static (NAT) 68-11
ip nat inside source static (NAPT) 68-12
ip nat ftp-control-port 68-14
ip nat translation max-entries 68-14
ipv6 nat translation max-entries 68-15
ip nat translation (timeouts) 68-16
ipv6 nat translation (timeouts) 68-17
ip nat translation protocol 68-17
ipv6 nat translation protocol 68-18
ip nat log translations 68-19
ipv6 nat log translations 68-20
ip nat inspect dns 68-21
ipv6 nat inspect dns 68-21
show ip nat bindings 68-22
show ipv6 nat bindings 68-24
clear ip nat bindings 68-26
clear ipv6 nat bindings 68-27
show ip nat info 68-28
show ipv6 nat info 68-29
show ip nat lists 68-31
show ipv6 nat lists 68-32
show ip nat pools 68-33
show ipv6 nat pools 68-34
show ip nat statics 68-35
show ipv6 nat statics 68-36
show ip nat statistics 68-36
show ipv6 nat statistics 68-37
clear ip nat statistics 68-38
clear ipv6 nat statistics 68-39

Chapter 69: LSNAT Commands

show ip slb serverfarms 69-3
show ipv6 slb serverfarms 69-3
description 69-4
inservice 69-5
this 69-6
ip slb binding finrst-timeout 69-6

ipv6 slb binding finrst-timeout 69-7
ip slb binding finrst-timeout disabled 69-8
ipv6 slb binding finrst-timeout disabled 69-8
ip slb tftpctrlport 69-9
ipv6 slb tftpctrlport 69-10
ip slb serverfarm 69-10
ipv6 slb serverfarm 69-11
real 69-11
predictor 69-12
faildetect probe 69-13
faildetect type 69-14
faildetect reset 69-15
show ip slb reals 69-16
show ipv6 slb reals 69-18
maxconns 69-21
weight 69-22
show ip slb vservers 69-23
show ipv6 slb vservers 69-24
ip slb vserver 69-26
ipv6 slb vserver 69-26
binding match source-port 69-27
serverfarm (Virtual Server) 69-28
virtual 69-29
virtual-range 69-30
udp-one-shot 69-32
vrrp vlan 69-33
client 69-34
source nat pool 69-35
idle timeout 69-36
sticky type 69-37
sticky timeout 69-38
ip slb real-server access client 69-39
ipv6 slb real-server access client 69-39
ip slb real-server access tcp-reset 69-40
ipv6 slb real-server access tcp-reset 69-41
ip slb real-server access unrestricted 69-41
ipv6 slb real-server access unrestricted 69-42
show ip slb statistics 69-42
show ipv6 slb statistics 69-43
show ip slb info 69-44
show ipv6 slb info 69-45
show ip slb sticky 69-46
show ipv6 slb sticky 69-47
show ip slb statistics-sticky 69-49
show ipv6 slb statistics-sticky 69-49
show ip slb bindings 69-50
show ipv6 slb bindings 69-51
clear ip slb 69-53
clear ipv6 slb 69-54
clear ip slb statistics 69-54
clear ipv6 slb statistics 69-55

Chapter 70: Transparent Web Cache Balancing (TWCB) Commands

ip twcb wcserverfarm 70-2
ipv6 twcb wcserverfarm 70-3
description 70-3
predictor 70-4
cache 70-5
weight 70-6
faildetect probe 70-7
faildetect app-port 70-8
faildetect type 70-9
faildetect reset 70-10
maxconns 70-11
inservice 70-12
this 70-13
ip twcb webcache 70-14
ipv6 twcb webcache 70-14
destination ip 70-15
idle timeout 70-16
serverfarm 70-17
source nat pool 70-17
bypass-list 70-19
host redirect 70-20
ip twcb redirect out 70-21
ipv6 twcb redirect out 70-22
show ip twcb wcserverfarms 70-22
show ipv6 twcb wcserverfarms 70-23
show ip twcb webcaches 70-24
show ipv6 twcb webcaches 70-25
show ip twcb info 70-26
show ipv6 twcb info 70-26
show ip twcb caches 70-27
show ipv6 twcb caches 70-29
show ip twcb bindings 70-31
show ipv6 twcb bindings 70-32
show ip twcb statistics 70-34
show ipv6 twcb statistics 70-35
clear ip twcb 70-36
clear ipv6 twcb 70-36

Chapter 71: RIP Commands

router rip 71-1
network 71-2
distance 71-3
ip rip offset 71-4
timers 71-4
key chain 71-5
key 71-6
key-string 71-6
accept-lifetime 71-7
send-lifetime 71-8
ip rip authentication keychain 71-9
ip rip authentication mode 71-10
passive-interface 71-10
redistribute 71-11
show ip protocols 71-12

Chapter 72: Border Gateway Protocol Commands

BGP Configuration Commands 72-1
router bgp 72-3
bgp address-family 72-4
aggregate-address 72-5
bgp aggregate-med 72-7
bgp always-compare-med 72-8
bgp automatic-route-refresh 72-9
bgp cluster-id 72-9
bgp confederation-id 72-10
bgp deterministic-med 72-11
bgp distance 72-11
bgp orf comm-filter 72-12
bgp orf extcomm-filter 72-13
bgp orf prefix-filter 72-14
bgp graceful-restart 72-15
bgp local-pref 72-16
bgp max-ebgp-ecmp-routes 72-16
bgp max-ibgp-ecmp-routes 72-17
bgp restart-defer 72-18
bgp restart-time 72-19
bgp restart-timeout 72-19
bgp router-id 72-20
bgp stale-path-time 72-21
bgp strict-confeds 72-22
bgp trap 72-22
enable 72-23
ip prefix-list 72-24
ipv6 prefix-list 72-25
log-up-down 72-27
network 72-27
redistribute bgp 72-29
redistribute blackhole 72-30
redistribute connected 72-31
redistribute rip 72-32
redistribute static 72-33
redistribute ospf 72-34
redistribute isis 72-35
neighbor advertisement-interval 72-36
neighbor advertise-map 72-37
neighbor activate 72-39
neighbor aggregate-confed 72-39
neighbor as-origination-interval 72-40
neighbor check-next-hop 72-41
neighbor clear-counters 72-42
neighbor confed-member 72-42
neighbor connect-retry-interval 72-43
neighbor default-originate 72-44
neighbor enable 72-45
neighbor idle-hold-interval 72-45
neighbor ignore-leading-as 72-46
neighbor maximum-orf 72-47
neighbor maximum-prefix 72-48
neighbor next-hop-peer 72-49
neighbor next-hop-self 72-49

neighbor open-delay 72-50
neighbor passive 72-51
neighbor peer-group 72-52
neighbor peer-type 72-53
neighbor peering-type 72-53
neighbor remote-as 72-54
neighbor remove-private-as 72-55
neighbor route-map 72-56
neighbor route-reflector-client 72-57
neighbor route-withdraw-interval 72-58
neighbor soft-reconfiguration 72-58
neighbor timers 72-59
neighbor ttl 72-60
neighbor update-source 72-61
Route Flap Damping Commands 72-62
dampen-flap 72-62
cutoff 72-63
half-life-reach 72-64
half-life-unreach 72-64
hold-time 72-65
memory-limit-reach 72-66
memory-limit-unreach 72-67
reuse 72-67
Querying and Clearing Commands 72-68
clear ip bgp 72-68
clear ip bgp flap-all-stats 72-69
clear ip bgp flap-count 72-70
clear ip bgp topology 72-70
show ip bgp 72-71
show ip bgp dampened-routes 72-75
show ip bgp groups 72-76
show ip bgp neighbors 72-77
show ip bgp topology 72-78
show ip bgp summary 72-79
show ipv6 bgp 72-79
show ipv6 bgp neighbors 72-80
show ipv6 bgp summary 72-82

Chapter 73: OSPFv2 Commands

router ospf 73-3
address-family ipv4 73-3
network 73-4
router-id 73-5
neighbor 73-5
passive-interface 73-6
redistribute 73-7
distribute-list route-map in 73-8
rfc1583compatible 73-9
log-adjacency 73-9
spf lsa-thresholds 73-10
spf pause-frequency 73-11
timers spf 73-12
bfd all-intfs-on 73-12
distance ospf 73-13
enable-pe-ce 73-14

domain-tag 73-15
domain-id 73-16
area range 73-17
area stub 73-18
area default cost 73-18
area nssa 73-19
area nssa-range 73-20
area sham-link 73-20
area sham-link authentication-key 73-21
area sham-link dead-interval 73-22
area sham-link hello-interval 73-23
area sham-link keychain 73-24
area sham-link message-digest-key 73-25
area sham-link retransmit-interval 73-26
area sham-link transmit-delay 73-27
area sham-link cost 73-28
area virtual-link 73-29
auto-cost reference-bandwidth 73-30
graceful-restart enable 73-31
graceful-restart restart-interval 73-32
ip ospf cost 73-32
ip ospf cost track 73-33
ip ospf network 73-34
ip ospf priority 73-35
ip ospf poll-interval 73-35
ip ospf retransmit-interval 73-36
ip ospf transmit-delay 73-37
ip ospf ignore-mtu 73-37
ip ospf hello-interval 73-38
ip ospf dead-interval 73-39
ip ospf authentication-key 73-40
ip ospf message-digest-key md5 73-40
ip ospf helper-disable 73-41
ip ospf network 73-42
show ip ospf 73-42
show ip ospf database 73-44
show ip ospf border-routers 73-46
show ip ospf interface 73-47
show ip ospf neighbor 73-48
show ip ospf sham-link 73-49
show ip ospf virtual-links 73-50
show ip protocols 73-51
clear ip ospf process 73-52
debug ip ospf 73-52

Chapter 74: OSPFv3 Commands

Router OSPFv3 Configuration Commands 74-1
ipv6 router ospf 74-2
address-family ipv6 74-3
area default-cost 74-3
area nssa 74-4
area nssa-range 74-5
area range 74-6
area sham-link 74-6
area sham-link authentication-key 74-8

area sham-link dead-interval 74-9
area sham-link hello-interval 74-10
area sham-link keychain 74-11
area sham-link message-digest-key 74-11
area sham-link retransmit-interval 74-12
area sham-link transmit-delay 74-13
area sham-link cost 74-14
show ip ospf sham-link 74-15
area stub 74-16
area virtual-link 74-16
auto-cost reference-bandwidth 74-18
bfd all-intfs-on 74-19
distance (OSPF) 74-19
distribute-list route-map in 74-21
domain-id 74-21
enable-pe-ce 74-22
graceful-restart enable 74-23
graceful-restart restart-interval 74-24
log-adjacency 74-24
passive-interface 74-25
redistribute 74-26
router-id 74-27
spf lsa-thresholds 74-27
spf pause-frequency 74-28
timers spf 74-29
OSPFv3 Interface Commands 74-30
ipv6 ospf 74-30
ipv6 ospf authentication 74-31
ipv6 ospf encryption 74-32
crypto ipsec 74-34
ipv6 ospf cost 74-34
ip ospf cost track 74-35
ipv6 ospf dead-interval 74-36
ipv6 ospf hello-interval 74-37
ipv6 ospf helper-disable 74-38
ipv6 ospf ignore-mtu 74-38
ipv6 ospf neighbor 74-39
ipv6 ospf poll-interval 74-40
ipv6 ospf neighbor priority 74-40
ipv6 ospf neighbor cost 74-41
ipv6 ospf neighbor database-filter-all-out 74-42
ipv6 ospf network 74-42
ipv6 ospf priority 74-43
ipv6 ospf retransmit-interval 74-44
ipv6 ospf transmit-delay 74-44
OSPFv3 Show Commands 74-45
show ipv6 ospf 74-45
show ipv6 ospf database 74-46
show ipv6 ospf border-routers 74-48
show ipv6 ospf interface 74-48
show ipv6 ospf neighbor 74-50
show ipv6 ospf virtual-links 74-51

Chapter 75: Intermediate System To Intermediate System (IS-IS) Commands

IS-IS Configuration Overview 75-1
Configuration Commands 75-1
router isis 75-2
address-family 75-3
area-password 75-4
authentication key-chain 75-4
authentication mode 75-5
authentication send-only 75-6
distance (IS-IS) 75-7
domain-password 75-8
graceful-restart enable 75-9
graceful-restart enable-help-peer 75-9
graceful-restart restart-adj-interval 75-10
graceful-restart restart-interval 75-11
graceful-restart restart-sync-interval 75-11
hostname dynamic 75-12
ignore-lsp-errors 75-13
is-type 75-13
lsp-buf-size 75-14
lsp-gen-interval 75-15
max-lsp-lifetime 75-16
maximum-paths 75-16
metric-style 75-17
net 75-18
redistribute 75-19
set-overload-bit 75-20
spf-interval 75-21
summary-address 75-22
Interface Commands 75-22
ip router isis 75-23
ipv6 router isis 75-24
isis authentication key-chain 75-24
isis authentication mode 75-25
isis authentication send-only 75-26
isis circuit-type 75-27
isis csnp-interval 75-28
isis hello-interval 75-29
isis hello-multiplier 75-30
isis hello-padding 75-30
isis lsp-mtu 75-31
isis lsp-throttle 75-32
isis metric 75-33
isis network-point-to-point 75-33
isis passive-interface 75-34
isis password 75-35
isis priority 75-35
isis retransmit-interval 75-36
Show Commands 75-37
show isis database 75-37
show isis hostname 75-39
show isis lsp-log 75-40
show isis neighbors 75-40
show isis topology 75-41

Chapter 76: VRRP Commands

vrrp create 76-1
vrrp address 76-2
vrrp primary-address 76-3
vrrp priority 76-4
vrrp accept-mode 76-5
vrrp advertise-interval 76-6
vrrp authentication 76-7
vrrp critical-ip 76-7
vrrp enable 76-9
vrrp interface-up-delay 76-10
vrrp fabric-route-mode 76-10
vrrp host-mobility 76-11
vrrp host-mobility-acl 76-12
host-mobility timeout 76-13
vrrp preempt 76-14
vrrp preempt-delay 76-14
show ip vrrp 76-15

Chapter 77: MAC Locking Commands

show maclock 77-2
set maclock enable 77-4
set maclock disable 77-4
set maclock disable-port 77-5
clear maclock disable-port 77-5
set maclock 77-6
set maclock firstarrival 77-7
clear maclock firstarrival 77-7
set maclock agefirstarrival 77-8
clear maclock agefirstarrival 77-9
set maclock clearonlinkchange 77-9
clear maclock clearonlinkchange 77-10
set maclock move 77-10
set maclock static 77-11
clear maclock static 77-11
set maclock trap 77-12
clear maclock trap 77-12
set maclock syslog 77-13
clear maclock syslog 77-13
clear maclock 77-14

Chapter 78: TACACS+ Commands

show tacacs 78-1
set tacacs 78-3
show tacacs server 78-3
set tacacs server 78-4
clear tacacs server 78-5
show tacacs session 78-5
set tacacs session 78-6
clear tacacs session authorization 78-8
show tacacs command 78-8
set tacacs command 78-9
show tacacs singleconnect 78-10
set tacacs singleconnect 78-10

Chapter 79: Host DoS Commands

show hostdos 79-1
hostdos 79-3

Chapter 80: Flow Setup Throttling (FST) Commands

show flowlimit 80-1
set flowlimit 80-3
set flowlimit limit 80-3
clear flowlimit limit 80-4
set flowlimit action 80-5
clear flowlimit action 80-6
show flowlimit class 80-7
set flowlimit port 80-8
set flowlimit port class 80-9
set flowlimit port status 80-9
clear flowlimit port class 80-10
set flowlimit shutdown 80-10
set flowlimit notification 80-11
clear flowlimit notification interval 80-12
clear flowlimit stats 80-12

Chapter 81: Access Control List Commands

Named Access Control Lists 81-1
ip access-list standard 81-1
ip access-list extended 81-2
ip access-list copy to 81-3
ip access-list append to 81-4
ip access-list check 81-4
Access Control List Entry Configuration Commands 81-5
permit 81-6
deny 81-9
log 81-12
delete 81-12
insert before 81-13
replace 81-15
move before 81-16
remark 81-17
Displaying and Applying Access Control List Commands 81-18
ip access-group 81-18
ip host-access 81-19
show access-lists 81-19
show access-lists applied 81-21
clear access-lists counters 81-22

Chapter 82: IPv6 Access Control List Commands

Named Access Control Lists 82-1
ipv6 access-list standard 82-1
ipv6 access-list extended 82-2
ipv6 access-list copy to 82-3
ipv6 access-list append to 82-3
ipv6 access-list check 82-4
Access Control List Entry Configuration Commands 82-5
permit 82-5
deny 82-9

log 82-12
delete 82-13
insert before 82-14
name 82-16
replace 82-17
move before 82-20
remark 82-21
Displaying and Applying Access Control List Commands 82-21
ipv6 access-group 82-22
ipv6 host-access 82-23
show access-lists 82-23
show access-lists applied 82-24
clear access-lists counters 82-25

Chapter 83: Layer 2 Access Control List Commands

Named Layer 2 Access Control Lists 83-1
l2 access-list 83-1
l2 access-list copy to 83-2
l2 access-list append to 83-3
l2 access-list check 83-3
Access Control List Entry Configuration Commands 83-4
permit 83-4
deny 83-6
log 83-8
log-verbose 83-9
delete 83-10
insert before 83-10
replace 83-12
move before 83-14
remark 83-15
Displaying and Applying Access Control List Commands 83-15
l2 access-group 83-16
show access-lists l2 83-16
show access-lists applied 83-17
clear access-lists counters 83-18

Chapter 84: VRF Access Control List Commands

vrf-access 84-1
ip access-group from-vrf 84-2
ip access-group from-any-vrf 84-3
ip access-group to-vrf 84-3
ip access-group to-any-vrf 84-4
ipv6 access-group from-vrf 84-5
ipv6 access-group from-any-vrf 84-5
ipv6 access-group to-vrf 84-6
ipv6 access-group to-any-vrf 84-7

Chapter 85: Route-Map Manager Commands

General Route-Map Commands 85-1
route-map probe 85-1
show ip policy 85-3
show route-map 85-4
Policy-Based Route-Map Commands 85-4
route-map policy 85-5
ip policy route-map 85-6

ipv6 policy route-map 85-7
ip policy priority 85-8
ipv6 policy priority 85-8
ip policy load-policy 85-9
ipv6 policy load-policy 85-10
match ip address (policy) 85-11
set next-hop (policy) 85-12
set next-hop-v6 (policy) 85-12
set default-next-hop (policy) 85-13
set default-next-hop-v6 (policy) 85-14
set vrf (policy) 85-15
Redistribution Route-Map Commands 85-16
route-map redistribution 85-16
match interface (redistribution) 85-18
match ip address (redistribution) 85-18
match ipv6 address (redistribution) 85-19
match metric (redistribution) 85-19
match tag (redistribution) 85-20
set tag (redistribution) 85-21
set metric (redistribution) 85-22
set metric decrement (redistribution) 85-22
set metric increment (redistribution) 85-23
set metric-type (redistribution) 85-24
Filter-Based Route-Map Commands 85-24
route-map filter 85-25
match interface (filter) 85-26
match ip (filter) 85-26
match ipv6 (filter) 85-27
match tag (filter) 85-28
match metric (filter) 85-29
match route-type (filter) 85-30
BGP Route-Map Commands 85-31
route-map bgp 85-31
match afi 85-32
match safi 85-33
match as-path 85-34
match community 85-35
match extended-community 85-36
match prefix-list 85-37
match med 85-38
set as 85-38
set as-path-limit 85-39
set community 85-40
set extended-community ip-route-target 85-41
set extended-community as-route-target 85-42
set extended-community ip-site-of-origin 85-43
set extended-community as-site-of-origin 85-44
set extended-community as4-route-target 85-45
set extended-community as4-site-of-origin 85-46
set extended-community ospf-domain-id 85-47
set extended-community ospf-router-id 85-48
set extended-community ospf-route-type 85-49
set local-preference 85-50
set med 85-51
set ip next-hop 85-51
set origin 85-52

set orf-association local 85-53
set weight 85-54
set flap-table 85-54

Chapter 86: RADIUS Commands

show radius 86-1
set radius 86-3
set radius mgmt attribute 86-4
set radius retries 86-5
set radius timeout 86-5
set radius server 86-6
set radius realm 86-6
clear radius 86-7
show radius accounting 86-7
set radius accounting 86-9
clear radius accounting 86-10

Chapter 87: RFC 3580 Commands

show vlanauthorization 87-1
set vlanauthorization 87-2
clear vlanauthorization 87-2
set vlanauthorization port 87-3

Chapter 88: Quarantine Agent Authentication Commands

show quarantine-agent 88-1
set quarantine-agent 88-2
set quarantine-agent port 88-4
clear quarantine-agent 88-4
set quarantine accounting 88-5
set quarantine-agent port authallocated 88-5
set quarantine-agent port idle-timeout 88-6
set quarantine-agent port session-timeout 88-7

Chapter 89: 802.1X Authentication Commands

show dot1x 89-1
show dot1x auth-config 89-3
set dot1x 89-5
set dot1x auth-config 89-6
clear dot1x auth-config 89-7

Chapter 90: Port Web Authentication (PWA) Commands

show pwa 90-2
set pwa 90-4
set pwa hostname 90-4
clear pwa hostname 90-5
show pwa banner 90-5
set pwa banner 90-6
clear pwa banner 90-6
set pwa displaylogo 90-7
set pwa redirecttime 90-7
clear pwa redirecttime 90-8
set pwa ipaddress 90-8
clear pwa ipaddress 90-9
set pwa protocol 90-9

clear pwa protocol 90-10
set pwa enhancedmode 90-10
set pwa guestname 90-11
clear pwa guestname 90-11
set pwa guestpassword 90-12
set pwa gueststatus 90-12
set pwa initialize 90-13
set pwa quietperiod 90-14
clear pwa quietperiod 90-14
set pwa maxrequest 90-15
clear pwa maxrequest 90-15
set pwa portcontrol 90-16
show pwa session 90-17
show pwa summary 90-17

Chapter 91: MAC Authentication Commands

show macauthentication 91-1
show macauthentication session 91-3
set macauthentication 91-4
set macauthentication password 91-5
clear macauthentication password 91-5
set macauthentication significant-bits 91-6
clear macauthentication significant-bits 91-6
set macauthentication port 91-7
set macauthentication authallocated 91-7
clear macauthentication authallocated 91-8
set macauthentication portinitialize 91-8
set macauthentication macinitialize 91-9
set macauthentication reauthentication 91-9
set macauthentication portreauthenticate 91-10
set macauthentication macreauthenticate 91-10
set macauthentication reauthperiod 91-11
clear macauthentication reauthperiod 91-11
set macauthentication quietperiod 91-12
clear macauthentication quietperiod 91-12

Chapter 92: Convergence End Points (CEP) Phone Detection Commands

show cep connections 92-1
show cep detection 92-2
show cep policy 92-3
show cep port 92-4
set cep 92-4
set cep accounting 92-5
set cep port 92-5
set cep policy 92-6
set cep detection-id 92-6
set cep detection-id type 92-7
set cep detection-id address 92-8
set cep detection-id protocol 92-9
set cep detection-id porthigh | portlow 92-9
set cep initialize 92-10
clear cep 92-11

Chapter 93: RADIUS Snooping Commands

set radius-snooping 93-1
set radius-snooping accounting 93-2
set radius-snooping timeout 93-2
set radius-snooping port 93-3
set radius-snooping flow 93-4
set radius-snooping initialize 93-5
clear radius-snooping all 93-5
clear radius-snooping flow 93-6
clear radius-snooping port 93-6
show radius-snooping 93-7
show radius-snooping port 93-8
show radius-snooping flow 93-9
show radius-snooping session 93-10

Chapter 94: Auto-Tracking Authentication Commands

show auto-tracking 94-1
set auto-tracking 94-2
set auto-tracking accounting 94-4
set auto-tracking port 94-4
clear auto-tracking 94-5
set auto-tracking port authallocated 94-5
set auto-tracking port idle-timeout 94-6
set auto-tracking port radius-timeout-profile 94-7
set auto-tracking port radius-reject-profile 94-7
set auto-tracking port session-timeout 94-8

Chapter 95: Anti-Spoofing Commands

show antispoof 95-2
set antispoof 95-2
clear antispoof 95-3
set antispoof notifications 95-4
clear antispoof notifications 95-4
set antispoof notifications interval 95-5
clear antispoof notifications interval 95-5
set antispoof duplicateIP 95-6
clear antispoof duplicateIP 95-6
show antispoof class 95-7
set antispoof class 95-8
set antispoof class threshold-index 95-9
clear antispoof class 95-11
set antispoof dhcp-snooping 95-11
set antispoof dhcp-snooping mac-verification 95-13
set antispoof dhcp-snooping port-mode 95-13
clear antispoof dhcp-snooping 95-14
set antispoof arp-inspection 95-15
clear antispoof arp-inspection 95-16
set antispoof ip-inspection 95-17
clear antispoof ip-inspection 95-18
show antispoof port 95-18
set antispoof port-class 95-19
clear antispoof port-class 95-20
show antispoof binding 95-21
clear antispoof binding 95-22
show antispoof counters 95-23

clear antispoof counters 95-24

Chapter 96: MultiAuth Commands

set multiauth mode 96-2
clear multiauth mode 96-2
show multiauth 96-3
show multiauth counters 96-4
set multiauth precedence 96-5
clear multiauth precedence 96-6
show multiauth port 96-6
set multiauth port 96-7
clear multiauth port 96-8
show multiauth station 96-8
clear multiauth station 96-9
show multiauth session 96-9
show multiauth idle-timeout 96-11
set multiauth idle-timeout 96-11
clear multiauth idle-timeout 96-12
show multiauth session-timeout 96-13
set multiauth session-timeout 96-14
clear multiauth session-timeout 96-15
clear multiauth session 96-16
set multiauth sessions-unique-per-port 96-17
clear multiauth sessions-unique-per-port 96-17
set multiauth trap 96-18
clear multiauth trap 96-19
show multiauth trap 96-19

Tables

1-1 show version Output Details 1-7
2-1 Basic Line Editing Emacs & vi Commands 2-1
3-1 show system login Output Details 3-4
3-2 show system password Output Details 3-14
3-3 show system lockout Output Details 3-20
5-1 X.509 Subject Field Distinguished Name Attributes 5-14
7-1 Show System Output Display 7-9
8-1 show mac Output Details 8-4
11-1 show ip dns Output Details 11-11
12-1 show nodealias Output Details 12-2
12-2 Supported Node Alias Entry Protocols 12-3
12-3 show nodealias config Output Details 12-6
13-1 show sntp Output Details 13-3
17-1 dir Output Details 17-4
17-2 show boot high-availability Output Details 17-10
18-1 show bonding Output Details 18-3
20-1 show cdp Output Details 20-9
20-2 show ciscodp Output Details 20-14
20-3 show port ciscodp info Output Details 20-15
20-4 show lldp port local-info Output Details 20-26
20-5 show lldp port remote-info Output Details 20-30
21-1 show dcb cn global Output Details 21-5
21-2 show dcb cn priority Output Details 21-7
21-3 show dcb cn port-priority Output Details 21-18
21-4 show dcb cn congestion-point Output Details 21-25
21-5 show dcb cn cp-mapping Output Details 21-28

21-6 show dcb cn profile Output Details 21-30
22-1 show probe detail Output Details 22-14
22-2 show probe sessions Output Details 22-17
26-1 show port advertise Output Details 26-9
26-2 show port counters Output Details 26-14
26-3 show port flow control Output Details 26-18
26-4 show port jumbo Output Details 26-21
26-5 Frame-Period Window Values 26-37
26-6 Symbol-Period Window Values 26-37
26-7 show port oam uld-config Output Details 26-41
26-8 show port status Output Details 26-49
27-1 show linkflap parameters Output Details 27-4
27-2 show linkflap metrics Output Details 27-4
29-1 show port broadcast Output Details 29-2
31-1 show lacp Output Details 31-2
32-1 show snmp user Output Details 32-3
32-2 show snmp group Output Details 32-7
32-3 show snmp access Output Details 32-12
33-1 show snmp view Output Details 33-2
34-1 show snmp targetparams Output Details 34-2
34-2 show snmp targetaddr Output Details 34-5
34-3 show snmp notify Output Details 34-9
34-4 show snmp engineid Output Details 34-17
34-5 show snmp counters Output Details 34-19
35-1 show spantree Output Details 35-4
35-2 Port-Specific show spantree stats Output Details 35-6
38-1 show spb port Output Display 38-7
38-2 show spb neighbors Output Details 38-10
39-1 show raas Output Display 39-2
40-1 show vlan Output Details 40-3
40-2 show vlan interface Output Details 40-10
40-3 show vlan constraint Output Details 40-15
41-1 show gvrp Output Details 41-2
41-2 show garp timer configuration Output Details 41-3
42-1 show mrp timer Output Details 42-2
42-2 show garp timer configuration Output Details 42-5
43-1 show policy profile Output Details 43-3
43-2 show policy rule Output Details 43-20
43-3 Valid Values for Policy Classification Rules 43-26
44-1 show logging all Output Details 44-3
44-2 show logging server Output Details 44-5
44-3 show logging application Output Details 44-11
44-4 Sample Mnemonic Values for Logging Applications 44-12
45-1 show cos port-type Output Details 45-4
46-1 show netstat Output Details 46-3
48-1 show rmon stats Output Details 48-3
48-2 show rmon alarm Output Details 48-10
48-3 show rmon event Output Details 48-13
48-4 show rmon topN Output Details 48-19
48-5 show rmon matrix Output Details 48-23
50-1 MEP Defect Definitions 50-22
50-2 show cfm default-md Output Display 50-38
50-3 show cfm md Output Display 50-39
50-4 show cfm md ma Output Display 50-41
50-5 show cfm md ma ma-comp Output Display 50-42
50-6 show cfm md ma mep Output Display 50-44

50-7 show cfm md ma mep ccm-errors Output Display 50-46
50-8 show cfm md ma mep linktrace Output Display 50-48
50-9 show cfm md ma mep-list Output Display 50-50
50-10 show cfm md ma mep remote-mep Output Display 50-52
50-11 show cfm md mip-ccm Output Display 50-54
50-12 show cfm stack-table Output Display 50-55
56-1 Show IPv6 Neighbors Output Display 56-15
58-1 show ip bgp vpn Output Details 58-22
58-2 show ip bgp vpn vrf Output Details 58-25
58-3 show ipv6 bgp vpn vrf Output Details 58-28
58-4 show ipv6 bgp vpn vrf Output Details 58-30
59-1 show arp Output Details 59-2
62-1 show igmp config Output Details 62-4
64-1 show ip pim bsr Output Details 64-22
64-2 show ip pim interface Output Details 64-24
64-3 show ip pim neighbor Output Details 64-28
64-4 show ip pim neighbor detail Output Details 64-29
64-5 show ip pim neighbor brief Output Details 64-30
64-6 show ip pim rp mapping Output Details 64-31
65-1 show ipv6 pim bsr Output Details 65-21
65-2 show ipv6 pim interface Output Details 65-23
65-3 show ipv6 pim neighbor Output Details 65-28
65-4 show ipv6 pim rp mapping Output Details 65-30
68-1 show ip nat info Output Display 68-29
68-2 show ipv6 nat info Output Display 68-30
69-1 show ip slb reals Output Display 69-17
69-2 show ip slb reals detail Output Details 69-18
69-3 show ipv6 slb reals Output Display 69-19
69-4 show ipv6 slb reals detail Output Details 69-21
70-1 show ip twcb caches Output Display 70-29
70-2 show ipv6 twcb caches Output Display 70-30
72-1 show ip bgp Output Details 72-72
72-2 show ip bgp peer Output Details 72-74
72-3 show ip bgp dampened-routes Output Details 72-75
72-4 show ipv6 bgp peer Output Details 72-80
73-1 show ip ospf database Output Details 73-45
73-2 show ip ospf interface Output Details 73-47
73-3 show ip ospf neighbor Output Details 73-49
73-4 show ip ospf sham-link Details 73-50
73-5 show ip ospf virtual links Output Details 73-51
74-1 show ip ospf sham-link Details 74-15
74-2 show ipv6 ospf database database-summary Output Details 74-47
74-3 show ipv6 ospf interface Output Details 74-49
74-4 show ipv6 ospf neighbor Output Details 74-51
74-5 show ipv6 ospf virtual links Output Details 74-52
77-1 show maclock Output Details 77-2
77-2 show maclock stations Output Details 77-3
78-1 show tacacs Output Details 78-2
81-1 ICMP Message Types 81-8
82-1 ICMP Message Types 82-8
85-1 show ip policy Output Details 85-3
86-1 show radius Output Details 86-2
86-2 show radius server verbose Output Details 86-3
88-1 show quarantine-agent Output Display 88-2
90-1 show pwa Output Details 90-3
91-1 show macauthentication Output Details 91-2

91-2 show macauthentication session Output Details 91-4
93-1 Radius-Snooping Settings 93-7
93-2 Radius-Snooping Port Settings 93-8
93-3 Radius-Snooping Flow Settings 93-9
93-4 Radius-Snooping Session Port Settings 93-11
93-5 Radius-Snooping Session MAC Settings 93-11
94-1 show auto-tracking Output Display 94-2
95-1 show antispoof class Output Display 95-8
95-2 show antispoof port Output Display 95-19
95-3 show antispoof port Output Display 95-22
95-4 show antispoof port Output Display 95-24

About This Guide

This manual explains how to access the device's Command Line Interface (CLI) and how to use it to configureExtreme Networks S-Series® switch/router devices.

Important Notice

Depending on the firmware version used in your Extreme Networks S-Series device, some features described in this document may not be supported. Refer to the Release Notes shipped with your Extreme Networks S-Series device to determine which features are supported.

Using This Guide

A general working knowledge of basic network operations and an understanding of CLI management applications is helpful before configuring the Extreme Networks S-Series device.

This manual describes how to do the following:

- Access the Extreme Networks S-Series CLI.
- Use CLI commands to perform network management and device configuration operations.
- Establish and manage Virtual Local Area Networks (VLANs).
- Manage static and dynamically-assigned user policies.
- Establish and manage priority classification.
- Configure IP routing and routing protocols, including RIP version 2, OSPF, DVMRP, and VRRP.
- Configure security protocols, including 802.1X and RADIUS, SSHv2, MAC locking, MAC authentication, multiple authentication, DoS attack prevention, and flow setup throttling.
- Configure policy-based routing.
- Configure access control lists (ACLs).

Related Documents

The manuals listed below can be obtained from the World Wide Web in Adobe Acrobat Portable Document Format (PDF) at the following site:

http://support.extremenetworks.com/

The *Extreme Networks S-Series Configuration Guide* provides information on how to configure the S-Series switch/router.

Conventions Used in This Guide

The following conventions are used in the text of this document:

Convention	Description
Bold font	Indicates mandatory keywords, parameters or keyboard keys.
italic font	Indicates complete document titles.
`Courier` font	Used for examples of information displayed on the screen.
`Courier` font in italics	Indicates a user-supplied value, either required or optional.
[ ]	Square brackets indicate an optional value.
{ }	Braces indicate required values. One or more values may be required.
|	A vertical bar indicates a choice in values.
[x | y | z]	Square brackets with a vertical bar indicates a choice of a value.
{x | y | z}	Braces with a vertical bar indicate a choice of a required value.
[x {y | z}]	A combination of square brackets with braces and vertical bars indicates a required choice of an optional value.

The following icons are used in this guide:

Note: Calls the reader's attention to any item of information that may be of special importance.

Router: Calls the reader's attention to router-specific commands and information.

CLI "Defaults" Descriptions

Each command description in this guide includes a section entitled "Defaults" which defines CLI behavior if the user enters a command without typing optional parameters (indicated by square brackets [ ]). For commands without optional parameters, the defaults section lists "None". For commands with optional parameters, this section describes how the CLI responds if the user opts to enter only the keywords of the command syntax.

CLI Command Modes

Each command description in this guide includes a section entitled "Command Mode" which states whether the command is executable in Admin (Super User), Read-Write or Read-Only mode. Users with Read-Only access will only be permitted to view Read-Only (**show**) commands. Users with Read-Write access will be able to modify all modifiable parameters in **set** and **show** commands, as well as view Read-Only commands. Administrators or Super Users will be allowed all Read-Write and Read-Only privileges, and will be able to modify local user accounts. The S-Series device indicates which mode a user is logged in as by displaying one of the following prompts:

- Super-User: S Chassis(su)->
- Read-Write: S Chassis(rw)->
- Read-Only: S Chassis(ro)->

Note: Depending on which S-Series device you are using, your default command prompt may be different than the examples shown.

Commonly Used Acronyms

The following acronyms are used extensively throughout this guide:

- IOM – Input/Output Module
- FM – Fabric Module
- CM – Control Module
- LED – Light Emitting Diode
- USB – Universal Serial Bus

Getting Help

For additional support related to the S-Series or this document, contact Extreme Networks using one of the following methods:

World Wide Web	http://support.extremenetworks.com/
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-603-952-5000 For the Extreme Networks Support toll-free number in your country: www.extremenetworks.com/support/contact/
Internet mail	support@extremenetworks.com To expedite your message, please type [**S-SERIES**] in the subject line.

Before contacting Extreme Networks for technical support, have the following data ready:

- Your Extreme Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (for example, changing mode switches or rebooting the unit)
- The serial and revision numbers of all involved Extreme Networks products in the network
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load and frame size at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any previous Return Material Authorization (RMA) numbers

1

CLI Properties Commands

This chapter provides detailed information for the CLI properties set of commands. For information about configuring CLI properties, refer to the "Using the CLI" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
set prompt	1-1
set cli completion	1-2
loop	1-2
show banner	1-3
set banner	1-4
clear banner	1-5
history	1-5
show history	1-6
set history	1-6
show version	1-7
show width	1-8
show length	1-8
set width	1-9
set length	1-9
show logout	1-10
set logout	1-10
cls (clear screen)	1-11
configure	1-11
exit | quit	1-12

set prompt

Use this command to modify the command prompt.

Syntax

set prompt *prompt-string*

Parameters

prompt-string	Specifies a text string for the command prompt. A prompt string containing a space in the text must be enclosed in quotes as shown in the example below.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the command prompt to Switch 1:

```
S Chassis(rw)->set prompt "Switch 1"
Switch 1(rw)->
```

set cli completion

Use this command to enable or disable the CLI command completion function. When enabled, this allows you to complete a unique CLI command fragment using the keyboard spacebar.

Syntax

set cli completion {**enable** | **disable**} [**default**]

Parameters

enable | **disable**	Enables or disables the CLI command completion function.
default	(Optional) Maintains this setting for all future sessions.

Defaults

If not specified, the status setting will not be maintained as the default.

Mode

All command modes.

Example

This example shows how to enable the CLI command completion function and maintain it as the default setting:

```
S Chassis(rw)->set cli completion enable default
```

loop

Use this command to execute a command loop.

Syntax

loop *count* [*delay*] [**-r**] [**-k**]

Parameters

count	Specifies the number of times to loop. A value of 0 will make the command loop forever.
delay	(Optional) Specifies the number of seconds to delay between executions.
-r	(Optional) Refreshes the cursor to the home position on the screen.
-k	(Optional) Loop continues if an error occurs.

Defaults

- If a *delay* is not specified, none will be set.
- If -r is not specified, the cursor will not refresh.

Mode

All command modes

Example

This example shows how to execute a command loop 10 times with a 30 second delay:

```
S Chassis(rw)->loop 10 30
```

show banner

Use this command to show the banner message that will display at pre- and post-session login.

Syntax

show banner {**login** | **motd**}

Parameters

login	Displays the pre-session login banner.
motd	Displays the post-session login message of the day.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the banner message of the day:

```
S Chassis(rw)->show banner motd
Not one hundred percent efficient, of course ... but nothing ever is.
                -- Kirk, "Metamorphosis", stardate 3219.8
```

set banner

Use this command to set the banner message for pre- and post-session login.

Syntax

set banner {**login** *message* **| motd** *message*}

Parameters

login *message*	Specifies a message displayed pre-session login. This is a text string that can be formatted with tabs (**\t**) and new line escape (**\n**) characters. The \t tabs will be converted into 8 spaces in the banner output.
motd *message*	Specifies a message of the day displayed post-session login. This is a text string that can be formatted with tabs (**\t**) and new line escape (**\n**) characters. The \t tabs will be converted into 8 spaces in the banner output.

Defaults

None.

Mode

All command modes.

Usage

Use the **\?** escape sequence when ending a banner with a question mark to avoid the question mark being treated as a help request.

A pre-session login banner will cause a prompt to display when logging on to the system requiring the user to verify y/n before the login will continue. For example if the banner login is "By proceeding with this login you are verifying that you are a member of the Extreme Networks documentation group and are authorized to use this system." The following will display prior to entering the login password:

```
By proceeding with this login you are verifying that you are a member of the
Extreme Networks documentation group and are authorized to use this system.

Proceed to login? (y/n) [n]?
```

Examples

This example shows how to set the post-session message of the day banner to read "Change is the price of survival.
-- Winston Churchill" :

```
S Chassis(rw)->set banner motd Change is the price of survival. \n\t--Winston
Churchill
```

This example shows how to set the pre-session login to read "There is nothing more important than our customers." :

```
S Chassis(rw)->set banner login There is nothing more important than our customers
```

clear banner

Use this command to clear the banner message displayed at pre- and post-session login to a blank string.

Syntax

```
clear banner {login | motd}
```

Parameters

login	Clears the pre-session login banner.
motd	Clears the post-session login message of the day.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear the post-session message of the day banner to a blank string:

```
S Chassis(rw)->clear banner motd
```

history

Use this command to display the contents of the command history buffer.

Syntax

```
history
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

The command history buffer includes all the switch commands entered up to a maximum of 100, as specified in the **set history** command (page 1-6).

Example

This example shows how to display the contents of the command history buffer. It shows there are four commands in the buffer:

```
S Chassis(rw)->history
 1 hist
 2 show gvrp
 3 show vlan
 4 show igmp
```

show history

Use this command to display the size (in lines) of the history buffer.

Syntax

show history

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the size of the history buffer:

```
S Chassis(rw)->show history
 History buffer size: 20
```

set history

Use this command to set the size of the history buffer.

Syntax

set history *size* [**default**]

Parameters

size	Specifies the size of the history buffer in lines. Valid values are **1** to **100**. Default: **20**.
default	(Optional) Makes this setting persist for all future sessions.

Defaults

If **default** is not specified, the history setting will not be persistent.

Mode

All command modes.

Example

This example shows how to set the size of the command history buffer to 25 lines and make this the default setting:

```
S Chassis(rw)->set history 25 default
```

show version

Use this command to display hardware and firmware information. Refer to the *Extreme Networks S-Series Configuration Guide* for instructions on how to download a firmware image.

Syntax

show version

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display version information:

```
S Chassis(su)->show version


Copyright (c) 2014 by Enterasys Networks, Inc.

Slot    Model             Serial #              Versions
------  ----------------  --------------------  -------------------------
1       SSA-T4068-0252    094454536352          Hw: 1
                                                Bp: 01.00.21x
                                                Fw: 07.11.01.0011
```

Table 1-1 provides an explanation of the command output.

Table 1-1 show version Output Details

Output...	What it displays...
Slot	Slot location designation. For details on how slots are numbered, refer to the *Extreme Networks S-Series Configuration Guide*.
Model	Device's model number.

Table 1-1 show version Output Details (continued)

Output...	What it displays...
Serial #	Device's serial number.
Versions	• **Hw**: Hardware version number. • **Bp**: BootPROM version. • **Fw**: Current firmware version number.

show width

Use this command to show the number of columns for the terminal connected to the device's console port.

Syntax

show width

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

```
S Chassis(su)->show width
Screen width currently set to: 80
```

show length

Use this command to show the current screen length.

Syntax

show length

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

```
S Chassis(su)->show length
Screen length currently set to: 0
```

set width

Use this command to set the number of columns for the terminal connected to the device's console port. The length of the CLI is set using the **set length** command as described in "set length" on page 1-9.

Syntax

set width *screenwidth* [**default**]

Parameters

screenwidth	Sets the number of terminal columns. Valid values are **50–200**.
default	Make this setting persist for all future sessions.

Defaults

None.

Mode

All command modes

Example

This example shows how to set the terminal columns to 100:

```
S Chassis(rw)->set width 100
```

set length

Use this command to set the number of lines the CLI will display.

Syntax

set length *screenlength* [**default**]

Parameters

screenlength	Sets the number of lines in the CLI display. Valid values are **0**, which disables the scrolling screen feature.
default	Make this setting persist for all future sessions.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the terminal length to 50:

```
S Chassis(rw)->set length 50
```

show logout

Use this command to display the time (in minutes) an idle console, SSH or Telnet CLI session will remain connected before being logged out.

Syntax

show logout

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the CLI logout setting:

```
S Chassis(rw)->show logout
Logout currently set to: 10 minutes.
```

set logout

Use this command to set the time (in minutes) an idle console, SSH or Telnet CLI session will remain connected before being logged out.

Syntax

set logout *timeout* [**default**]

Parameters

timeout	Sets the number of minutes for the idle-timeout timer. • If the security profile = C2, the default value is **15** • If the security profile = normal, the default value is **10**
default	Make this setting persist for all future sessions.

Defaults

None.

Mode

All command modes.

Usage

When *timeout* expires, the idle console, SSH or Telnet session will be terminated and logged out.

If *timeout* is set to **0**, logout is disabled.

Example

This example shows how to set the system timeout to 10 minutes:

```
S Chassis(rw)->set logout 10
```

cls (clear screen)

Use this command to clear the screen for the current CLI session.

Syntax

cls

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear the CLI screen:

```
S Chassis(rw)->cls
```

configure

Use this command to enter global configuration mode.

Syntax

configure

Parameters

None.

Defaults

None.

Mode

Switch command mode.

Example

This example shows how to enter global configuration mode:

```
S Chassis(rw)->configure
```

exit | quit

Use either of these commands to leave a CLI session.

Syntax

exit

quit

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

By default, device timeout occurs after 15 minutes of user inactivity, automatically closing your CLI session. Use the **set logout** command as described in "set logout" on page 1-10 to change this default.

When operating in any configuration mode, the **exit** command jumps to the next lower CLI command level. When operating in executive command mode, the **exit** command leaves a CLI session.

Example

This example shows how to exit a CLI session:

```
S Chassis(rw)->exit
```

2

Line Editor Commands

This chapter provides detailed information for the line editor set of commands. The command line editor determines which key sequences can be used in the CLI. Example: Ctrl+A will move the cursor to the beginning of the command line when in Emacs mode. The CLI supports both vi- and Emacs-like line editing commands. By default, the "default" line-editing mode is configured, with no special key sequences. Table 2-1 lists some commonly used Emacs and vi commands. Use the **set line-editor** command ("set line-editor" on page 2-3) to change the line-editor mode. For information about configuring the line editor, refer to the "Using the CLI" chapter of the *Extreme Networks S-Series Configuration Guide*.

Table 2-1 Basic Line Editing Emacs & vi Commands

Key Sequence	Emacs Command
Ctrl+A	Move cursor to beginning of line.
Ctrl+B	Move cursor back one character.
Ctrl+C	Abort command.
Ctrl+D	Delete a character.
Ctrl+E	Move cursor to end of line.
Ctrl+F	Move cursor forward one character.
Ctrl+H	Delete character to left of cursor.
Ctrl+I or TAB	Complete word.
Ctrl+K	Delete all characters after cursor.
Ctrl+L or Ctrl+R	Re-display line.
Ctrl+N	Scroll to next command in command history (use the CLI **history** command to display the history).
Ctrl+P	Scroll to previous command in command history.
Ctr1+Q	Resume the CLI process.
Ctr1+S	Pause the CLI process (for scrolling).
Ctrl+T	Transpose characters.
Ctrl+U or Ctrl+X	Delete all characters before cursor.
Ctrl+W	Delete word to the left of cursor.
Ctrl+Y	Restore the most recently deleted item.
h	Move left one character.
l	Move right one character.

Table 2-1 Basic Line Editing Emacs & vi Commands (continued)

Key Sequence	Emacs Command
k	Get previous shell command in history.
j	Get next shell command in history.
$	Go to end of line.
0	Go to beginning of line.
a	Append.
A	Append at end of line.
c SPACE	Change character.
cl	Change character.
cw	Change word.
cc	Change entire line.
c$	Change everything from cursor to end of line.
i	Insert.
I	Insert at beginning of line.
R	Type over characters.
*n*r*c*	Replace the following *n* characters with *c*.
*n*x	Delete *n* characters starting at cursor.
*n*X	Delete *n* characters to the left of the cursor.
d SPACE	Delete character.
dl	Delete character.
dw	Delete word.
dd	Delete entire line.
d$	Delete everything from cursor to end of line.
D	Same as “d$”.
p	Put last deletion after the cursor.
P	Put last deletion before the cursor.
u	Undo last command.
~	Toggle case, lower to upper or vice versa.

For information about...	Refer to page...
show line-editor	2-3
set line-editor	2-3

show line-editor

Use this command to show current and default line-editor mode and Delete character mode.

Syntax

show line-editor

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to view the current and default line-editor mode and Delete mode:

```
S Chassis(su)->show line-editor
Current Line-Editor mode is set to: Default
Default Line-Editor mode is set to: Default

Current DEL mode is set to: backspace
System DEL mode is set to: backspace
```

set line-editor

Use this command to set the current and default line editing mode or the way the Delete character is treated by the line editor. You can also set the persistence of your line editing selections.

Syntax

set line-editor {**emacs** | **vi** | **default** | **delete** {**backspace | delete**}} [**default**]

Parameters

emacs	Selects emacs command line editing mode. See Table 2-1 for some commonly used emacs commands.
vi	Selects vi command line editing mode.
default	Selects default line editing mode.
delete {**backspace** | **delete**}	Sets the way the line editor treats the Delete ASCII character. **delete backspace** — The line editor will treat Delete (0x7f) as a Backspace (0x08) character. **delete delete** — The line editor will treat Delete as the Delete character (the default condition).
default	(Optional) Make the line editor or Delete mode setting persist for all future sessions.

Defaults

If **default** is not entered after selecting a line editing or Delete mode, the selection will apply only to the current session and will not persist for future sessions.

Mode

All command modes.

Examples

This example sets the current line-editor to vi mode:

```
S Chassis(rw)->set line-editor vi
```

This example sets the default line-editor to emacs mode and sets the selection to persist for future sessions:

```
S Chassis(rw)->set line-editor emacs default
```

3

User Management Commands

This chapter provides detailed information for the user management set of commands. User management functionality includes how to set user accounts and passwords, the authentication login method, and WebView. For information about configuring user management, refer to the "System Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
Setting User Accounts and Passwords	3-1
Setting the Authentication Login Method	3-22
Setting WebView	3-24

Setting User Accounts and Passwords

This section provides command details for:

- Configuring system login and system password
- Configuring system lockout settings
- Configuring security mode

Commands

For information about...	Refer to page...
show system login	3-2
set system login	3-5
clear system login	3-6
show security boot-access	3-7
set security boot-access	3-7
clear security boot-access	3-8
show security fips mode	3-8
set security fips mode	3-9
clear security fips mode	3-9
show security profile	3-10
set security profile	3-10

For information about...	Refer to page...
clear security profile	3-11
set password	3-12
show system password	3-13
set system password	3-15
clear system password	3-18
show system lockout	3-19
set system lockout	3-20
clear system lockout	3-22

show system login

Use this command to display user login account information.

Syntax

show system login [**-verbose**]

Parameters

-verbose	(Optional) When specified, a verbose level of information displays for each user account.

Defaults

If -verbose is not specified, a standard level of information displays.

Mode

All command modes.

Examples

This example shows how to display login account information. In this case, device defaults are user names **admin**, **ro,** and **rw** and have not been changed; **911** is an administratively configured user account:

```
S Chassis(su)->show system login
Username        Access      State     Local  Login Access Allowed
                                      Only?  Start  End    Days
911             super-user  enabled   yes    ***access always allowed***
admin           super-user  enabled   no     ***access always allowed***
ro              read-only   enabled   no     ***access always allowed***
rw              read-write  enabled   no     ***access always allowed***
S Chassis(su)->
```

This example shows a verbose level of information for this system login configuration:

```
S Chassis(su)->show system login -verbose
Username: 911
---------
   Access                    : super-user
   State                     : enabled
   Local                     : yes
   Login start time          : any
   Login end time            : any
   Allowed login days        : any
   Simultaneous logins       : no limit
   Password aging            : using system password aging
   Password timestamp        : TUE MAY 03 07:43:53 2011
   Last login timestamp      : WED JUN 15 08:29:37 2011
   Failed logins             : 0
   Lockout started           : None
   Logins during grace period: 0

Username: admin
---------
   Access                    : super-user
   State                     : enabled
   Local                     : no
   Login start time          : any
   Login end time            : any
   Allowed login days        : any
   Simultaneous logins       : no limit
   Password aging            : using system password aging
   Password timestamp        : TUE MAY 03 06:23:46 2011
   Last login timestamp      : TUE JUN 14 09:48:39 2011
   Failed logins             : 0
   Lockout started           : None
   Logins during grace period: 0

Username: ro
---------
   Access                    : read-only
   State                     : disabled
   Local                     : no
   Login start time          : any
   Login end time            : any
   Allowed login days        : any
   Simultaneous logins       : no limit
   Password aging            : using system password aging
```

```
   Password timestamp        : None
   Last login timestamp      : None
   Failed logins             : 0
   Lockout started           : None
   Logins during grace period: 0

Username: rw
---------
   Access                    : read-write
   State                     : disabled
   Local                     : no
   Login start time          : any
   Login end time            : any
   Allowed login days        : any
   Simultaneous logins       : no limit
   Password aging            : using system password aging
   Password timestamp        : None
   Last login timestamp      : None
   Failed logins             : 0
   Lockout started           : None
   Logins during grace period: 0
S Chassis(su)->
```

Table 3-1 provides an explanation of the command output.

Table 3-1 show system login Output Details

Output...	What it displays...
Username	Login user names.
Access	Access assigned to this user account: **super-user**, **read-write** or **read-only**.
State	Whether this user account is **enabled** or **disabled**.
Local Only? | Local	Specifies authentication scope for this user. • **yes** — Specifies that authentication is only by way of the local user database even with RADIUS or TACACS+ configured. • **no** — Specifies that authentication is via configured methods.
Login Start | Login start time	Specifies the time at which access begins for this user.
Access End | Login end time	Specifies the time at which access ends for this user.
Allowed Days | Allowed login days	Specifies the time periods by start and end in 24 hour time and the days of the week for which access is allowed, or states that access is always allowed.
Simultaneous logins	Specifies the current number of simultaneous logins for this user.
Password aging	Specifies the current password aging setting for this user.
Password timestamp	Specifies the start date of the current password for this user.
Last login timestamp	Specifies the date and time this user last logged into the system.

Table 3-1 show system login Output Details (continued)

Output...	What it displays...
Failed logins	Specifies the number of times this user failed a login attempt.
Lockout started	Specifies if this this user is currently locked out.
Logins during grace period	Specifies the number of times this user has logged in during the grace period after this password has aged out.

set system login

Use this command to create a new user login account, or to disable or enable an existing account. The S-Series device supports up to 16 user accounts, including the admin account, which cannot be disabled or deleted.

Syntax

set system login *username* [**read-write** | **read-only** | **super-user**] [**enable** | **disable**] [**password** {*password* | **aging** {*days* | **disable** | **system**}] [**allowed-interval** {*HH:MM HH:MM*}] [**allowed-days** {[**Sun**] [**Mon**] [**Tue**] [**Wed**] [**Thu**] [**Fri**] [**Sat**]}] [**simultaneous-logins** *num*] [**local-only** {**yes | no**}]

Parameters

username	Specifies a login name for a new or existing user. This string can be a maximum of 80 characters, although a maximum of 16 characters is recommended for proper viewing in the **show system login** display.
read-write | **read-only** | **super-user**	Specifies the access privileges for this user.
enable | **disable**	Enables or disables the user account. The default admin (**su**) account cannot be disabled.
password *password*	(Optional) Specifies the encrypted password for this user account. This option is intended only for use in configurations generated by the **show config** command.
password aging *days* | **disable** | **system**	(Optional) Specifies password aging setting as: • *days* – The number of days to age the password. Valid values are **1** - **365**. • **disable** – Aging is disabled for this password. • **system** – The system password aging setting is used (default).
allowed-interval *HH:MM HH:MM*	(Optional) Specifies the start and end hour *HH* and minute *MM* time period for which access will be allowed for this user based upon 24 hour time.
allowed-days	(Optional) Specifies at least 1 and up to 7 days of the week for which access will be allowed for this user.

simultaneous-logins *num*	(Optional) Specifies the Number of simultaneous sessions allowed for the specified user account. Valid values are **0** - **5**. Default value is **0** (no limit).
local-only	(Optional) Specifies the authentication scope for this user. Valid values: **yes**, **no**. **yes** specifies that authentication is only by way of the local user database even with RADIUS or TACACS+ configured. **no** specifies that authentication is by way of configured methods.

Defaults

- **allowed-interval**: 00:00-24:00 (all hours allowed)
- **allowed-days**: Sun, Mon, Tue, Wed, Thu, Fri, Sat (all days allowed)
- **local-only**: no
- **password aging**: system

Mode

All command modes, Super User.

Usage

Allowed interval and allowed days may be configured on any user account but are not enforced on super-user accounts.

Example

This example shows how to enable a new user account with the login name **netops** with super user access privileges:

```
S Chassis(su)->set system login netops super-user enable
```

clear system login

Use this command to remove a local login user account or to reset a specified option to its default value.

Syntax

clear system login *username* [**allowed-interval**] [**allowed-days**] [**password** [**aging**]] [**simultaneous-logins**] [**local-only**]

Parameters

username	Specifies the login name of the account to be cleared if no optional parameters are specified. If an optional parameter(s) is specified, the account is not cleared and the specified parameter(s) is reset to the default value. The default admin (su) account cannot be deleted.
allowed-interval	(Optional) When specified, the configured allowed interval setting is reset to the default value.
allowed-days	(Optional) When specified, the configured allowed days setting is reset to the default value.
password	(Optional) When specified, the configured system password is deleted.

password aging	(Optional) When specified, password aging is reset to the default value of **system**.
simultaneous-logins	(Optional) When specified, the simultaneous logins setting is set to **0** (no limit).
local-only	(Optional) When specified, the configured local only setting is reset to the default value.

Defaults

The account is removed if no optional parameters are entered.

Mode

All command modes, Super User.

Example

This example shows how to remove the “netops” user account:

```
S Chassis(su)->clear system login netops
```

show security boot-access

Use this command to display the current boot access state for this device.

Syntax

show security boot-access

Parameters

None.

Defaults

None.

Mode

All command modes, Super User.

Example

This example shows how to display the security boot access state for this device:

```
S Chassis(su)->show security boot-access
Current boot menu access state  : enabled
S Chassis(su)->
```

set security boot-access

Use this command to enable or disable access to the boot menu during bootup.

Syntax

set security boot-access {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables access to the boot menu during bootup. The default value is **enable**.

Defaults

None.

Mode

All command modes, Super User.

Example

This example shows how to disable access to the boot menu during bootup for this device:

```
S Chassis(su)->set security boot-access disable
```

clear security boot-access

Use this command to reset access to the boot menu during bootup to the default state.

Syntax

clear security boot-access

Parameters

None.

Defaults

None.

Mode

All command modes, Super User.

Example

This example shows how to reset access to the boot menu during bootup to the default value of enabled for this device:

```
S Chassis(su)->clear security boot-access
```

show security fips mode

Use this command to display the current security FIPS mode state for this device.

Syntax

show security fips mode

Parameters

None.

Defaults

None.

Mode

All command modes, Super User.

Example

This example shows how to display the security FIPS mode for this device:

```
S Chassis(su)->show security fips mode
Current fips mode               : enabled
S Chassis(su)->
```

set security fips mode

Use this command to enable or disable FIPS mode on the device.

Syntax

set security fips mode {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables FIPS mode on the device. The default value is **disable**.

Defaults

None.

Mode

All command modes, Super User.

Usage

This command puts the switch into Federal Information Processing Standards (FIPS) mode. FIPS mode is a mode where only FIPS approved authentication and encryption algorithms and methods are used.

Example

This example shows how to enable FIPS mode for this device:

```
S Chassis(su)->set security fips mode enable
This command will reset the system.  Are you sure you want to continue? (y/n) [n]?n
```

clear security fips mode

Use this command to reset FIPS mode state to the default value on the device.

Syntax

clear security fips mode

Parameters

None.

Defaults

None.

Mode

All command modes, Super User.

Usage

This command resets FIPS mode to the default behavior of disabled on the device.

Example

This example shows how to reset FIPS mode to the default state of disabled for this device:

```
S Chassis(su)->clear security fips mode
```

show security profile

Use this command to display the current security profile for this device.

Syntax

show security profile

Parameters

None.

Defaults

None.

Mode

All command modes, Super User.

Example

This example shows how to display the security profile for this device:

```
S Chassis(su)->show security profile
Current security profile setting: c2
S Chassis(su)->
```

set security profile

Use this command to set the device's security profile.

Syntax

set security profile {**c2** | **normal**}

Parameters

c2	Specifies that the security profile is set to be optimized for Command and Control environments.
normal	Specifies that the security profile is set for the default security settings (default).

Defaults

None.

Mode

All command modes, Super User.

Usage

C2 security profile mode can affect the range, default, and access to certain commands. Individual command details specify any changes related to enabling C2 security profile mode.

Changing the security mode of the switch requires a system reset.

Example

This example shows how to set the security profile to **C2**:

```
S Chassis(su)->set security profile c2
This command will reset the system.  Are you sure you want to continue? (y/n) [n]?n
S Chassis(su)->
```

clear security profile

Use this command to reset the device security profile to the default value.

Syntax

clear security profile

Parameters

None.

Defaults

None.

Mode

All command modes, Super User.

Usage

This command resets the device security profile to the default value of normal. In normal mode, FIPS mode is disabled.

Changing the security mode of the switch requires a system reset.

Example

This example shows how to reset the security profile to the normal default mode:

```
S Chassis(su)->set security profile
```

set password

Use this command to change system default passwords or to set a new login password on the CLI.

Syntax

set password [*username*]

Parameters

username	(Only available to users with super-user access.) Specifies a system default or a user-configured login account name. By default, the Extreme Networks S-Series device provides the following account names: **ro** for Read-Only access, **rw** for Read-Write access. **admin** for Super User access. (This access level allows Read-Write access to all modifiable parameters, including user accounts).

Defaults

None.

Mode

All command modes. Read-Write users can change their own passwords. Super Users (Admin) can change any password on the system.

Usage

Only users with admin (**su**) access privileges can change any password on the system.

Users with Read-Write (**rw**) access privileges can change their own passwords, but cannot enter or modify other system passwords.

Passwords must be a minimum of 8 characters and a maximum of 40 characters.

If configured, password length must conform to the minimum number of characters set with the **set system password length** command ("set system password" on page 3-15).

The **admin** password can be reset by toggling DIP switch 8 on the device as described in your *I/O Module Hardware Installation Guide* or, if you a managing an SSA, in the SSA *Hardware Installation Guide.*

Examples

This example shows how a super-user would change the Read-Write password from the system default (blank string):

```
S Chassis(su)->set password rw
Please enter new password: ********
Please re-enter new password: ********
```

```
Password changed.
S Chassis(su)->
```

This example shows how a user with Read-Write access would change his password:

```
S Chassis(rw)->set password
Please enter old password: ********
Please enter new password: ********
Please re-enter new password: ********
Password changed.
S Chassis(rw)->
```

show system password

Use this command to display current password configuration settings.

Syntax

show system password

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display password configuration settings. In this case, the settings displayed are the default settings:

```
S Chassis(su)->show system password
Password history size  : 8
Password aging         : disabled
Password minimum length: 8
Password minimum character requirements:
   Uppercase: 0
   Lowercase: 0
     Numeric: 0
     Special: 0
Password assignment required at account creation               : no
Allow multiple accounts to share same password                 : yes
Length of substrings in previous password not allowed in new one: 0
Allow the same character to appear consecutively in a password  : yes
Times the same character may consecutively repeat in a password : no limit
Password may contain, repeat or reverse the user id            : yes
Require users to change password at first login                : no
```

```
Account access change at first login applied to                : non-superusers
Minimum interval between password changes                      : 1440 minutes
Account access change interval applied to                      : non-superusers
Number of days before password expiration to display warning   : 21 days
Number of logins allowed after password expiration             : 3
Grace period to allow logins after password expiration         : 30 days
```

Table 3-2 provides an explanation of the command output:

Table 3-2 show system password Output Details

Output...	What it displays...
Password history size	Number of previously used user login passwords that will be checked for duplication when the **set password** command is executed. Configured with **set system password history** (“set system password” on page 3-15).
Password aging	Number of days user passwords will remain valid before aging out. Configured with **set system password aging** (“set system password” on page 3-15).
Password minimum length	The minimum length user passwords.
Password minimum character requirements	The minimum number of uppercase letters, lowercase letters, numbers, and special characters required in a password.
Password assignment required at account creation	Whether password assignment is required when an account is created.
Allow multiple accounts to share same password	Whether multiple accounts can share the same password.
Length of substrings in the previous password not allowed in new password	The number of characters from the most previous password that cannot be used in the new password.
Allow the same character to appear consecutively in a password	Whether the same character can appear consecutively in a password.
Times the same character may consecutively repeat in a password	Whether the same character can consecutively repeat in a password.
Password may contain, repeat or reverse the user id	Whether the password contents can contain, repeat, or reverse the contents of the User ID.
Require users to change password at first login	Specifies whether users are required to change the password at first login. When set to yes the setting only applies to rw and ro user modes. If the all option is also configured, the setting applies to all user modes.
Account access change at first login applied to	User modes to which an account access change is applied at first login.
Minimum interval between password changes	Minimum interval, in minutes, between password changes by users.
Account access change interval applied to	The user modes the account access change interval is applied to.
Number of days before password expiration to display warning	The number of days before password expiration a warming displays that the password expiration is due.

Table 3-2 show system password Output Details (continued)

Output...	What it displays...
Number of logins allowed after password expiration	The number of grace logins allowed before user access information is cleared due to password expiration.
Grace period to allow logins after password expiration	The time in days a user is allowed to log into an account before the user access information is cleared due to password expiration.

set system password

Use this command to configure system password parameters.

Syntax

set system password [**aging** {*days* | **disable**}] [**history** {*size*}] [**length** *characters*] [**min-required-chars** {[**uppercase** *characters*] [**lowercase** *characters*] [**numeric** *characters*] [**special** *characters*]}][**require-at-creation** {**yes** | **no**}] [**allow-duplicates** {**yes** | **no**}] [**allow-user-id** {**yes** | **no**}] [**substring-match-len** *characters*] [**allow-repeating-chars** {*num* | **yes** | **no**}] [**change-first-login** {**yes** | **no**} [**all**]] [**change-frequency** *minutes* [**all**]] [**expire-warning** *days*] [**grace-period** {**logins** *num* | **time** *days*}]

Parameters

aging *days* | **disable**	Specifies the number of days to age the password. • *days* — Valid values are **1–365** • **disable** — Aging is not taken into account for user account passwords.
history *size*	Specifies the number of passwords to keep in the password history for a user account. Valid values: **0–10**. • If the security profile = C2, the default value is **8** entries • If the security profile = normal, the default value is **0** entries
length *characters*	Specifies the minimum number of characters in a user account password.
min-required-chars	Specifies the minimum number of characters of the specified type that must be present in a user account password as follows: • **uppercase** *characters* — minimum number of upper case characters • **lowercase** *characters* — minimum number of lower case characters • **numeric** *characters* — minimum number of numeric characters • **special** *characters* — minimum number of special characters Valid values: **0–40** in all cases.
require-at-creation	Specifies whether a password is required at the time of user account creation: • **yes** — Password is required when creating a user account • **no** — Password is not required when creating a user account

allow-duplicates	Specifies whether multiple accounts can share the same password: • **yes** — Specifies that multiple accounts may share the same password • **no** — Specifies that multiple accounts may not share the same password
allow-user-id	Allows the password to contain, repeat, or reverse the account name: • **yes** – Specifies that the contents of the password can contain, repeat, or reverse the content of the account name (default). • **no** – Specifies that the contents of the password can not contain, repeat, or reverse the content of the account name.
substring-match-len *characters*	Specifies the length of any substring present in the most previous password for this account that may not be used in a new password. Valid values: **0**–**40**. Default value is **4** characters.
allow-repeating-chars	Specifies whether the same character may appear consecutively in the same password: • *num* – Specifies the number of repeating characters allowed. Valid values are 0 - 40. • **yes** — specifies that the same character may appear consecutively in a password with no maximum character limit (default). • **no** — specifies that the same character may not appear consecutively in a password.
change-first-login	Specifies whether new users are required to change their password upon first login: • **yes** — specifies that new users must change the password for this account upon first login • **no** — specifies that new users are not required to change the password for this account upon first login • **all** – (Optional) specifies that this new setting is applied to all user modes; by default this setting only applies to read-write and read-only.
change-frequency *minutes* [**all**]	Specifies a minimum interval in minutes between password changes allowed for non-superusers. Valid values: **0**–**65535**. The **all** option specifies that this new setting is applied to all user modes; by default this setting only applies to read-write and read-only. • If the security profile = C2, the default value is **1440** (24 hours) • If the security profile = normal, the default value is **0**
expire-warning *days*	Specifies the number of days (1-28) before password expiration to display a warning of the impending expiration. Valid values are **1** - **28** days. Default value is **21** days.
grace-period logins *num* | **time** *days*	Sets a grace period in either the number of logins or days before the password is locked out: **logins** *num* – Number of logins after a password expires allowed before the password is locked out. Valid values are **0** - **5**. Default value is **3** for C2 security mode and **0** (no limit) for normal security mode. **time** *days* – Number of days after a password expires before the password is locked out. Valid values are **0** - **30** days. Default value is **30** days for C2 security mode and **0** (no limit) for normal security mode.

Defaults

- **aging**: disable
- **history**: normal mode: 0 passwords; C2 mode: 8
- **length**: 8 characters
- **min-required-chars**: 0 characters for all cases
- **require-at-creation**: No. Password is not required at user account creation.
- **allow-duplicates**: Yes. Multiple accounts may use the same password.
- **allow-user-id**: Yes.
- **substring-match-len**: 0 characters.
- **allow-repeating-chars**: Yes. Consecutive use of the same character in a password is allowed.
- **change-first-login**: No. The password does not have to be changed upon first login.
- **change-frequency**: 0 minutes.
- **expire-warning**: 21 days.
- **grace-period**: 3 logins or 30 days for C2 security mode; unlimited logins or days for normal security mode.

Mode

All command modes, Super User.

Usage

The set of special characters recognized by this command is: !@#$%^&*()-=[]\;?,./`.

If the **require-at-creation** option is enabled, the **set system login** command will interactively prompt for a cleartext password upon creation of a new user account. It will be as if a **set password** *username* command was implicitly executed. The new account will not be successfully created until a valid password has been specified. A cleartext password will not be solicited if an encrypted password is already specified by way of the **set system login** command's **password** option.

If the **allow-duplicates** option is set to **no**, a user will not be able to select as a new password one which is already being used by another user.

If a **substring-match-len** option is set to zero, no substring matching will be performed when validating new passwords. If the **substring-match-len** option is configured with a nonzero length, any substring of the specified length appearing in the current password for this user may not appear in a new password. If the configured **history** size is nonzero, then all historical passwords up to that size will also be compared with the input of the new password. Any substring of the configured length appearing in any of the historical passwords may not be used in the new password. This option is not enforced when a password is changed by a superuser.

A password **change-frequency** interval of zero means there is no restriction on the frequency of password changes.

A configured minimum **change-frequency** interval applies only to users without super-user privileges attempting to change their own passwords unless the **all** option is specified. Users with super-user privileges may change their passwords at any time if the **all** option is not specified.

Example

This example shows how to set the age of a system password for 60 days, the minimum length of the password to 6 and that the same character can not repeat consecutively in the same password:

```
S Chassis(su)->set system password age 60 length 6 allow-repeating-chars no
```

clear system password

Use this command to clear local login password parameters to default values.

Syntax

```
clear system password [aging] [history] [length] [min-required-chars {[uppercase]
[lowercase] [numeric] [special]}] [require-at-creation] [allow-duplicate]
[allow-user-id] [substring-match-len] [allow-repeating-chars]
[change-first-login] [change-frequency] [expire-warning] [grace-period]
```

Parameters

aging	Specifies that the number of days to age the password be reset to the default value.
history	Specifies that the number of passwords to keep in the password history for a user account be reset to the default value.
length	Specifies that the minimum number of characters that must be present in a user account password be reset to the default value.
min-required-chars	Specifies that the minimum number of characters of the specified type that must be present in a user account password be set to the default value: **uppercase, lowercase, numeric, special**.
require-at-creation	Specifies that the requirement that a password be configured at the time of user account creation be set to the default value.
allow-duplicates	Specifies that the option controlling whether multiple accounts can share the same password be set to the default value.
allow-user-id	Specifies that the password can contain, repeat, or reverse the account name.
substring-match-len	Specifies that the length of any substring present in a previous password(s) for this account that may not be used in a new password be set to the default value.
allow-repeating-chars	Specifies that the option controlling whether the same character may appear consecutively in the same password be set to the default value of repeating characters allowed.
change-first-login	Specifies that the option controlling whether new users are required to change their password upon first login be set to the default value.
change-frequency	Specifies that the minimum interval between password changes be set to the default value.
expire-warning	Specifies that a warning will be displayed 21 days before the password is due to expire.
grace-period	Specifies that no grace period exists and account access settings are cleared upon expiration of the password.

Defaults

If no options are specified, all options are reset to default values.

Mode

All command modes, Super User.

Example

This example shows how to reset the minimum system password length to the default number of characters:

```
S Chassis(su)->clear system password length
```

show system lockout

Use this command to display settings for locking out users.

Syntax

show system lockout

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display user lockout settings. In this case, device defaults have not been changed:

```
S Chassis(su)->show system lockout
Unsuccessful login attempts before lockout        : 3
Duration of lockout                               : 1 minutes
Lockout entire port upon failed logins            : disabled
Ports currently locked out due to failed logins   : none
Account access lockout duration applied to        : superusers
Period of inactivity before account lockout       : 90 days
Account access inactivity timer applied to        : non-superusers
Account assigned emergency-access from the console: admin
```

Table 3-3 provides an explanation of the command output. These settings are configured with "set system lockout" on page 3-20.

Table 3-3 show system lockout Output Details

Output...	What it displays...
Unsuccessful login attempts	Number of failed login attempts allowed before a read-write or read-only user's account will be disabled.
Duration of lockout	Number of minutes the default admin user account will be locked out after the maximum login attempts.
Lockout entire port upon failed logins	Current setting of the lockout port feature: enabled or disabled.
Ports currently locked out due to failed logins	Ports or none currently locked out due to failed logins
Account access lockout duration applied to	User mode the account access lockout duration is applied to.
Period of inactivity	Number of days of inactivity before a non-superuser account is locked out. Zero specifies no lockout will occur for inactivity.
Account access inactivity timer applied to	User mode account access inactivity timer is applied to or none.
Account assigned emergency-access from the console	Name of the account assigned emergency access from the console or none.

set system lockout

Use this command to set the number of failed login attempts before locking out (disabling) a read-write or read-only user account, the number of minutes to lockout the default admin super user account after maximum login attempts, and the number of inactive days before a non-superuser account is locked out.

Syntax

```
set system lockout {[attempts attempts] [time minutes [all]] [port {enable | disable] [inactive days [all]] [emergency-access]}
```

Parameters

attempts *attempts*	Specifies the number of failed login attempts allowed before a read-write or read-only user's account will be disabled. Valid values are: • If the security profile = C2, range is from **2 - 5** • If the security profile = normal, range is from **1** - **15**
time *minutes*	Specifies the number of minutes the default admin user account will be locked out after the maximum login attempts. Valid values are **0–65565**. • If the security profile = C2, the default value is **1** minute • If the security profile = normal, the default value is **15** minutes

port enable | **disable**	Specifies port type lockout behavior: • When enabled, if the number of failed logins, configured in **set system lockout attempts**, is exceeded for port types telnet, SSH, webView, or console, access for the offending port type will be locked out for the time specified in the **set system lockout time** configuration. • When disabled, no lockout occurs for port type failed attempts.
inactive *days*	Specifies the period of inactivity in days after which a non-superuser account will be locked out. Valid values are **0–65565**. • If the security profile = C2, the default value is **90** days • If the security profile = normal, the default value is **0**, accounts will not be locked out due to inactivity
all	(Optional) Specifies that the setting is to be applied to all user accounts including super-user.
emergency-access *user-name*	Specifies the user name of an account with super-user privileges that is always available through the console.

Defaults

- **attempts**: 3
- **time**: normal mode: 15 minutes; C2 mode 60 minutes
- **inactive**: normal mode: 0 days; C2 mode 90 days

Mode

All command modes, Super User.

Usage

A disabled account can only be restored administratively using an account with super-user privileges. A locked out account will be accessible after a period of time has passed.

An inactivity timer value of zero means that no account will be locked out due to inactivity.

Once a user account is disabled, it can only be re-enabled by a super user with the **set system login** command (“set system login” on page 3-5).

The **admin** user is set to emergency access by default. Emergency access can only be applied to a user with super-user privileges. Except for port lockout, all other lockout behaviors are not applied to a super-user account set for emergency access, when that user is accessing the device from the console. In the case of a port being lockedout, all users are denied access to the port until the lockout expires.

Example

This example shows how to set login attempts to 5 and lockout time to 30 minutes and the inactivity timer to 60 days:

```
S Chassis(su)->set system lockout attempts 5 time 30 inactive 60
```

clear system lockout

Use this command to reset system lockout parameters to default values.

Syntax

```
clear system lockout [attempts] [time] [inactive]
```

Parameters

attempts	Resets the number of failed login attempts allowed before a read-write or read-only user's account will be disabled to the default value of **3**.
time	Resets the number of minutes the default admin user account will be locked out after the maximum login attempts to the default value of **15** minutes.
inactive	Resets the period of inactivity in days after which a non-superuser account will be locked out to the default value of 0 days.

Defaults

If no option is specified, all lockout parameters are reset to default values:

- **attempts**: 3
- **time**: 15 minutes
- **inactive**: 0 days

Mode

All command modes, Super User.

Example

This example shows how to reset login attempts, lockout time and the inactivity timer to default values:

```
S Chassis(su)->clear system lockout attempts time inactive
```

Setting the Authentication Login Method

This section provides command details for setting and clearing authentication login.

For information about...	Refer to page...
show authentication login	3-22
set authentication login	3-23
clear authentication login	3-24

show authentication login

Use this command to display the current authentication login method.

Syntax

```
show authentication login
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the current authentication login method:

```
S Chassis(rw)->show authentication login
Current authentication login is any
```

set authentication login

Use this command to set the authentication login method.

Syntax

set authentication login {**any** | **local** | **radius** | **tacacs**}

Parameters

any	Specifies that the authentication protocol will be selected using the following precedence order: • TACACS+ • RADIUS • Local
local	Specifies that the local network password settings will be used for authentication login.
radius	Specifies that RADIUS will be used for authentication login.
tacacs	Specifies that TACACS+ will be used for authentication login.

Defaults

None.

Mode

All command modes.

Usage

If C2 security mode is enabled, You can not create, modify, or delete an authentication login configuration while in Read-Write user mode.

Example

This example shows how to set the authentication login method to use the local password settings:

```
S Chassis(rw)->set authentication login local
```

clear authentication login

Use this command to reset the authentication login method to the default setting of “any”.

Syntax

clear authentication login

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

If C2 security mode is enabled, You can not reset an authentication login configuration while in Read-Write user mode.

Example

This example shows how to reset the authentication login method:

```
S Chassis(rw)->clear authentication login
```

Setting WebView

This section provides details for enabling and disabling WebView, as well as setting the WebView port.

For information about...	Refer to page...
show webview	3-24
set webview	3-25
set webview port	3-25

show webview

Use this command to display WebView status.

Syntax

show webview

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows that WebView is enabled on TCP port 80, the default port number.

```
S Chassis(rw)->show webview
```

WebView is Enabled. Configured listen port is 80.

set webview

Use this command to enable or disable WebView.

Syntax

set webview {**enable** | **disable**}

Parameters

enable | **disable**	Enable or disable WebView.

Defaults

None.

Mode

All command modes.

Example

This example shows how to enable WebView.

```
S Chassis(rw)->set webview enable
```

set webview port

Use this command to change the TCP port for WebView.

Syntax

set webview port *port*

Parameters

port	TCP port on which to run WebView. Valid values are **1–65565**.

Defaults

Default port is 80.

Mode

All command modes.

Example

This example shows how to set the WebView TCP port to 100.

```
S Chassis(rw)->set webview port 100
```

4

Internet Protocol Security (IPsec) Commands

This chapter describes the Internet Protocol Security (IPsec) and Internet Key Exchange (IKE) set of commands and how to use them. For information about configuring IPsec, refer to the "IPsec Protocol Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
IPsec Commands	4-1
IKE Proposal Commands	4-4
IKE Policy Commands	4-8
IKE Map Commands	4-14
Show Commands	4-22

IPsec Commands

This section details the commands required to enable IPsec on the router, enable traps, and to configure a default IPsec instance.

For information about...	Refer to page...
crypto ipsec enable	4-1
crypto ipsec default	4-2
crypto ipsec trap-enable	4-3
ike map	4-3

crypto ipsec enable

Use this command to enable IPsec on the router.

Syntax

```
crypto ipsec enable
no crypto ipsec enable
```

Parameters

None.

Defaults

None.

Mode

Global VRF router configuration.

Usage

IPsec must be enabled on the global VRF router in order for IPsec to run on the router. Enable IPsec on the Global VRF router using the **crypto ipsec enable** command.

Example

This example shows how to enable IPsec on the global VRF router:

```
S Chassis(su-config)->crypto IPsec enable
S Chassis(su-config)->
```

crypto ipsec default

Use this command to enter the IPsec default instance configuration mode.

Syntax

crypto ipsec default

no crypto ipsec default

Parameters

None.

Defaults

None.

Mode

Global VRF router configuration.

Usage

Use this command to enter the IPsec default instance configuration mode. Within the the IPsec default instance configuration mode, an IKE map pointing to all IKE configuration including IKE proposal, policy, and map configuration is associated with the IPsec default instance using “ike map” on page 4-3. The IPsec default instance is the only supported IPsec instance for this release.

Example

This example shows how to enter configuration mode for the IPsec default instance:

```
S Chassis(su-config)->crypto ipsec default
```

```
S Chassis(su-crypto-ipsec-defaul)->
```

crypto ipsec trap-enable

Use this command to enable IPsec traps.

Syntax

crypto ipsec trap-enable

no crypto ipsec trap-enable

Parameters

None.

Defaults

None.

Mode

Global VRF router configuration.

Usage

IPsec traps are disabled by default.

Use the “no” option for this command to disable IPsec traps for this device.

Example

This example shows how to enable IPsec traps on this device:

```
S Chassis(su-config)->crypto ipsec trap-enable
S Chassis(su-config)->
```

ike map

Use this command to assign an IKE map to the IPsec default instance.

Syntax

ike map *ike-map*

no ike map *ike-map*

Parameters

ike-map	Specifies the IKE map to assign to the IPsec default instance. Valid value is up to 32 alpha-numeric characters plus special characters dash (**-**) and underscore (_).

Defaults

None.

Mode

IPsec default instance configuration.

Usage

IKE maps are configured in IKE map configuration mode entered using "crypto ike-map" on page 4-14.

Example

This example shows how to assign the winRadius IKE map to the IPsec default instance:

```
S Chassis(su-config)->crypto ipsec default
S Chassis(su-crypto-ipsec-defaul)->ike map winRadius
S Chassis(su-crypto-ipsec-defaul)->
```

IKE Proposal Commands

This section details commands for entering IKE proposal configuration mode for the specified proposal and the configuration of that proposal.

For information about...	Refer to page...
crypto ike-proposal	4-4
dh_group	4-5
encryption	4-6
hash	4-7
integrity	4-7

crypto ike-proposal

Use this command to create or modify an IKE proposal and enter IKE proposal configuration mode.

Syntax

crypto ike-proposal *proposal-identifier*

no crypto ike-proposal *proposal-identifier*

Parameters

proposal-identifier	Specifies the IKE proposal to create or modify. Valid value is up to 32 alpha-numeric characters plus special characters dash (-) and underscore (_).

Defaults

None.

Mode

Global VRF router configuration.

Usage

There are two types of IKE proposals:

- The main mode or key exchange proposal that is assigned to an IKE map
- The quick mode or data protection proposal that is assigned to an IKE policy

Main mode is the IKE negotiation that establishes a secure channel, known as the Internet Security Association and Key Management Protocol (ISAKMP) Security Association (SA), between two devices.

Quick mode negotiates on behalf of the IPsec SAs. During Quick mode, keying material is refreshed or, if necessary, new keys are generated.

The same proposal can be assigned to both the main and quick mode or they can be different proposals depending upon your needs.

Use this command to name the proposal and enter the configuration mode that provides the commands required to configure the proposal.

Use the "no" option for this command to delete the specified IKE proposal.

Example

This example shows how to enter configuration mode for the **winRadius_main** IKE proposal:

```
S Chassis(su-config)->crypto ike-proposal winRadius_main
S Chassis(su-crypto-proposal)->
```

dh_group

Use this command to configure the IKE Diffie-Hellman (DH) key exchange group for the IKE proposal .

Syntax

dh_group {**1** | **2** | **14**}

no dh_group {**1** | **2** | **14**}

Parameters

1	Specifies DH group 1 (modp768).
2	Specifies DH group 2 (modp1024).
14	Specifies DH group 14 (modp2048).

Defaults

None.

Mode

IKE proposal configuration.

Usage

IKE uses the Diffie-Hellman key derivation algorithm to generate IPsec SA keys. The difference between the DH 1, 2, and 14 algorithms is the size of the generated key:

- **1** – 768 bit key

- **2** – 1024 bit key
- **14** – 2048 bit key

The larger the generated key, the greater the security, but also the greater the system overhead. This release does not support a default DH group. You must manually configure a DH group.

Use the “no” option for this command to remove the IKE proposal DH group configuration.

Example

This example shows how to configure the winRadius_main proposal for DH group 14:

```
S Chassis(su-config)->crypto ike-proposal winRadius_main
S Chassis(su-crypto-proposal)->dh_group 14
S Chassis(su-crypto-proposal)->
```

encryption

Use this command to configure the encryption algorithm for the IKE proposal.

Syntax

encryption {**3des** | **aes128cbc** | **aes192cbc** | **aes256cbc**}

no encryption {**3des** | **aes128cbc** | **aes192cbc** | **aes256cbc**}

Parameters

3des	Specifies the Triple Data Encryption Standard encryption algorithm.
aes128cbc	Specifies the Advanced Encryption Standard (AES) 128 bit key size Cipher-Block Chaining (CBC) encryption algorithm.
aes192cbc	Specifies the Advanced Encryption Standard (AES) 192 bit key size Cipher-Block Chaining (CBC) encryption algorithm.
aes256cbc	Specifies the Advanced Encryption Standard (AES) 1256 bit key size Cipher-Block Chaining (CBC) encryption algorithm.

Defaults

None.

Mode

IKE proposal configuration.

Usage

This release does not support a default encryption algorithm. You must manually enter an encryption algorithm.

Use the “no” option for this command to remove the IKE proposal encryption configuration.

Example

This example shows how to configure the **winRadius_main** proposal for the **aes128cbc** encryption method:

```
S Chassis(su-config)->crypto ike-proposal winRadius_main
S Chassis(su-crypto-proposal)->encryption aes128cbc
```

```
S Chassis(su-crypto-proposal)->
```

hash

Use this command to configure the hash algorithm for the IKE proposal.

Syntax

hash sha1

no hash sha1

Parameters

sha1	Specifies the Secure Hash Algorithm 1 (SHA1) hash algorithm.

Defaults

None.

Mode

IKE proposal configuration.

Usage

The hash algorithm is used during phase 1 negotiation between the SA authenticating devices. This release does not support a hash default value. You must manually enter the hash algorithm for one to be configured.

Use the “no” option for this command to remove the IKE proposal hash configuration.

Example

This example shows how to configure the **winRadius_main** proposal for the **sha1** hash algorithm:

```
S Chassis(su-config)->crypto ike-proposal winRadius_main
S Chassis(su-crypto-proposal)->hash sha1
S Chassis(su-crypto-proposal)->
```

integrity

Use this command to configure the integrity (data authentication) algorithm for the IKE proposal.

Syntax

integrity sha1

no integrity sha1

Parameters

sha1	Specifies the SHA1 integrity algorithm.

Defaults

None.

Mode

IKE proposal configuration.

Usage

Integrity (data authentication) verifies that the data has not been altered as opposed to a user authentication which verifies the identity of the user.

SHA1 produces a 160-bit message digest for which no known attacks or partial attacks have yet been demonstrated.

This release does not support a default integrity algorithm. You must manually enter the integrity algorithm for one to be configured.

Use the "no" option for this command to remove the IKE proposal integrity configuration.

Example

This example shows how to configure the winRadius_main proposal for the **sha1** integrity method:

```
S Chassis(su-config)->crypto ike-proposal winRadius_main
S Chassis(su-crypto-proposal)->integrity sha1
S Chassis(su-crypto-proposal)->
```

IKE Policy Commands

This section details commands for entering IKE policy configuration mode for the specified policy and the configuration of that policy.

For information about...	Refer to page...
crypto ike-policy	4-8
authentication psk	4-9
initial-contact	4-10
lifetime time	4-10
passive	4-11
peer	4-12
proposal	4-12
version	4-13

crypto ike-policy

Use this command to create or modify an IKE policy and enter IKE policy configuration mode.

Syntax

crypto ike-policy *policy-identifier*

no crypto ike-policy *policy-identifier*

Parameters

policy-identifier	Specifies the IKE policy to create or modify. Valid value is up to 32 alpha-numeric characters plus special characters dash (-) and underscore (_).

Defaults

None.

Mode

Global VRF router configuration.

Usage

Use the “no” option for this command to delete the specified IKE policy.

Example

This example shows how to enter IKE policy command mode for the winRadius IKE policy:

```
S Chassis(su-config)->crypto ike-policy winRadius
S Chassis(su-crypto-policy)->
```

authentication psk

Use this command to configure the authentication pre-shared key (PSK) for the IKE policy.

Syntax

authentication psk *pre-shared-key*

no authentication psk *pre-shared-key*

Parameters

pre-shared-key	Specifies the PSK for this IKE policy. Valid value is up to 32 alpha-numeric characters plus special characters dash (-) and underscore (_).

Defaults

None.

Mode

IKE policy configuration.

Usage

The authentication PSK is a pre-shared authentication key that is used to initiate the connection and exchange encryption keys during the session.

Use the “no” option for this command to remove the specified IKE policy PSK configuration.

Example

This example shows how to configure the winRadius IKE policy for an authentication PSK of **testkey**:

```
S Chassis(su-config)->crypto ike-policy winRadius
S Chassis(su-crypto-policy)->authentication psk testkey
S Chassis(su-crypto-policy)->
```

initial-contact

Use this command to enable the initial contact feature for the IKE policy.

Syntax

initial-contact

no initial-contact

Parameters

None.

Defaults

None.

Mode

IKE policy configuration.

Usage

If the local host has rebooted, peers may have SAs that are no longer valid. If the initial contact feature is enabled, upon reboot an initial contact message is sent to a peer so that it will delete old SAs.

Use the “no” option for this command to disable the initial contact feature for the IKE policy.

Example

This example shows how to enable the initial contact feature for the winRadius IKE policy:

```
S Chassis(su-config)->crypto ike-policy winRadius
S Chassis(su-crypto-policy)->initial-contact
S Chassis(su-crypto-policy)->
```

lifetime time

Use this command to configure the lifetime for the IKE policy.

Syntax

lifetime time *minutes*

no lifetime time *minutes*

Parameters

minutes	Specifies the number of minutes before the IKE policy times out. Valid values are 1 - 2879 minutes.

Defaults

None.

Mode

IKE policy configuration.

Usage

The lifetime time configuration specifies the life cycle of an SA and is configured in minutes. The policy lifetime determines when a policy times out. A lifetime renegotiation automatically occurs before the lifetime is to expire. If the renegotiation is unsuccessful, the policy expires.

This release does not support a default policy lifetime value. You must manually enter a lifetime value.

Use the “no” option for this command to reset the lifetime to the default value for the IKE policy.

Example

This example shows how to configure the winRadius IKE policy lifetime to **360** minutes:

```
S Chassis(su-config)->crypto ike-policy winRadius
S Chassis(su-crypto-policy)->lifetime time 360
S Chassis(su-crypto-policy)->
```

passive

Use this command to enable passive mode for the IKE policy.

Syntax

passive

no passive

Parameters

None.

Defaults

None.

Mode

IKE policy configuration.

Usage

If passive mode is enabled, the local device waits for the peer to initiate the IKE session. By default a device is in active mode and constantly polls to see if the peer is up.

Use the “no” option for this command to reset passive mode to the default state. Passive mode is disabled by default for the IKE policy.

Example

This example shows how to enable passive mode for the winRadius IKE policy:

```
S Chassis(su-config)->crypto ike-policy winRadius
S Chassis(su-crypto-policy)->passive
S Chassis(su-crypto-policy)->
```

peer

Use this command to configure the SA peer for the IKE policy.

Syntax

peer *address*

no peer *address*

Parameters

address	Specifies the IPv4 or IPv6 address of the SA peer for the IKE policy.

Defaults

None.

Mode

IKE policy configuration.

Usage

Use the “no” option for this command to delete the peer address configuration for the IKE policy.

Example

This example shows how to configure the winRadius IKE policy peer to **1.1.191.22**:

```
S Chassis(su-config)->crypto ike-policy winRadius
S Chassis(su-crypto-policy)->peer 1.1.191.22
S Chassis(su-crypto-policy)->
```

proposal

Use this command to assign an IKE proposal to the IKE policy.

Syntax

proposal *proposal-identifier*

no proposal *proposal-identifier*

Parameters

proposal-identifier	Specifies the IKE proposal to assign to the IKE policy. Valid value is up to 32 alpha-numeric characters plus special characters dash (**-**) and underscore (_).

Defaults

None.

Mode

IKE policy configuration.

Usage

The proposal assigned to an IKE policy is the quick mode or data protection proposal. Quick mode negotiates on behalf of the IPsec SAs. During Quick mode, keying material is refreshed or, if necessary, new keys are generated. The quick mode proposal assigned to the IKE policy can be the same proposal assigned to main mode or it can be a different one.

Use the “no” option for this command to remove the IKE proposal from the IKE policy configuration.

Example

This example shows how to assign the winRadius_quick IKE proposal to the winRadius IKE policy:

```
S Chassis(su-config)->crypto ike-policy winRadius
S Chassis(su-crypto-policy)->proposal winRadius_quick
S Chassis(su-crypto-policy)->
```

version

Use this command to configure the IKE version for the IKE policy.

Syntax

version *version*

no version *version*

Parameters

version	Specifies the IKE version for this IKE policy. Valid value is **1**.

Defaults

None.

Mode

IKE policy configuration.

Usage

A default value is not supported for IKE version. You must manually set the IKE version.

Use the “no” option for this command to remove the IKE version from the IKE policy configuration.

Example

This example shows how to set the IKE version to **1** for the IKE policy:

```
S Chassis(su-config)->crypto ike-policy winRadius
S Chassis(su-crypto-policy)->version 1
S Chassis(su-crypto-policy)->
```

IKE Map Commands

This section details commands for entering IKE map configuration mode for the specified map and the configuration of that map.

For information about...	Refer to page...
crypto ike-map	4-14
dst	4-15
dst-port	4-16
encapsulation	4-16
lifetime	4-17
policy	4-18
proposal	4-19
protocol udp	4-19
request	4-20
src	4-21
src-port	4-21

crypto ike-map

Use this command to create or modify an IKE map and enter IKE map configuration mode.

Syntax

crypto ike-map *map-identifier*

no crypto ike-map *map-identifier*

Parameters

map-identifier	Specifies the IKE map to create or modify. Valid value is up to 32 alpha-numeric characters plus special characters dash (-) and underscore (_).

Defaults

None.

Mode

Global VRF router configuration.

Usage

Use the “no” option for this command to delete the specified IKE map.

Example

This example shows how to enter IKE map configuration mode for the winRadius IKE map:

```
S Chassis(su-config)->crypto ike-map winRadius
S Chassis(su-crypto-map)->
```

dst

Use this command to configure a destination (peer) address for this IKE map.

Syntax

dst *address*

no dst *address*

Parameters

address	Specifies an SA destination device IPv4 or IPv6 address for this IKE map.

Defaults

None.

Mode

IKE map configuration.

Usage

Address ranges are supported using the slash (/) length notation.

Use the “no” option for this command to delete the IKE map destination address.

Example

This example shows how to set the IKE map destination address to 1.1.191.0/24:

```
S Chassis(su-config)->crypto ike-map winRadius
S Chassis(su-crypto-map)->dst 1.1.191.0/24
S Chassis(su-crypto-map)->
```

This example shows how to set the IKE map destination address to 2001:2010::0/64:

```
S Chassis(su-config)->crypto ike-map winRadius
S Chassis(su-crypto-map)->dst 2001:2010::0/64
S Chassis(su-crypto-map)->
```

dst-port

Use this command to configure a destination port for this IKE map.

Syntax

dst-port *port*

no dst-port *port*

Parameters

port	Specifies an SA destination device port for this IKE map. Default value is any port.

Defaults

None.

Mode

IKE map configuration.

Usage

Use this command to specify a destination port for this SA when a specific protocol such as HTTPS is being authenticated.

Use the “no” option for this command to reset the IKE map destination port configuration to the default value of any port.

Example

This example shows how to set the destination port for this SA to the standard RADIUS port 500:

```
S Chassis(su-config)->crypto ike-map winRadius
S Chassis(su-crypto-map)->dst-port 500
S Chassis(su-crypto-map)->
```

encapsulation

Use this command to configure the encapsulation mode for this IKE map.

Syntax

encapsulation {**tunnel** | **transport**}

no encapsulation {**tunnel** | **transport**}

Parameters

tunnel	Sets the IKE map encapsulation mode to tunnel.
transport	Sets the IKE map encapsulation mode to transport.

Defaults

None.

Mode

IKE map configuration.

Usage

Transport mode is used for host-to-host communications. In transport mode, only the transferred data of the IP packet is encrypted or authenticated. The routing is intact, since the IP header is neither modified nor encrypted; however, when the authentication header is used, the IP addresses cannot be translated, because to do so would invalidate the hash value.

Tunnel mode is used to create virtual private networks. In tunnel mode, the entire IP packet is encrypted or authenticated. It is then encapsulated into a new IP packet with a new IP header.

Use the “no” option for this command to delete the specified IKE map encapsulation configuration.

Example

This example shows how to set the IKE map encapsulation mode to transport for this SA:

```
S Chassis(su-config)->crypto ike-map winRadius
S Chassis(su-crypto-map)->encapsulation transport
S Chassis(su-crypto-map)->
```

lifetime

Use this command to configure the lifetime in time and bandwidth for this IKE map.

Syntax

lifetime {**time** *minutes* | **bandwidth** *kilobytes*}

no lifetime {**time** *minutes* | **bandwidth** *kilobytes*}

Parameters

time *minutes*	Specifies the time in minutes before this IKE map times-out. Valid values are 5 - 2879 minutes
bandwidth *kilobytes*	Specifies the amount of bandwidth used that will cause this IKE map to timeout. Valid values are 20480 to 2147483647 kilobytes.

Defaults

None.

Mode

IKE map configuration.

Usage

Use the “no” option for this command to reset the time or bandwidth to the default value for this IKE map.

Example

This example shows how to set the winRadius IKE map lifetime to 5 minutes and 100000 kilobytes of bandwidth:

```
S Chassis(su-config)->crypto ike-map winRadius
S Chassis(su-crypto-map)->lifetime time 5
S Chassis(su-crypto-map)->lifetime bandwidth 100000
S Chassis(su-crypto-map)->
```

policy

Use this command to assign the specified IKE policy to the IKE map.

Syntax

policy *policy-identifier*

no policy *policy-identifier*

Parameters

policy-identifier	Specifies the IKE policy assigned to this IKE map. Valid value is up to 32 alpha-numeric characters. Valid value is up to 32 alpha-numeric characters plus special characters dash (**-**) and underscore (_).

Defaults

None.

Mode

IKE map configuration.

Usage

Use this command to assign an IKE policy to the an IKE map. An IKE policy is configured by entering IKE policy configuration mode using “crypto ike-policy” on page 4-8.

The IKE policy does not have to exist in order to assign it to the IKE map. If the assigned policy does not exist, the **show ike map** command will specify that the policy does not exist.

Use the “no” option to remove the specified IKE policy from the IKE map.

Example

This example shows how to assign the **winRadius** IKE policy to the **winRadius** IKE map:

```
S Chassis(su-config)->crypto ike-map winRadius
S Chassis(su-crypto-map)->policy winRadius
S Chassis(su-crypto-map)->
```

proposal

Use this command to assign the specified IKE proposal to the IKE map.

Syntax

proposal *proposal-identifier*

no proposal *proposal-identifier*

Parameters

proposal-identifier	Specifies the IKE proposal assigned to this IKE map. Valid value is up to 32 alpha-numeric characters plus special characters dash (-) and underscore (_).

Defaults

None.

Mode

IKE map configuration.

Usage

The proposal assigned to an IKE map is the main mode or key exchange proposal. Main mode is the IKE negotiation that establishes a secure channel, known as the Internet Security Association and Key Management Protocol (ISAKMP) SA, between two devices.

The IKE proposal does not have to exist in order to assign it to the IKE map. If the assigned proposal does not exist, the **show ike map** command will specify that the proposal does not exist.

An IKE proposal is configured by entering IKE proposal configuration mode using "crypto ike-proposal" on page 4-4.

Use the "no" option to remove the specified IKE proposal from the IKE map.

Example

This example shows how to assign the **winRadius_main** IKE proposal to the **winRadius** IKE map:

```
S Chassis(su-config)->crypto ike-map winRadius
S Chassis(su-crypto-map)->proposal winRadius_main
S Chassis(su-crypto-map)->
```

protocol udp

Use this command to configure the IKE map with the UDP protocol.

Syntax

protocol udp

no protocol udp

Parameters

None.

Defaults

None.

Mode

IKE map configuration.

Usage

Use this command to configure the UDP protocol as the means of message transmission for this SA. There is no default protocol configuration. Manually configure the UDP protocol for the SA to be active.

Use the “no” option to remove the UDP protocol configuration.

Example

This example shows how to set UDP as the transmission protocol for the **winRadius** IKE map:

```
S Chassis(su-config)->crypto ike-map winRadius
S Chassis(su-crypto-map)->protocol udp
S Chassis(su-crypto-map)->
```

request

Use this command to request rather than require that encryption be used by the SA.

Syntax

request

no request

Parameters

None.

Defaults

None.

Mode

IKE map configuration.

Usage

By default encryption is required to be used for the SA both locally and by the peer. If the peer does not support encryption, packets are not sent for the SA. If encryption request is enabled and the peer cannot encrypt, packets are sent unencrypted. Use this command to set the requirement for encryption to request for the SA. Request is disabled by default.

Use the “no” option to require encryption for the SA (disable the request feature).

Example

This example shows how to request that encryption be used by the SA for the **winRadius** IKE map:

```
S Chassis(su-config)->crypto ike-map winRadius
S Chassis(su-crypto-map)->request
S Chassis(su-crypto-map)->
```

src

Use this command to configure a source address for this IKE map.

Syntax

src *address*

no src *address*

Parameters

address	Specifies a SA source device IPv4 or IPv6 address for this IKE map.

Defaults

None.

Mode

IKE map configuration.

Usage

The source address is the IPv4 or IPv6 address for this device. An address range is supported using the slash (/) length notation.

Use the “no” option for this command to delete the IKE map source address.

Example

This example shows how to set the source address to 192.1.192.4 for this IKE map:

```
S Chassis(su-config)->crypto ike-map winRadius
S Chassis(su-crypto-map)->src 192.1.192.4
S Chassis(su-crypto-map)->
```

src-port

Use this command to configure a source port for this IKE map.

Syntax

dst-port *port*

no dst-port *port*

Parameters

port	Specifies an SA source device port for this IKE map. The default value is any port.

Defaults

None.

Mode

IKE map configuration.

Usage

Use this command to specify a source port for this SA when a specific protocol such as HTTPS is being authenticated.

Use the “no” option for this command to reset the IKE map source port configuration to the default value of any port.

Example

This example shows how to set the source port for this SA to the standard RADIUS port 500 for IKE map winRadius:

```
S Chassis(su-config)->crypto ike-map winRadius
S Chassis(su-crypto-map)->src-port 500
S Chassis(su-crypto-map)->
```

Show Commands

For information about...	Refer to page...
show ike stats	4-23
show ike proposal	4-24
show ike policy	4-25
show ike map	4-26
show ike sa	4-27
show ipsec counters	4-27
show ipsec map	4-29
show ipsec sa	4-30
show ipsec flow	4-31
show ipsec instance	4-33
show ipsec interface	4-34

show ike stats

Use this command to display IKE statistics.

Syntax

show ike stats

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display IKE statistics:

```
S Chassis(su)->show ike stats
-------------------------------------------------------------------------------------------
IKE version 1
       ID PROT -----------> OK  secs:  1389   usecs:     150000  count:  1992 rate(ms): 697.36
        ID PROT -----------> NOK secs: 813799939   usecs:     110000  count:  9102 rate(ms):
89408914.43
     AGGRESSIVE -----------> OK  secs:     0   usecs:          0  count:     0 rate(ms): 0.00
     AGGRESSIVE -----------> NOK secs:     0   usecs:          0  count:     0 rate(ms): 0.00
     QUICK MODE -----------> OK  secs:    16   usecs:     890000  count:  1628 rate(ms): 10.37
     QUICK MODE -----------> NOK secs:     0   usecs:          0  count:   364 rate(ms): 0.00
    TRANSACTION -----------> OK  secs:     0   usecs:          0  count:     0 rate(ms): 0.00
    TRANSACTION -----------> NOK secs:     0   usecs:          0  count:     0 rate(ms): 0.00
  INFORMATIONAL -----------> OK  secs:     1   usecs:     360000  count:   136 rate(ms): 10.00
  INFORMATIONAL -----------> NOK secs:     0   usecs:          0  count: 17255 rate(ms): 0.00
         REKEY -----------> OK  secs:    51   usecs:     180000  count:  4817 rate(ms): 10.62
         REKEY -----------> NOK secs: -5447446   usecs:     190000  count:    89 rate(ms):
-61207256.29
-------------------------------------------------------------------------------------------
IKE version 2
   SA INIT/AUTH -----------> OK  secs:     0   usecs:          0  count:     0 rate(ms): 0.00
   SA INIT/AUTH -----------> NOK secs:     0   usecs:          0  count:     0 rate(ms): 0.00
       CHILD SA -----------> OK  secs:     0   usecs:          0  count:     0 rate(ms): 0.00
       CHILD SA -----------> NOK secs:     0   usecs:          0  count:     0 rate(ms): 0.00
  INFORMATIONAL -----------> OK  secs:     0   usecs:          0  count:     0 rate(ms): 0.00
  INFORMATIONAL -----------> NOK secs:     0   usecs:          0  count:     0 rate(ms): 0.00
         REKEY -----------> OK  secs:     0   usecs:          0  count:     0 rate(ms): 0.00
         REKEY -----------> NOK secs:     0   usecs:          0  count:     0 rate(ms): 0.00
-------------------------------------------------------------------------------------------
Uptime 872328 seconds
Number of active exchanges: 0
```

```
Number of active IKE SA:    1
-------------------------------------------------------------------------------------------

S Chassis(su)->
```

show ike proposal

Use this command to display IKE proposal configuration.

Syntax

show ike proposal

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display IKE proposals:

```
S Chassis(su)->show ike proposal
IPIke proposal winRadiusV6_quick (index 0)
 Dh groups:                not configured
 Encryption Algs:          aes256cbc
 Hash Algs:                not configured
 Integrity Algs:           sha1
 Valid config:             yes
 Status flags:

IPIke proposal winRadius_quick (index 1)
 Dh groups:                not configured
 Encryption Algs:          aes192cbc
 Hash Algs:                not configured
 Integrity Algs:           sha1
 Valid config:             yes
 Status flags:

S Chassis(su)->
```

show ike policy

Use this command to display IKE policy configuration.

Syntax

show ike policy

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display IKE policy:

```
S Chassis(su)->show ike policy
IPIke policy winRadiusV6 (index 0)
 Proposal:                winRadiusV6_main
 Lifetime:                60 minutes
 Exchange versions:       1
 Passive mode:            disabled
 Initial contact:         enabled
 Keepalive:               0
 Local:                   2001:4094::102 (mgmt)
 Peer:                    2001:14::172:1:191:210
 Authentication type:     pre_shared_key
 Authentication data:     :a8c78abe01874ec1096808973dcec135015db26d:
 Valid config:            yes
 Status flags:

IPIke policy winRadius (index 1)
 Proposal:                winRadius_main
 Lifetime:                60 minutes
 Exchange versions:       1
 Passive mode:            disabled
 Initial contact:         enabled
 Keepalive:               0
 Local:                   1.1.191.6 (mgmt)
 Peer:                    1.1.191.22
 Authentication type:     pre_shared_key
 Authentication data:     :364567b02e23c1f6418c85f3162085ef7718c180:
 Valid config:            yes
 Status flags:
S Chassis(su)->
```

show ike map

Use this command to display IKE map configuration.

Syntax

show ike map

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display IKE map information:

```
S Chassis(su)->show ike map
IPIke map winRadiusV6 (index 0)
 Policy id:                winRadiusV6
 Proposal id:              winRadiusV6_quick
 Protocol:                 udp
 Lifetime (time):          5 minutes
 Lifetime (bandwidth):     100000 kilobytes
 Src addr:                 2001:4094::102/128
 Dst addr:                 2001:14::172:1:191:210/128
 Src port:                 0
 Dst port:                 0
 Encap mode:               transport
 Valid config:             yes
 Request:                  Disabled
 Status flags:

IPIke map winRadius (index 1)
 Policy id:                winRadius
 Proposal id:              winRadius_quick
 Protocol:                 udp
 Lifetime (time):          5 minutes
 Lifetime (bandwidth):     100000 kilobytes
 Src addr:                 1.1.191.6/32
 Dst addr:                 1.1.191.22/32
 Src port:                 0
 Dst port:                 0
 Encap mode:               transport
 Valid config:             yes
 Request:                  Disabled
```

```
 Status flags:
S Chassis(su)->
```

show ike sa

Use this command to display IKE SA information.

Syntax

show ike sa

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display IKE SA information:

```
S Chassis(su)->show ike sa
[0] initiator cookie: 0x6cd01c6d1f7b01ea responder cookie: 0x0000000000000000
        created 2 seconds ago as initiator, ref.count: 1, state: CONSTRUCTING
        peer addr: 1.1.191.23, local addr: 192.1.191.2
        sent bytes: 80, received bytes: 0
S Chassis(su)->
```

show ipsec counters

Use this command to display IPsec counter statistics.

Syntax

show ipsec counters [**all** | **ipsec** | **global** | **memory** | **resources** | **task**]

Parameters

all	(Optional) Displays all IPsec counters.
ipsec	(Optional) Displays IPsec global, SA, and diagnostic counters.
global	(Optional) Displays global IPsec counters.
memory	(Optional) Displays IPsec memory counters.
resources	(Optional) Displays IPsec resource counters.
task	(Optional) Displays IPsec task counters.

Defaults

If no option is specified, all IPsec counters display.

Mode

All command modes.

Example

This example shows how to display all IPsec counters :

```
S Chassis(su)->show ipsec counters

IP Security Global Counters:

IPSec Global Counters:
PfKeyv2 Flushes(Total)                  1
IPSec Global SA Counters:
SA Alloc Error:                         0
SA DelPend(Total)                      12
SA DelePend(Cur):                       0
SA Programmed(Total)                    8
SA Program WorkItems:                   0
SA De-Programmed(Total)                12

IPSec Global Flow Counters:
FLOW Alloc Error:                       0
FLOW DelPend(Total)                   186
FLOW DelePend(Cur):                     0
FLOW Programmed(Total)                 76
FLOW Program WorkItems:                 0
FLOW De-Programmed(Total)             186


Global Resources:
Resource                   Limit  Allocated       Free
Vrf                            1          1          0
IPSec SA (Static)            128          0        128
IPSec SA (Dynamic)           400          2        398
IPSec Flow (Static)          256          0        256
IPSec Flow (Dynamic)         400          6        394
IPSec Instance (Static)          64          0          64
IPSec Instance (Dynamic)         192          0        192
IPSec Interface             1024          0       1024
IPIke Policy                  10          2          8
IPIke Proposal                20          4         16
IPIke Map                     10          2          8
IPSec Map                     10          1          9
```

```
Task Global Counters:
Loops:         3328 Timeouts:         0 Wakeups:        1084 WakeupTrig:      1084

Memory Global Counters:
Total Allocs:            4 Total Frees:             0 Total Misses:             0
Current Allocs:          4 Current Bytes:      322068
High Allocs:             4 High Bytes:         322068

***** IPsec Diagnostic Counters *****
 RAD_sa      = 0x00000008 | RAD_flow    = 0x0000004c | RAD_inst    = 0x00000001
 RAD_intf    = 0x00000008 | RDD_sa      = 0x0000000c | RDD_inst    = 0x00000005
 OSPFv3Set   = 0x00000004 | OSPFv3Clr   = 0x00000004 | InstFindNE  = 0x00000001
```

show ipsec map

Use this command to display IPsec map information.

Syntax

show ipsec map

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display all IPsec counters :

```
S Chassis(su)->show ipsec map
IPSec map winRadius (index 0)
 Instance id:              0
 VR id:                    0
 Minor tag:                20
 Attached Flow Indexes:    8 9 10 11
 Valid config:             yes
 Status flags:             programmed

IPSec map winRadiusV6 (index 1)
 Instance id:              0
 VR id:                    0
 Minor tag:                21
 Attached Flow Indexes:    12 13 14 15
```

```
Valid config:              yes
Status flags:              programmed
```

show ipsec sa

Use this command to display IPsec SA information.

Syntax

show ipsec sa [**spi** *spi*] [**instance_id** *instance_id*] [**index** *index*] [**ipv4** | **ipv6**] [**brief**]

Parameters

spi *spi*	(Optional) Filters the display by the specified Security Parameter Index (SPI).
instance_id *instance_id*	(Optional) Filters the display based upon the IPsec instance ID.
index *index*	(Optional) Filters the display based upon the SA index.
ipv4 | **ipv6**	(Optional) Filters the display based upon either IPv4 or IPv6 addressing.
brief	(Optional) Displays a summary version of IPsec SA information

Defaults

If no option is specified, all IPsec SAs are displayed.

Mode

All command modes.

Usage

SA SPI, index, and instance IDs for all SAs are available by entering the **show ipsec sa** or **show ipsec flow** commands without specifying an option.

The current release only supports the manual configuration of a **default** instance, specified as either **default** or **0**. An instance ID above 64 is dynamically created when you provision authentication or encryption for OSPFv3.

Example

This example shows how to display all IPsec counters :

```
S Chassis(su)->>show ipsec sa

IPSec IPv6 SA (Index: 4) SPI: 1915327043 (0x72299243)
 Source IP:           2001::1
 Destination IP:      2001:4094::8c3c:6041:22ff:6cb0
 IPSec Protocol:      esp
 Direction:           egress
 Persistence:         dynamic
 Active:              yes
 Instance Id:         default
```

```
 Vrf Id:              0
 Number of Flows:     1
 Encap Mode:          transport
 Auth Algorithm:      sha1-hmac
 Cipher Algorithm:    aescbc

IPSec IPv6 SA (Index: 8) SPI:  574398787 (0x223ca143)
 Source IP:           2001:4094::8c3c:6041:22ff:6cb0
 Destination IP:      2001::1
 IPSec Protocol:      esp
 Direction:           ingress
 Persistence:         dynamic
 Active:              yes
 Instance Id:         default
 Vrf Id:              0
 Number of Flows:     1
 Encap Mode:          transport
 Auth Algorithm:      sha1-hmac
 Cipher Algorithm:    aescbc

Number of SAs displayed: 2
```

show ipsec flow

Use this command to display IPsec flow information.

Syntax

show ipsec flow [**spi** *spi*] [**instance_id** *instance_id*] [**index** *index*] [**ipv4** | **ipv6**] [**brief**]

Parameters

spi *spi*	(Optional) Filters the display by the specified SPI.
instance_id *instance_id*	(Optional) Filters the display based upon the IPsec instance ID.
index *index*	(Optional) Filters the display based upon the instance index.
ipv4 | **ipv6**	(Optional) Filters the display based upon either IPv4 or IPv6 addressing.
brief	(Optional) Displays a summary version of IPsec flow information

Defaults

If no option is specified, all IPsec flows are displayed.

Mode

All command modes.

Usage

The SA SPI, index, and instance IDs for all SAs are available by entering the **show ipsec sa** or **show ipsec flow** commands without specifying an option.

The current release only supports the manual configuration of a **default** instance, specified as either **default** or **0**. An instance ID above 64 is dynamically created when you provision authentication or encryption for OSPFv3.

Example

This example shows how to display all IPsec information for all flows:

```
S Chassis(su)->show ipsec flow

IPSec IPv6 Flow 10 (Associated SA index 4):
 Type:                    use
 Protocol:                udp
 Source Port:             any
 Destination Port:        any
 Direction:               egress
 Persistence:             dynamic
 Active:                  yes
 Priority:                -50
 Instance Id:             default
 Source IP:               2001::1/128
 Destination IP:          2001:4094::8c3c:6041:22ff:6cb0/128

IPSec IPv6 Flow 11 (Associated SA index 8):
 Type:                    use
 Protocol:                udp
 Source Port:             any
 Destination Port:        any
 Direction:               ingress
 Persistence:             dynamic
 Active:                  yes
 Priority:                -50
 Instance Id:             default
 Source IP:               2001:4094::8c3c:6041:22ff:6cb0/128
 Destination IP:          2001::1/128

Number of flows displayed: 2
```

show ipsec instance

Use this command to display IPsec instance information.

Syntax

show ipsec instance [**vlan** *vlan-id*] [**instance_id** *instance_id*] [**index** *index*] [**static** | **dynamic**] [**brief**]

Parameters

vlan *vlan-id*	(Optional) Filters the display by the specified VLAN.
instance_id *instance_id*	(Optional) Filters the display based upon the IPsec instance ID.
index *index*	(Optional) Filters the display based upon the instance index.
static | **dynamic**	(Optional) Filters the display based upon either static or dynamic instances.
brief	(Optional) Displays a summary version of IPsec instance information

Defaults

If no option is specified, all IPsec instances are displayed.

Mode

All command modes.

Usage

The SA index and instance IDs for all instances are available by entering the **show ipsec instance** command without specifying an option.

The current release only supports the manual configuration of a **default** instance, specified as either **default** or **0**. An instance ID above 64 is dynamically created when you provision authentication or encryption for OSPFv3.

Example

This example shows how to display all IPsec information for all instances:

```
S Chassis(su)->show ipsec instance

IPsec instance default (Index: 2):
 Vrf Id:                   0
 Persistence:              static
 Owner:                    cli
 Attached SAs:             0
 Attached Flows:           0
 Attached Vlans:           all

IPsec instance 65 (Index: 1):
 Vrf Id:                   0
 Persistence:              dynamic
```

```
 Owner:                    ospf
 Attached SAs:             2
 Attached Flows:           2
 Attached Vlans:           4000

Number of Instances displayed: 2
```

show ipsec interface

Use this command to display IPsec interface information.

Syntax

show ipsec instance [**vlan** *vlan-id*] [**instance_id** *instance_id*] [**static** | **dynamic**] [**brief**]

Parameters

vlan *vlan-id*	(Optional) Filters the display by the specified VLAN.
instance_id *instance_id*	(Optional) Filters the display based upon the IPsec instance ID.
static | **dynamic**	(Optional) Filters the display based upon either static or dynamic instances.
brief	(Optional) Displays a summary version of IPsec interface information

Defaults

If no option is specified, all IPsec interfaces are displayed.

Mode

All command modes.

Example

This example shows how to display all IPsec information for all interfaces:

```
S Chassis(su)->show ipsec interface

IPSec Interface Index 4000:
 Vlan Id:                  4000
 Vrf Id:                   0
 Persistence:              dynamic
 Associated Instances:     default, 65

Number of Interfaces displayed: 1
S Chassis(su)->
```

5

Public-Key Infrastructure (PKI) Commands

This chapter describes the Public-Key Infrastructure (PKI) set of commands and how to use them. For information about configuring PKI, refer to the "Public-Key Infrastructure (PKI) Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show pki certificate	5-1
show config pki	5-4
set pki certificate	5-5
clear pki certificate	5-6
show pki oscp	5-7
set pki ocsp	5-8
set pki ocsp signature-ca-list	5-9
clear pki ocsp signature-ca-list	5-10
set pki ocsp nonce	5-10
set pki ocsp responder	5-11
clear pki ocsp responder	5-12
show pki authorization	5-12
set pki authorization username	5-13
set pki authorization username attribute	5-14
clear pki authorization	5-15

show pki certificate

Use this command to display certificate lists and certificate details.

Syntax

show pki certificate [*pki-cert-list* [*fingerprint*]]

Parameters

pki-cert-list	(Optional) Specifies the name of the certificate list to display.

fingerprint	(Optional) Specifies a specific public key fingerprint member of a certificate list to display. This options displays certificate information details as defined in RFC 5280.

Defaults

- If *pki-cert-list* is not specified, all configured certificate lists display.
- If *fingerprint* is not specified, all members of the specified certificate list display.

Mode

All command modes.

Examples

This example shows how to display the fingerprint **a2:33:a9:df:df:8a:fb:9a:d2:f0:5e:c0:c3:8a:8a:4b:ad:0a:6f:1b** member of the **myTrustedOcspSigningCerts** list:

```
S Chassis(rw)->show pki certificate myTrustedOcspSigningCerts
a2:33:a9:df:df:8a:fb:9a:d2:f0:5e:c0:c3:8a:8a:4b:ad:0a:6f:1b
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4 (0x4)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=Enterasys, OU=DoD, OU=PKI, CN=Esys JITC Root CA 2
        Validity
            Not Before: Feb 21 18:44:14 2012 GMT
            Not After : Feb 18 18:44:14 2022 GMT
        Subject: C=US, O=Enterasys, OU=DoD, OU=PKI, CN=Esys JITC Root CA 2 OCSP
Delegate 2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:ab:de:7f:15:88:a1:44:47:ff:7d:a2:c3:c9:92:
                    eb:83:08:73:49:34:fb:ff:33:37:69:47:7f:fb:3e:
                    4f:e3:1b:aa:59:94:aa:b8:82:03:1d:89:7c:21:8c:
                    d6:37:29:81:00:78:81:d3:14:d1:fa:8c:b2:06:f5:
                    ...
                    17:79:31:f9:ac:9f:c7:46:98:bc:51:ae:9e:88:ba:
                    46:b1
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Authority Key Identifier:
               keyid:57:24:01:5D:5B:25:E3:78:42:B2:47:DF:3F:7B:F9:83:90:CA:B2:E0
                DirName:/C=US/O=Enterasys/OU=DoD/OU=PKI/CN=Esys JITC Root CA 2
```

```
                serial:05

            X509v3 Subject Key Identifier:
                4B:D3:68:BB:FF:4A:6D:7D:87:17:31:5C:B1:6A:89:7F:71:E4:97:22
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Extended Key Usage:
                OCSP Signing
            OCSP No Check:

    Signature Algorithm: sha1WithRSAEncryption
        97:29:e9:f6:b1:7b:fa:f0:06:80:ec:92:b5:b8:98:55:0f:dc:
        51:b9:6c:3b:3b:e2:77:43:cc:c0:e0:1f:c1:33:9b:e4:86:26:
        ...
        ef:36:72:6b:e4:b2:7e:c6:ac:f4:81:f4:83:24:1d:fc:e5:94:
        cc:ea:8e:1b
-----BEGIN TRUSTED CERTIFICATE-----
MIIELjCCAxagAwIBAgIBBDANBgkqhkiG9w0BAQUFADBbMQswCQYDVQQGEwJVUzES
MBAGA1UEChMJRW50ZXJhc3lzMQwwCgYDVQQLEwNEb0QxDDAKBgNVBAsTA1BLSTEc
MBoGA1UEAxMTRXN5cyBKSVRDIFJvb3QgQ0EgMjAeFw0xMjAyMjExODQ0MTRaFw0y
MjAyMTgxODQ0MTRaMGsxCzAJBgNVBAYTAlVTMRIwEAYDVQQKEwlFbnRlcmFzeXMx
DDAKBgNVBAsTA0RvRDEMMAoGA1UECxMDUEtJMSwwKgYDVQQDEyNFc3lzIEpJVEMg
Um9vdCBDQSAyIE9DU1AgRGVsZWdhdGUgMjCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAKvefxWIoURH/32iw8mS64MIc0k0+/8zN2lHf/s+T+MbqlmUqriC
Ax2JfCGM1jcpgQB4gdMU0fqMsgb1aQ5Vy3adtAzj7jZ9IS3OmX2O0ZBRi4rXr1dg
NukkfOdSBg68/pzzjdaZEsbeeXNdZnbtlemex+9KvBJ9TLw8pt4ZxQF12AIulRAI
Ov4WVcpnHHQL7WAcEcF56xqcYLkDYKDHhqkwanM8kEnHptWvTVqv9hEr054wu88a
lqzPYLnhNdY8mqsOAFuBM/kJcblSZjb+VI4bfwOAAn/SikbBqn9+9jG4lE1WUPDB
sWIdfZt6p+7tF3kx+ayfx0aYvFGunoi6RrECAwEAAaOB7DCB6TAOBgNVHQ8BAf8E
BAMCAYYwgYMGA1UdIwR8MHqAFFckAV1bJeN4QrJH3z97+YOQyrLgoV+kXTBbMQsw
CQYDVQQGEwJVUzESMBAGA1UEChMJRW50ZXJhc3lzMQwwCgYDVQQLEwNEb0QxDDAK
BgNVBAsTA1BLSTEcMBoGA1UEAxMTRXN5cyBKSVRDIFJvb3QgQ0EgMoIBBTAdBgNV
HQ4EFgQUS9Nou/9KbX2HFzFcsWqJf3HklyIwDAYDVR0TAQH/BAIwADATBgNVHSUE
DDAKBggrBgEFBQcDCTAPBgkrBgEFBQcwAQUEAgUAMA0GCSqGSIb3DQEBBQUAA4IB
AQCXKen2sXv68AaA7JK1uJhVD9xRuWw7O+J3Q8zA4B/BM5vkhiZZMK+Ro70HaQSI
ebAjrXsZ1VUD1pS5nkud2TawYwICyL8jxxbIX9nnIC6esr9shmCaxv/pCXMI5iZr
3zPism/n8OJpk6ZR75F/8Tnt8lUXrSFvJdwxb76nFR6zPStNorSuSgrZaGtmftUj
xZs7/PKXxWoryZmfua6oIg7SACWApBSu6Jhj7lgS6wAvow4K3WCbso+afmnpcNT7
kMkWJO7J4jUaKS/yjn8xkO2HhZZ+g1Lh1lK00i+hOx515aUHj2DpxMNQtiTvNnJr
5LJ+xqz0gfSDJB385ZTM6o4b
-----END TRUSTED CERTIFICATE-----
S Chassis(rw)->
```

show config pki

Use this command to display the original Privacy Enhanced Mail (PEM) data used to configure the certificates.

Syntax

show config pki [**outfile** *slotN/file-name*]

Parameters

outfile *slotN/file-name*	(Optional) Specifies a filename of a file to be created on the specified slot containing the contents of the display.

Defaults

If the **outfile** option is not specified, no file is created containing the display output.

Mode

All command modes.

Examples

This example shows how to display the fingerprint **a2:33:a9:df:df:8a:fb:9a:d2:f0:5e:c0:c3:8a:8a:4b:ad:0a:6f:1b** member of the **myTrustedOcspSigningCerts** list:

```
S Chassis(rw)->show pki config
This command shows non-default configurations only.
Use 'show config all' to show both default and non-default configurations.

begin
!
# ***** NON-DEFAULT CONFIGURATION *****
!
!
# Chassis Firmware Revision:  08.00.01.0007T
!
# pki
set pki certificate myTrustedCaCerts no-confirm
-----BEGIN TRUSTED CERTIFICATE-----
MIIDcDCCAligAwIBAgIBBTANBgkqhkiG9w0BAQUFADBbMQswCQYDVQQGEwJVUzES
MBAGA1UEChMJRW50ZXJhc3lzMQwwCgYDVQQLEwNEb0QxDDAKBgNVBAsTA1BLSTEc
MBoGA1UEAxMTRXN5cyBKSVRDIFJvb3QgQ0EgMjAeFw0xMjAyMTAxNTI4MTdaFw0y
...
NdJyMX14xpzxKuBvcgi02ADkNER9122dFKuGsQca9vM9LrRhiyROGXiL4bKz9XrE
ZgIHZ5Ozhibhp7NTODveUsda8OKn4TForK3uT3KYFqArG1MtfltfETm0fVheKCxw
/ZCg6s8umuM22HbFkR9TIgbNA+Y=
-----END TRUSTED CERTIFICATE-----
S Chassis(rw)->
```

set pki certificate

Use this command to add a PEM formatted certificate to a certificate list.

Syntax

set pki certificate *pki-cert-list* [**no-confirm**]

Parameters

pki-cert-list	Specifies the name of the certificate list. Valid Values are up to 32 printable characters.
no-confirm	(Optional) Specifies that an entered certificate should be accepted without confirmation.

Defaults

If the no-confirm option is not entered, you are asked to confirm the entered certificate value.

Mode

All command modes with admin privilege.

Usage

This command is used to configure PKI with an X.509 certificate and to group configured X.509 certificates in the specified certificate list. Applications which require PKI services, such as SSH, reference these certificate lists when authenticating.

If the specified list does not exist, it will be automatically created. If all certificates are removed from a list, the list will be automatically deleted. You can delete a single certificate from a certificate list using the **clear pki certificate** command.

The user must have admin (**su**) privilege to use this command. Users with read-only, read-write, or admin privilege can display PKI settings using the **show pki certificate** command.

Once you enter the command specifying the name of the certificate list to be entered, you are asked to enter the PKI certificate:

```
Enter the PEM encoded certificate-list-name certificate
```

Certificate data must be entered in Privacy Enhanced Mail (PEM) format, complete with the appropriate X.509 header **-----BEGIN CERTIFICATE-----** and footer **-----END CERTIFICATE-----**. Certificate entry is terminated by entering a blank line or the word “quit” on a line by itself.

Certificate information then displays. If you did not specify the no-confirm option, you are asked to confirm the entered certificate.

Examples

This example shows how to set the myTrustedOcspSigningCerts PKI certificate, followed by a display of the entered certificate details:

```
S Chassis(su)->set pki certificate myTrustedOcspSigningCerts
Enter the PEM encoded myTrustedOcspSigningCerts certificate
End with a blank line or the word "quit" on a line by itself
-----BEGIN TRUSTED CERTIFICATE-----
MIIELjCCAxagAwIBAgIBBDANBgkqhkiG9w0BAQUFADBbMQswCQYDVQQGEwJVUzES
MBAGA1UEChMJRW50ZXJhc3lzMQwwCgYDVQQLEwNEb0QxDDAKBgNVBAsTA1BLSTEc
```

```
MBoGA1UEAxMTRXN5cyBKSVRDIFJvb3QgQ0EgMjAeFw0xMjAyMjExODQ0MTRaFw0y
MjAyMTgxODQ0MTRaMGsxCzAJBgNVBAYTAlVTMRIwEAYDVQQKEwlFbnRlcmFzeXMx
DDAKBgNVBAsTA0RvRDEMMAoGA1UECxMDUEtJMSwwKgYDVQQDEyNFc3lzIEpJVEMg
Um9vdCBDQSAyIE9DU1AgRGVsZWdhdGUgMjCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAKvefxWIoURH/32iw8mS64MIc0k0+/8zN2lHf/s+T+MbqlmUqriC
Ax2JfCGM1jcpgQB4gdMU0fqMsgb1aQ5Vy3adtAzj7jZ9IS3OmX2O0ZBRi4rXr1dg
NukkfOdSBg68/pzzjdaZEsbeeXNdZnbtlemex+9KvBJ9TLw8pt4ZxQF12AIulRAI
Ov4WVcpnHHQL7WAcEcF56xqcYLkDYKDHhqkwanM8kEnHptWvTVqv9hEr054wu88a
lqzPYLnhNdY8mqsOAFuBM/kJcblSZjb+VI4bfwOAAn/SikbBqn9+9jG4lE1WUPDB
sWIdfZt6p+7tF3kx+ayfx0aYvFGunoi6RrECAwEAAaOB7DCB6TAOBgNVHQ8BAf8E
BAMCAYYwgYMGA1UdIwR8MHqAFFckAV1bJeN4QrJH3z97+YOQyrLgoV+kXTBbMQsw
CQYDVQQGEwJVUzESMBAGA1UEChMJRW50ZXJhc3lzMQwwCgYDVQQLEwNEb0QxDDAK
BgNVBAsTA1BLSTEcMBoGA1UEAxMTRXN5cyBKSVRDIFJvb3QgQ0EgMoIBBTAdBgNV
HQ4EFgQUS9Nou/9KbX2HFzFcsWqJf3HklyIwDAYDVR0TAQH/BAIwADATBgNVHSUE
DDAKBggrBgEFBQcDCTAPBgkrBgEFBQcwAQUEAgUAMA0GCSqGSIb3DQEBBQUAA4IB
AQCXKen2sXv68AaA7JK1uJhVD9xRuWw7O+J3Q8zA4B/BM5vkhiZZMK+Ro70HaQSI
ebAjrXsZ1VUD1pS5nkud2TawYwICyL8jxxbIX9nnIC6esr9shmCaxv/pCXMI5iZr
3zPism/n8OJpk6ZR75F/8Tnt8lUXrSFvJdwxb76nFR6zPStNorSuSgrZaGtmftUj
xZs7/PKXxWoryZmfua6oIg7SACWApBSu6Jhj7lgS6wAvow4K3WCbso+afmnpcNT7
kMkWJO7J4jUaKS/yjn8xkO2HhZZ+g1Lh1lK00i+hOx515aUHj2DpxMNQtiTvNnJr
5LJ+xqz0gfSDJB385ZTM6o4b
-----END TRUSTED CERTIFICATE-----
quit
Entered certificate has the following attributes:
  Fingerprint: a2:33:a9:df:df:8a:fb:9a:d2:f0:5e:c0:c3:8a:8a:4b:ad:0a:6f:1b
        Issuer: C=US, O=Enterasys, OU=DoD, OU=PKI, CN=Esys JITC Root CA 2
        Validity
            Not Before: Feb 21 18:44:14 2012 GMT
            Not After : Feb 18 18:44:14 2022 GMT
        Subject: C=US, O=Enterasys, OU=DoD, OU=PKI, CN=Esys JITC Root CA 2 OCSP
Delegate 2

Do you accept this certificate (y/n) [n]?y
S Chassis(su)->
```

clear pki certificate

Use this command to remove a single certificate from a list, an entire list of certificates, or to completely remove every certificate and list.

Syntax

clear pki certificate [*pki-cert-list* [*fingerprint*]] [**no-confirm**]

Parameters

pki-cert-list	(Optional) Specify the certificate list to be cleared.
fingerprint	(Optional) Specify a single certificate to clear using the certificate fingerprint.
no-confirm	(Optional) Specify that no confirmation of the clear will take place.

Defaults

If no options are specified, all PKI certificates and certificate lists are deleted.

If *fingerprint* is not specified, all certificates for the specified certificate list are deleted and the certificate list is deleted.

If **no-confirm** is not specified, you will be asked to confirm the clear request before it takes place.

Mode

All command modes with admin privilege.

Usage

A certificate fingerprint is a Hex sequence used to authenticate or look up a longer public key. Fingerprints are created by applying a cryptographic hash function to the public portion of the certificate. Fingerprints simplify certificate management.

Examples

This example shows how to clear all certificates and certificate lists:

```
S Chassis(su)->clear pki certificate
This command will remove all certificate lists and all of their certificates.
Do you want to continue (y/n) [n]?y
1 Certificate(s) cleared.
S Chassis(su)->
```

This example shows how to clear the myTrustedOcspSigningCerts certificate list and all member certificates:

```
S Chassis(su)->clear pki certificate myTrustedOcspSigningCerts
This command will remove certificate list "myTrustedOcspSigningCerts" and all of
its certificates.
Do you want to continue (y/n) [n]?y
1 Certificate(s) cleared.
S Chassis(su)->
```

show pki oscp

Use this command to display the current Online Certificate Status Protocol (OCSP) certificate revocation checking configuration.

Syntax

show pki oscp

Parameters

None.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to display the current OCSP certificate revocation checking configuration:

```
S Chassis(rw)->show pki ocsp
OCSP Status:              Enabled
OCSP Nonce Extension:     Enabled
Signature CA List:        myTrusted
Alternate OCSP Responder: http://12.1.213.145:9999 (preferred)
S Chassis(rw)->
```

set pki ocsp

Use this command to globally enable or disable OCSP certificate revocation checking.

Syntax

set pki ocsp {**enable** | **disable**}

Parameters

enable	Enables OCSP certificate revocation checking.
disable	Disables OCSP certificate revocation checking.

Defaults

OCSP certificate revocation checking is enabled by default.

Mode

All command modes with admin privilege.

Usage

This command is used to globally enable or disable OCSP certificate revocation checking. A Certificate Authority (CA) may need to revoke an issued certificate's authorization prior to the issued certificate's expiration date. Some reasons for revocation include

- The user was compromised (keyCompromise)
- A CA in the chain was compromised (cACompromise)
- A newer certificate was issued (superseded)

When OCSP is disabled, checking is not performed and the revocation status of all certificates is assumed to be good (not revoked).

When OCSP is enabled, the device will attempt to obtain revocation status from one of the available OCSP Responders (OCSRs). If an OCSR replies with a revocation status of good, certificate chain verification will resume. If an OCSR replies with a request failure or with a certificate revocation status other than good (REVOKED or UNKNOWN), certificate authentication will fail.

Examples

This example shows how to disable OCSP certificate revocation checking on the device:

```
S Chassis(su)->set pki ocsp disable
S Chassis(rw)->
```

set pki ocsp signature-ca-list

Use this command to specify a list of trusted CA certificates used to verify OCSP response signatures.

Syntax

set pki ocsp signature-ca-list *pki-cert-list*

Parameters

pki-cert-list	Specifies a PKI certificate list created using "set pki certificate" on page 5-5 containing the OCSP response signing certificate.

Defaults

None.

Mode

All command modes with admin privilege.

Usage

This command establishes the OCSP signing certificate trust by matching a signing certificate with a local configuration of the OCSP signing authority in question. This option is specified in Section 4.2.2.2 Authorized Responders of RFC 2560 *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP* as a way of verifying that the entity which issued the OCSP signing certificate is actually authorized to sign a particular certificate's OCSP response message.

See the "Specifying an OCSP Signature Certificate Authority List" section of the *Extreme Networks S-Series Configuration Guide* for details on specifying an OCSP signature certificate authority list.

Examples

This example shows how to specify myTrustedOcspSigningCerts as the certificate list containing trusted CA certificates used to verify OCSP response signatures:

```
S Chassis(su)->set pki ocsp signature-ca-list myTrustedOcspSigningCerts
S Chassis(su)->
```

clear pki ocsp signature-ca-list

Use this command to remove the configured list of trusted CA certificates used to verify OCSP response signatures.

Syntax

```
clear pki ocsp signature-ca-list
```

Parameters

None.

Defaults

None.

Mode

All command modes with admin privilege.

Examples

This example shows how to remove the configured certificate list containing trusted CA certificates used to verify OCSP response signatures:

```
S Chassis(su)->clear pki ocsp signature-ca-list
S Chassis(su)->
```

set pki ocsp nonce

Use this command to enable or disable the inclusion of a nonce extension in the outgoing OCSP request that must be included in the corresponding response.

Syntax

```
set pki ocsp nonce {enable | disable}
```

Parameters

enable	The nonce extension is included in the outgoing OCSP request and looked for in the corresponding OCSP response.
disable	The nonce extension is not included in the outgoing OCSP request.

Defaults

The inclusion of the nonce extension in the OCSP request is enabled by default.

Mode

All command modes with admin privilege.

Usage

This command enables or disables the inclusion of the nonce extension in outgoing OCSP requests. OCSP can be vulnerable to replay attacks, where a signed good response is captured by a malicious intermediary and replayed to the client at a later date after the subject certificate may have been revoked. OCSP overcomes this by including a nonce extension in the request that must

be included in the corresponding response. If the corresponding OSCP response does not contain a matching nonce, the certificate verification will fail.

Examples

This example shows how to disable the inclusion of the nounce extension in the outgoing OCSP request:

```
S Chassis(su)->set pki ocsp nonce disable
S Chassis(su)->
```

set pki ocsp responder

Use this command to configure an alternate OCSP responder (OCSR) URL for the OCSR used to check revocation status.

Syntax

set pki ocsp responder *url* [**preferred**]

Parameters

url	Specifies the URL of the alternate OCSR that will be used to check OCSP certificate revocation status.
preferred	Specifies that this alternate OCSR is preferred over other configured OCSRs for the checking of OCSP certificate revocation status.

Defaults

If preferred is not specified, the OCSR will not be preferred over other configured OCSRs.

Mode

All command modes with admin privilege.

Usage

X.509 certificates may contain an optional AIA extension which contains one or more addresses of OCSP Responders (OCSRs) to be used to check revocation status. In addition to these certificate OCSRs, one alternate OCSR URL may be configured. If this alternate responder is designated as preferred, then it will be tried before the certificate's AIA responders. If not preferred, then the alternate responder will be tried after the AIA responders.

Examples

This example shows how to configure the alternate OCSP Responder's URL to IP address **10.21.1.115**, port **8888**, and path **/mypath**. This configured URI will be tried first. If no response is received then a second OCSP request will be sent to the OCSP Responders defined in the certificate's AIA extension (if present):

```
S Chassis(su)->set pki ocsp responder http://10.21.1.115:8888/mypath preferred
S Chassis(su)->
```

clear pki ocsp responder

Use this command to remove the configured alternate OCSP responder (OCSR) URL for the OCSR used to check revocation status.

Syntax

clear pki ocsp responder

Parameters

None.

Defaults

None.

Mode

All command modes with admin privilege.

Usage.

This example shows how to remove the configured alternate OCSP Responder's URL:

```
S Chassis(su)->clear pki ocsp responder
S Chassis(su)->
```

show pki authorization

Use this command to display the current PKI authorization configuration.

Syntax

show pki authorization

Parameters

None.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to display the current PKI authorization configuration:

```
S Chassis(rw)->show pki authorization ?
  <cr>
MIKE-SSA(su)->show pki authorization
Username:
 Prefix              :
  Subject Attribute  : commonName
  Regular Expression : [0-9]{10}$
 Suffix              : army.mil
S Chassis(rw)->
```

set pki authorization username

Use this command to restrict the system to a single specified authorization credential which must be shared by all users.

Syntax

set pki authorization username *username*

Parameters

username	Specifies the username that is globally used by all users. Valid values are up to 80 printable characters.

Defaults

None.

Mode

All command modes with admin privilege.

Usage

An X.509 certificate can contain information about the roles or privileges associated with the certificate. In practice an individual's responsibilities may change over time, and it is cumbersome to revoke and re-issue certificates each time this happens. The ability to specify a fixed global authorization username provides for mapping the certificate content to a local system user database or remote authentication protocol such as RADIUS. Once communication is established with the server requiring authentication, the user is interactively prompted for a password. The username and password combination is presented to the authorization server.

This command provides for setting a fixed string as the username. The username can also be specified as an attribute that dynamically extracts the username from the subject field of the X.509 certificate. Refer to "set pki authorization username attribute" on page 5-14 for specifying an attribute based username configuration details.

Examples

This example shows how to specify **myusername** as a static username:

```
S Chassis(su)->set pki authorization username myusername
```

```
S Chassis(su)->
```

set pki authorization username attribute

Use this command to configure a dynamically extracted username from the X.509 certificate subject field.

Syntax

set pki authorization username attribute *attribute* [**prefix** *prefix*] [**match** *expression*] [**suffix** *suffix*]

Parameters

attribute	Specifies the distinguished name attribute to extract from the X.509 certificate subject field. Valid values are supported long names, short names, or OID.
prefix *prefix*	Specifies a fixed string to prefix to the username.
match *expression*	Specifies a regular expression to dynamically apply to the extracted attribute.
suffix *suffix*	Specifies a fixed string to suffix to the username.

Defaults

None.

Mode

All command modes with admin privilege.

Usage

This command allows each user to have their own set of authorization credentials based upon a specified distinguished name attribute extracted from the X.509 certificate subject field. The distinguished name attribute can be specified as a long name, short name, or an OID. Table 5-1 lists the supported distinguished name attributes.

Table 5-1 X.509 Subject Field Distinguished Name Attributes

Attribute	Long Name	Short Name	OID
Country Name	countryName	C	2.5.4.6
Organization Name	organizationName	O	2.5.4.10
Organizational Unit Name	organizationalUnitName	OU	2.5.4.11
Common Name	commonName	CN	2.5.4.3

The username can be prefixed with a fixed string. For example, if the distinguished name attribute is **Extremenetworks** and the specified prefix is **foo**, the extracted username will be **fooExtremenetworks**.

In some instances it may be desirable to use only a subset of the extracted attribute, rather than the entire attribute verbatim. The match option allows for the dynamic application of a regular expression to the extracted attribute. The matching character output is used as the username.

The username can be suffixed with a fixed string. For example, if the distinguished name attribute is **US**, and the specified suffix is **bar**, the extracted username will be **USbar**.

Examples

This example shows how to set the username to the organizational name in the X.509 certificate subject field:

```
S Chassis(su)-> set pki authorization username attribute organizationName
S Chassis(su)->
```

This example shows how to match only the final 10 digits in a dotted notation name (**doe.james.m.0123456789**) and append **@army.mil** to the extracted digits for an extracted user name of **0123456789@army.mil**:

```
S Chassis(su)->set pki authorization username attribute commonName match "[^.]*$"
suffix "@army.mil"
S Chassis(su)->
```

clear pki authorization

Use this command to clear the PKI authorization configuration.

Syntax

```
clear pki authorization
```

Parameters

None.

Defaults

None.

Mode

All command modes with admin privilege.

Examples

This example shows how to clear the current PKI authorization configuration:

```
S Chassis(rw)->clear pki authorization
S Chassis(rw)->
```

6

Management Authentication Notification MIB Commands

This chapter provides detailed information for the management authentication notification MIB set of commands. Management authentication notification MIB functionality includes: enabling/disabling the sending of SNMP notifications when a user login authentication event occurs for various management access types. The types of access currently supported by the MIB include console, telnet, ssh, and web. For information about configuring management authentication notification, refer to the "System Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show mgmt-auth-notify	6-1
set mgmt-auth-notify	6-2
clear mgmt-auth-notify	6-3

Note: Ensure that SNMP is correctly configured in order to send these notifications.

show mgmt-auth-notify

Use this command to display the current setting for the Management Authentication Notification MIB.

Syntax

```
show mgmt-auth-notify
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the current information for the Management Authentication Notification:

```
S Chassis(su)->show mgmt-auth-notify

Management Type  Status
---------------  --------
console          enabled
ssh              enabled
telnet           enabled
web              enabled
```

set mgmt-auth-notify

Use this command to either enable or disable the Management Authentication Notification MIB. By selecting the optional Management access type, a user can specifically enable or disable a single access type, multiple access types or all of the access types. The default setting is that all Management Authentication Notification types are enabled.

Syntax

set mgmt-auth-notify {**enable** | **disable**} [**console**] [**ssh**] [**telnet**] [**web**]

Parameters

enable	Enables selected or all notifications.
disable	Disables selected or all notifications.
console	(Optional) sets the console authentications.
ssh	(Optional) sets SSH authentications.
telnet	(Optional) sets telnet authentications.
web	(Optional) sets web authentications.

Defaults

If none of the optional Management Authentication access types are entered, than all authentications types listed above will either be enabled or disabled.

Mode

All command modes.

Usage

Ensure that SNMP is correctly configured on the module in order to send these notifications.

Examples

This example shows how to set all the authentication types to be disabled on the Management Authentication Notification MIB. That information is then displayed with the **show** command:

```
S Chassis(su)->set mgmt-auth-notify disable
S Chassis(su)->show mgmt-auth-notify
```

```
Management Type  Status
---------------  --------
console          disabled
ssh              disabled
telnet           disabled
web              disabled
```

This example shows how to set only the console and telnet authentication access types to be enabled on the Management Authentication Notification MIB. That information is then displayed with the **show** command:

```
S Chassis(su)->set mgmt-auth-notify enable console telnet
S Chassis(su)->show mgmt-auth-notify

Management Type  Status
---------------  --------
console          enabled
ssh              disabled
telnet           enabled
web              disabled
```

clear mgmt-auth-notify

Use this command to set the current setting for the Management Authentication Notification access types to the default setting of enabled.

Syntax

clear mgmt-auth-notify

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

Ensure that SNMP is correctly configured on the module in order to send these notifications.

Example

This example displays the state of Management Authentication Notification access types prior to using the **clear** command, then displays the same information after using the **clear** command:

```
S Chassis(su)->show mgmt-auth-notify

Management Type  Status
---------------  --------
console          enabled
ssh              disabled
telnet           enabled
web              disabled

S Chassis(su)->clear mgmt-auth-notify

S Chassis(su)->show mgmt-auth-notify

Management Type  Status
---------------  --------
console          enabled
ssh              enabled
telnet           enabled
web              enabled
```

7

System Properties Commands

Important Notice

Module, slot, and certain other hardware-based parameters in the Extreme Networks S-Series Standalone CLI support only chassis based S-Series devices, such as the S8, S4, or S3. Executing commands in the Standalone CLI with modular parameters not supported by the Standalone will result in an error message.

This chapter provides detailed information for the system properties set of commands. System properties functionality includes: how to display and set the system IP address and other basic system (device) properties, including time, contact name, timeout, and version information. For information about configuring system properties, refer to the "System Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show chassis compatibility-mode	7-2
set chassis compatibility-mode	7-3
clear chassis compatibility-mode	7-5
set ip interface	7-5
clear ip interface	7-6
set ip address	7-6
clear ip address	7-7
show system	7-8
show system hardware	7-9
show system utilization	7-11
set system utilization threshold	7-13
clear system utilization	7-13
show time	7-14
set time	7-14
show summertime	7-15
set summertime	7-15
set summertime date	7-16
set summertime recurring	7-17
clear summertime	7-18
set system name	7-18

For information about...	Refer to page...
set system location	7-19
set system contact	7-19
show mtu	7-20
set mtu	7-20
clear mtu	7-21
show reset	7-21
reset	7-22
reset nemcpu	7-22
reset at	7-23
reset in	7-24
clear config	7-24
show support	7-25
show physical alias	7-26
set physical alias	7-27
clear physical alias	7-28
show physical assetid	7-29
set physical assetid	7-30
clear physical assetid	7-30

show chassis compatibility-mode

Use this command to display compatibility mode configuration information and capabilities.

Syntax

show chassis compatibility-mode [**chassis-index** *chassis-idex*] [**capabilities**]

Parameters

chassis-index *chassis-index*	(Optional) Specifies the chassis index. Valid values are 1 - 2. Default value is 1. A chassis index of 2 can occur in a virtual switch bonding (VSB) context.
capabilities	(Optional) Displays the compatibility mode to which each installed module in the system can be set.

Defaults

- The default chassis index is **1**.
- If **capabilities** is not specified, compatibility mode settings are displayed.

Mode

All command modes.

Examples

This example displays compatibility settings for a system that is administratively set to **auto** and is operationally in **v1** compatibility mode:

```
S Chassis(rw)->show chassis compatibility-mode
Chassis Index:                              1
Current Fabric Compatibility Admin Mode:    auto
Current Fabric Compatibility Oper Mode:     v1
```

This example displays compatibility settings for a chassis index **2** system that is administratively set to **v2** and is operationally in **v2** compatibility mode:

```
S Chassis(rw)->set chassis compatibility-mode v2 chassis-index 2
S Chassis(rw)->show chassis compatibility-mode chassis-index 2
Chassis Index:                              2
Current Fabric Compatibility Admin Mode:    v2
Current Fabric Compatibility Oper Mode:     v2
```

set chassis compatibility-mode

Use this command to set the S-Series chassis module compatibility mode.

Syntax

set chassis compatibility-mode {**auto** | **v1** | **v2**} [**chassis-index** *chassis-idex*]

Parameters

auto	Specifies that the appropriate compatibility mode is actively auto detected in a default (cleared configuration) system boot context and persists on subsequent reboots.
v1	Specifies that the fabric compatibility mode is forced to be compatible with the presence of S-Series S130, S150, and S155 modules.
v2	Specifies that the fabric compatibility mode is forced to be compatible only with S-Series S140 and S180 modules.
chassis-index *chassis-index*	(Optional) Specifies the chassis index. Valid values are 1 - 2. Default value is 1. A chassis index of 2 can occur in a virtual switch bonding (VSB) context.

Defaults

- The default fabric compatibility mode is **auto**.
- The default chassis index is **1**.

Mode

All command modes.

Usage

There are currently two S-Series fabric module versions available. The older version exists on the S-Series S130, S150, and S155 modules. The newer version exists on the S-Series S140 and S180 modules. The two S-Series fabric versions are not compatible. Older and newer fabric modules can

not be installed in a mixed configuration on the same system. You can mix older and newer I/O modules in the same chassis, but if a newer I/O module exists in the chassis, only newer (S140 and S180) fabric modules can be installed in that chassis.

There are two exception to mixing older and newer I/O modules in the same chassis:

- You can not mix S130 and S140 I/O modules in an S3 chassis
- Older I/O modules can not be used in VSB configurations using dedicated VSB hardware interconnect ports (Refer to "set bonding mode" on page 18-11 for VSB hardware interconnect mode details).

Once older and newer S-Series module restrictions are met, you must assure that an appropriate compatibility mode is configured for the system. There are three compatibility mode settings: **auto**, **v1**, and **v2**.

When configured, the **auto** fabric compatibility mode actively determines the appropriate V1 or V2 setting for the system only when booting in a cleared (default) configuration state. Based upon the hardware installed at boot time, the appropriate fabric compatibility mode is operationally set and persists across subsequent system boots. If subsequent hardware changes occur requiring a module compatibility mode change, unless the configuration has been cleared, the module compatibility mode does not get changed, and any new hardware not appropriate to the current operational compatibility mode remains non-operational upon system boot. If changes that are not compatible with the current configuration occur subsequent to an initial auto compatibility mode bott, the appropriate **v1** or **v2** compatibility mode must be administratively entered or system configuration must be cleared for all hardware to be operational upon reboot.

Note: Chassis compatibility mode defaults to **auto**. You do not need to modify this default setting so long as you either do not modify the module configuration in the chassis or the modification of the module configuration is appropriate to the current operational chassis compatibility mode. The operational chassis compatibility mode is displayed in the **show chassis compatibility-mode** command output.

V1 compatibility mode is specified for chassis that have only older version modules installed or for chassis with supported mixed version modules installed.

V2 compatibility mode is specified for chassis that have only newer version modules. Should an older version module be present when the operational compatibility mode is set to v2, the older version modules will not become active.

Note: When administratively changing the compatibility mode to a mode that will change the current operational compatibility mode an appropriate warning displays and the system resets.

Refer to the Chassis Compatibility Mode section of the *Extreme Networks S-Series Configuration Guide* System Configuration chapter for a more detailed discussion of chassis compatibility mode.

Examples

This example shows how to set the chassis compatibility mode for chassis index 1 with a mixed configuration to **auto**:

```
S Chassis(rw)->set chassis compatibility-mode auto
S Chassis(rw)->show chassis compatibility-mode chassis-index 1
Chassis Index:                              1
Current Fabric Compatibility Admin Mode:    auto
Current Fabric Compatibility Oper Mode:     v1
```

This example shows how to set the chassis compatibility mode for chassis index 2 containing all S180 modules to v2:

```
S Chassis(rw)->set chassis compatibility-mode v2 chassis-index 2
S Chassis(rw)->show chassis compatibility-mode chassis-index 2
Chassis Index:                              2
Current Fabric Compatibility Admin Mode:    v2
Current Fabric Compatibility Oper Mode:     v2
```

clear chassis compatibility-mode

Use this command to reset the compatibility mode to the default value.

Syntax

clear chassis compatibility-mode [**chassis-index** *chassis-index*]

Parameters

chassis-index *chassis-index*	(Optional) Specifies that index value of the chassis. Valid values are **1** - **2**. Default value is **1**.

Defaults

If chassis-index is not specified, the compatibility mode for chassis index **1** is cleared.

Mode

All command modes.

Example

This example shows how to reset the compatibility mode for chassis index 2 to the default value of **auto**:

```
S Chassis(rw)->clear chassis compatibility-mode chassis-index 2
```

set ip interface

Use this command to set IP non-routing interfaces and optionally set it as the default for this system.

Syntax

set ip interface *interface-name* [**default**]

Parameters

interface-name	Sets the name of an IP interface.
default	(Optional) Sets this IP interface as the default management interface.

Defaults

None.

Mode

All command modes.

Usage

This command is used to create a non-routing IP interface. Non-routing IP interfaces can also be created using "set ip address" on page 7-6. This command is the only command that allows you to set the IP interface as the default for this system.

Example

This example shows how to set VLAN 5 as the default management IP interface:

```
S Chassis(rw)->set ip interface vlan.0.5 default
```

clear ip interface

Use this command to clear the IP interface.

Syntax

clear ip interface *interface-name*

Parameters

interface-name	The name of an IP interface.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear an IP interface:

```
S Chassis(rw)->clear ip interface vlan.0.5
```

set ip address

Use this command to set the IP address, subnet mask and default gateway for a non-routing IP interface.

Syntax

set ip address *ip_address* [**mask** *ip_mask*] [**gateway** *ip_gateway*] [**interface** *interface-name*]

Parameters

ip_address	Specifies the IPv4 or IPv6 address for a non-routing IP interface.
mask *ip_mask*	(Optional) Sets the system's subnet mask.
gateway *ip_gateway*	(Optional) Sets the IPv4 or IPv6 address of the system's default gateway (next-hop device).
interface *interface-name*	(Optional) Sets the IP interface for this system.

Defaults

- If not specified, *ip-mask* will be set to the natural mask of the *ip-address* and *ip-gateway* will be set to the *ip-address*.
- If not specified, the first IP interface configured on a system becomes the default IP interface.

Mode

All command modes.

Usage

In a multiple IP interface configuration the explicit setting of the interface is required. The specifying of the interface creates the interface if it does not already exist.

Example

This example shows how to set the system IP address to 10.1.10.1 with a mask of 255.255.128.0 and a default gateway of 10.1.0.1:

```
S Chassis(rw)->set ip address 10.1.10.1 interface vlan.0.5 mask 255.255.128.0
gateway 10.1.10.1
```

This example shows how to set the system IPv6 address to 2001:11ac:dcaa::/48 and a default gateway of 2001:11ac:dcaa::5 on interface VLAN 50:

```
S Chassis(rw)->set ip address 2001:11ac:dcaa::/48 v6_gateway 2001:11ac:dcaa::5
interface vlan.0.50
```

clear ip address

Use this command to clear an IP address assigned to a non-forwarding IP interface.

Syntax

clear ip address *ip-address*

Parameters

ip_address	Specifies the IPv4 or IPv6 address to clear.

Defaults

None.

Mode

All command modes.

Usage

You must clear the IP interface associated with this IP address using the **clear ip interface** command.

Example

This example shows how to clear IP address 125.10.0.1:

```
S Chassis(rw)->clear ip address 125.10.0.1
```

show system

Use this command to display system information, including contact information, power and fan tray status and uptime.

Syntax

show system

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display system information:

```
S Chassis(su)->show system
System contact:  daveh
System location: 3rd Floor North Cold Room
System name:     daveh-s-ac

PS1-Status       PS2-Status       PS3-Status       PS4-Status
---------------  ---------------  ---------------  ---------------
ok               not installed    not installed    not installed

PS1-Type         PS2-Type         PS3-Type         PS4-Type
---------------  ---------------  ---------------  ---------------
S-AC-PS          not installed    not installed    not installed

Fan-Status (flt=faulty, n/i=not installed, n/a=not available, unk=unknown)
-------------------------------------------------------------------------
1
---
ok

Temp-Alarm       Uptime d,h:m:s   Logout
---------------  ---------------  -------------
off                   0,04:53:45  10 min
```

Table 7-1 provides an explanation of the command output.

Table 7-1 Show System Output Display

Output...	What it displays...
System contact	Contact person for the system. Default of a blank string can be changed with the **set system contact** command (“set system contact” on page 7-19).
System location	Where the system is located. Default of a blank string can be changed with the **set system location** command (“set system location” on page 7-19).
System name	Name identifying the system. Default of a blank string can be changed with the **set system name** command (“set system name” on page 7-18).
PS1 and PS2-Status	Operational status for power supply 1 and, if installed, power supply 2.
Fan Status	Operational status of the fan tray.
Temp-Alarm	Whether or not the system temperature alarm is off (within normal temperature range) or on.
Uptime d,h:m:s	System uptime.
Logout	Time an idle console or Telnet CLI session will remain connected before timing out. Default of 15 minutes can be changed with the **set logout** command (“set mtu” on page 7-20).
PS1 and PS2-Type	Model number of power supply 1 and, if installed, power supply 2.

show system hardware

Use this command to display the system’s hardware configuration.

Syntax

```
show system hardware
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

The following example shows a portion of the information displayed with the **show system hardware** command.

Note: Depending on the hardware configuration of your S-Series system, your output will vary from the example shown.

```
S Chassis(su)->show system hardware
```

```
CHASSIS HARDWARE INFORMATION
----------------------------

   Chassis Type:               S-Series Standalone (SSA)
   Chassis Serial Number:      094454536352
   Chassis Power Supply 1:     Installed & Operating, AC High Power, Not Redundant
   Chassis Power Supply 2:     Not Installed
   Chassis Fan 1:              Installed & Operating
   Chassis Fan 2:              Installed & Operating
   Chassis Fan 3:              Installed & Operating
   Chassis Fan 4:              Installed & Operating
   Chassis Fan 5:              Installed & Operating
   Chassis Fan 6:              Installed & Operating
   Chassis Fan 7:              Installed & Operating
   Chassis Fan 8:              Installed & Operating
   Chassis Fan 9:              Installed & Operating
   Chassis Fan 10:             Installed & Operating
   Chassis Fan 11:             Installed & Operating
   Chassis Fan 12:             Installed & Operating
   Chassis Fan 13:             Installed & Operating
   PoE Power Supply 1:         Installed & Operating
   PoE Power Supply 2:         Not Installed

SLOT HARDWARE INFORMATION
-------------------------

   SLOT 1
      Model:                   SSA-T4068-0252
      Part Number:             9404332
      Serial Number:           094454536352
      Vendor ID:               1
      Base MAC Address:        00-1F-45-5B-F5-CF
      MAC Address Count:       54
      Hardware Version:        1
      Firmware Version:        07.11.01.0011.daveh4BFD5B25
      BootCode Version:        01.00.21x
      BootPROM Version:        01.01.05
      CPU Version:             28674 (PPC 750GX)
      SDRAM:                   1024 MB
      NVRAM:                   32  KB
      Flash System:            1024 MB
         /flash0 free space:   37  MB
         /flash1 free space:   62  MB
         /flash2 free space:   803 MB
```

```
      Temperature:
         LM75:                33.500  C
      Dip Switch Bank         1    2    3    4    5    6    7    8
         Position:            OFF  OFF  OFF  OFF  OFF  OFF  OFF  OFF
      HOST CHIP:
         Type:                FPGA
         Revision:            839   (0x347)
      FABRIC ACCESS PROC CHIP:
         FAP CHIP [0]:        FAP21V Revision A
         FAP CHIP [2]:        FAP21V Revision A
      FABRIC ELEMENT CHIP:
         FEs:                 Not present
      PLD CHIP:
         Revision:            3     (0x3)
      NIM[0]:
         Location:            lower left
         Model:               48 Port 10/100/1000 RJ45, 4X, Quad-Wide Bottom,
PoE+ Capable
         Board Revision:      5     (0x5)
         PLD Revision:        5     (0x5)
         FRU:                 no
         PoE[0]:
            Software Revision: 04.00.01.02
            Device Id:        0xe103
         SWITCH CHIP[0]:
            Type:             ASIC
            Revision:         0    (0x0)
            Id:               0
.
.
.
S Chassis(su)->
```

show system utilization

Use this command to display system resource utilization information.

Syntax

show system utilization [**cpu** | **process** | **storage**] [**slot** *slot*]

Parameters

cpu | **process** | **storage**	(Optional) Displays total CPU, individual process, or storage resource utilization only.
slot *slot*	(Optional) Displays system resource utilization for a specific module.

Defaults

- If not specified, CPU, process, and storage system utilization information will be displayed.
- If **slot** is not specified, information for all modules will be displayed.

Mode

All command modes.

Example

This example shows how to display all system utilization information for this device:

```
S Chassis(su)->show system utilization
CPU Utilization Threshold Traps enabled: Threshold = 80.0%
Total CPU Utilization:
Slot    CPU                5 sec   1 min   5 min
-----------------------------------------------------
 1      1                  39.8%    6.9%   18.5%

Process Utilization:
Slot: 1 CPU: 1

Name                           ProcID 5 sec   1 min   5 min
-------------------------------------------------------------
 ARP / ND                       1        0.0%    0.0%    0.0%
 CLI                            2        0.0%    0.0%    0.0%
 Chassis Data Synchronization   3        0.0%    0.0%    0.0%
 Connection Maintenance         4        0.0%    0.8%    0.8%
 External System Monitor        5        0.0%    0.0%    0.0%
 Hardware Maintenance           6       39.0%    5.6%    5.6%
 Hardware Reframer              7        0.0%    0.0%    0.0%
 Image & Config Management      8        0.0%    0.0%    0.0%
 Interrupts                     9        0.0%    0.0%    0.1%
.
.
.
 Switch STP                     43       0.1%    0.1%    0.1%
 Switch UPN                     44       0.0%    0.0%    0.0%
 Switch Web Server              45       0.0%    0.0%    0.0%
 Syslog                         46       0.0%    0.0%    0.0%
 OTHER                          47       0.0%    0.0%    0.1%
 IDLE                           48      99.1%   93.0%   82.4%

Storage Utilization:

Slot: 1
```

```
Type        Description               Size (Kb)      Available (Kb)
-------------------------------------------------------------------
 RAM        RAM device 1               1048576              636666
 Flash      Images                       65536               35164
 Flash      Nonvolatile Data Storage     65536               63384
 Flash      Miscellaneous Storage       824320              819600
```

set system utilization threshold

Use this command to set the threshold for sending CPU utilization notification messages.

Syntax

set system utilization threshold *threshold*

Parameters

threshold	Specifies a threshold value (in 1/10 of a percent).Valid range is **0–1000**. A value of **0** will disable utilization notification messages. Default value: 800 (80%).

Defaults

None.

Mode

All command modes.

Usage

The value range is 0–1000 and represents the percentage of system utilization to use as the trap threshold.

Example

This example shows how to set the system utilization threshold to 90%:

```
S Chassis(rw)->set system utilization threshold 900
```

clear system utilization

Use this command to clear the threshold for sending CPU utilization notification messages.

Syntax

clear system utilization

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

Using this command sets system utilization notifications to the factory default threshold of 80%.

Example

This example shows how to clear the system utilization threshold:

```
S Chassis(rw)->clear system utilization
```

show time

Use this command to display the current time of day in the system clock.

Syntax

show time

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the current time. The output shows the day of the week, month, day, and the time of day in hours, minutes, and seconds and the year:

```
S Chassis(su)->show time
TUE JUL 28 08:33:59 2009
```

set time

Use this command to change the time of day on the system clock.

Syntax

set time [*mm/dd/yyyy*] [*hh:mm:ss*]

Parameters

[*mm/dd/yyyy*] [*hh:mm:ss*]	Sets the time in: month, day, year and/or 24-hour format. At least one set of time parameters must be entered.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the system clock to 7:50 a.m:

```
S Chassis(rw)->set time 7:50:00
```

show summertime

Use this command to display daylight savings time settings.

Syntax

show summertime

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display daylight savings time settings:

```
S Chassis(su)->show summertime

Summertime is enabled and set to ''
Start : SUN MAR 08 02:00:00 2009
End   : SUN NOV 01 02:00:00 2009
Offset: 60 minutes (1 hours 0 minutes)
Recurring: yes, starting at 2:00 of the second Sunday of March and ending at 2:0
0 of the first Sunday of November
```

set summertime

Use this command to enable or disable the daylight savings time function.

Syntax

set summertime {**enable** | **disable**} [*zone*]

Parameters

enable | **disable**	Enables or disables the daylight savings time function.
zone	(Optional) Applies a name to the daylight savings time settings.

Defaults

If a zone name is not specified, none will be applied.

Mode

All command modes.

Example

This example shows how to enable daylight savings time function:

```
S Chassis(rw)->set summertime enable
```

set summertime date

Use this command to configure specific dates to start and stop daylight savings time.

Syntax

set summertime date *start_month start_date start_year start_hr_min end_month end_date end_year end_hr_min* [*offset_minutes*]

Parameters

start_month	Specifies the month of the year to start daylight savings time.
start_date	Specifies the day of the month to start daylight savings time.
start_year	Specifies the year to start daylight savings time.
start_hr_min	Specifies the time of day to start daylight savings time. Format is hh:mm.
end_month	Specifies the month of the year to end daylight savings time.
end_date	Specifies the day of the month to end daylight savings time.
end_year	Specifies the year to end daylight savings time.
end_hr_min	Specifies the time of day to end daylight savings time. Format is hh:mm.
offset_minutes	(Optional) Specifies the amount of time in minutes to offset daylight savings time from the non-daylight savings time system setting. Valid values are **1–1440**.

Defaults

If an *offset* is not specified, none will be applied.

Mode

All command modes.

Usage

These settings will be non-recurring and will have to be reset annually.

Example

This example shows how to set a daylight savings time start date of March 8, 2009 at 2 a.m. and an ending date of November 1, 2009 at 2 a.m. with an offset time of one hour:

```
S Chassis(rw)->set summertime date March 8 2009 02:00 November 1 2009 02:00 60
```

set summertime recurring

Use this command to configure recurring daylight savings time settings.

Syntax

set summertime recurring *start_week start_day start_month start_hr_min end_week end_day end_month end_hr_min* [*offset_minutes*]

Parameters

start_week	Specifies the week of the month to restart daylight savings time. Valid values are: **first**, **second**, **third**, **fourth**, and **last**.
start_day	Specifies the day of the week to restart daylight savings time.
start_month	Specifies the month to restart daylight saving time.
start_hr_min	Specifies the time of day to restart daylight savings time. Format is hh:mm.
end_week	Specifies the week of the month to end daylight savings time.
end_day	Specifies the day of the week to end daylight savings time.
end_month	Specifies the month to end daylight saving time.
end_hr_min	Specifies the time of day to end daylight savings time. Format is hh:mm.
offset_minutes	(Optional) Specifies the amount of time in minutes to offset daylight savings time from the non-daylight savings time system setting. Valid values are **1–1440**.

Defaults

If an *offset* is not specified, none will be applied.

Mode

All command modes.

Usage

These settings will start and stop daylight savings time at the specified day of the month and hour each year and will not have to be reset annually.

Example

This example shows how to set daylight savings time to recur starting on the second Sunday of March at 2 a.m. and an ending on the first Sunday in November at 2 a.m. with an offset time of one hour:

```
S Chassis(rw)->set summertime recurring second Sunday March 02:00 first Sunday
November 02:00 60
```

clear summertime

Use this command to clear the daylight savings time configuration.

Syntax

```
clear summertime
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear the daylight savings time configuration:

```
S Chassis(rw)->clear summertime
```

set system name

Use this command to configure a name for the system.

Syntax

set system name [*string*]

Parameters

string	(Optional) Specifies a text string that identifies the system. A text string containing one or more spaces must be enclosed in quotes as shown in the example below.

Defaults

If *string* is not specified, the system name will be cleared.

Mode

All command modes.

Example

This example shows how to set the system name to Information Systems:

```
S Chassis(rw)->set system name "Information Systems"
```

set system location

Use this command to identify the location of the system.

Syntax

set system location [*string*]

Parameters

string	(Optional) Specifies a text string that indicates where the system is located. A text string containing one or more spaces must be enclosed in quotes as shown in the example below.

Defaults

If *string* is not specified, the location name will be cleared.

Mode

All command modes.

Example

This example shows how to set the system location string:

```
S Chassis(rw)->set system location "Bldg N32-04 Closet 9"
```

set system contact

Use this command to identify a contact person for the system.

Syntax

set system contact [*string*]

Parameters

string	(Optional) Specifies a text string that contains the name of the person to contact for system administration. A text string containing one or more spaces must be enclosed in quotes as shown in the example below.

Defaults

If *string* is not specified, the contact name will be cleared.

Mode

All command modes.

Example

This example shows how to set the system contact string:

```
S Chassis(rw)->set system contact "Joe Smith"
```

show mtu

Use this command to display the status of the path MTU discovery protocol on the device.

Syntax

show mtu

Parameters

None.

Defaults

None.

Mode

All command modes, Read-Only.

Example

This example shows how to display path MTU discovery status:

```
S Chassis(rw)->show mtu
MTU discovery status: Enabled
```

set mtu

Use this command to disable or enable path MTU discovery protocol on the device.

Syntax

set mtu {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables path MTU discovery protocol.

Defaults

None.

Mode

All command modes.

Example

This example shows how to disable path MTU discovery:

```
S Chassis(rw)->set mtu disable
```

clear mtu

Use this command to reset the state of the path MTU discovery protocol back to enabled.

Syntax

clear mtu

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the state of MTU discovery:

```
S Chassis(rw)->clear mtu
```

show reset

Use this command to display information about scheduled device resets.

Syntax

show reset

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This command shows how to display reset information:

```
S Chassis(rw)->show reset


Reset scheduled for Fri Jan 23 2009, 23:00:00 (in 3 days 12 hours 56 minutes 57
seconds).
Reset reason: Software upgrade
```

reset

Use this command to reset the device without losing any user-defined configuration settings.

Syntax

reset {*module* | **system** | **cancel**}

Parameters

module	Specifies a module to be reset.
system	Resets the system upon confirming the reset in the CLI.
cancel	Cancels a reset scheduled using the **reset at** command as described in "reset at" on page 7-23, or the **reset in** command as described in "reset in" on page 7-24.

Defaults

None. You must enter one of the specified parameters.

Mode

All command modes.

Usage

An S-Series module or the Standalone chassis can also be reset with the RESET button located on its front panel. For information on how to do this, refer to the *Hardware Installation Guide* shipped with your device.

If a **reset** command is issued while an HA upgrade is pending, the HAU process will start.

Examples

This example shows how to reset the system.

```
S Chassis(rw)->reset system
 This command will reset the system and may disconnect your telnet session.
 Do you want to continue (y/n) [n]? y

 Resetting...
```

This example shows how to cancel a scheduled system reset:

```
S Chassis(rw)->reset cancel

Reset cancelled.
```

reset nemcpu

Use this command to reset an option module CPU.

Syntax

reset nemcpu *mod.nemcpu*

Parameters

mod.nemcpu	Resets the CPU on an option module, where *mod* specifies the module in which the option module is installed and *nemcpu* specifies the location of the option module. Currently, this value can only be 1.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset an option module installed on the module in slot 4.

```
S Chassis(rw)->reset nemcpu 4.1
This command will reset NEM CPU 4.1.
Do you want to continue (y/n) [n]? y
Resetting NEM CPU 4.1 ...
```

reset at

Use this command to schedule a system reset at a specific future time. This feature is useful for loading a new boot image.

Syntax

reset at *hh:mm* [*mm/dd*] [*reason*]

Parameters

hh:mm	Schedules the hour and minute of the reset (using the 24-hour system).
mm/dd	(Optional) Schedules the month and day of the reset.
reason	(Optional) Specifies a text string that indicates the reason for the reset.

Defaults

- If month and day are not specified, the reset will be scheduled for the first occurrence of the specified time.
- If a reason is not specified, none will be applied.

Mode

All command modes.

Examples

This example shows how to schedule a reset at 8 p.m. on January 10:

```
S Chassis(rw)->reset at 20:00 01/10
Reset scheduled at 20:00:00, Sat Jan 10 2009
Proceed with scheduled reset? (y/n) [n]? y
```

```
Reset scheduled for 20:00:00, Sat Jan 10 2009 (in 1 day 5 hours 40 minutes
```

This example shows how to schedule a reset at a specific future time and include a reason for the reset:

```
S Chassis(rw)->reset at 20:00 01/10 Software upgrade
Reset scheduled at 20:00:00, Sat Jan 10 2009
Reset reason: Software upgrade
Proceed with scheduled reset? (y/n) [n]? y
Reset scheduled for 20:00:00, Sat Jan 10 2009 (in 1 day 5 hours 40 minutes
```

reset in

Use this command to schedule a system reset after a specific time. This feature is useful for loading a new boot image.

Syntax

reset in *hh:mm* [*reason*]

Parameters

hh:mm	Specifies the number of hours and minutes into the future to perform a reset.
reason	(Optional) Specifies a reason for the reset

Defaults

If a *reason* is not specified, none will be applied.

Mode

All command modes.

Example

This example shows how to schedule a device reset in 5 hours and 20 minutes:

```
S Chassis(rw)->reset in 5:20
Reset scheduled in 5 hours and 20 minutes
Proceed with scheduled reset? (y/n) [n]? y
Reset scheduled for 19:56:01, Fri Dec 19 2008 (in 5 hours 20 minutes
```

clear config

Use this command to clear the user-defined switch and router configuration parameters for one or more modules.

Syntax

clear config {*mod_num* | **all** | **restore-point** *index*}

Parameters

mod_num | **all**	Clears configuration parameters in a specific module or in all modules.
restore-point *index*	Clears the restore point for the specified index.

Defaults

None.

Mode

All command modes.

Usage

Executing clear config on one or all Extreme Networks S-Series module resets that module back to its factory defaults. If that module is in a chassis with other active modules, it will inherit system settings from the system.

Example

This example shows how to clear configuration parameters in all modules:

```
S Chassis(rw)->clear config all
```

show support

Use this command to display output for technical support-related commands.

Syntax

show support [*filename*]

Parameters

filename	(Optional) The name of the file (entered at the command line in the format slotN/name) in which the show output will be saved.

Defaults

The following commands are executed:

- show version
- show system hardware
- show vlan
- show vlan static
- show logging all
- show snmp counters
- show port status
- show spantree status
- show spantree blockedports
- show ip route

- show netstat
- show arp
- show system utilization
- show config

Mode

All command modes.

Usage

If C2 security mode is enabled, the **show support** command can not be accessed while in Read-Write or Read-Only user modes.

Example

This example shows how to execute the **show support** command and save the results to slot 1 as a file named support3.txt:

```
S Chassis(su)->show support slot1/support3.txt
Writing output to file..................
Writing 'show config' output.....
Writing Message Log output.......
S Chassis(su)->
```

show physical alias

Use this command to display the alias, a text name, for one or more physical objects in the system.

Syntax

show physical alias [**chassis** *chassis* | **slot** *slot* | **backplane** *backplane* | **module** *module* | **sub-module** *slot module* | **powersupply** *powersupply* | **powersupply-slot** *powersupply-slot* | **fan** | **fan-slot** | **port** *port-string*]

Parameters

chassis *chassis*	(Optional) Displays the alias set for the chassis.
slot *slot*	(Optional) Displays the alias set for a specified slot in the chassis.
backplane *backplane*	(Optional) Displays the alias set for the backplane. Valid values are **1** for FTM 1 and **2** for FTM 2.
module *module*	(Optional) Displays the alias set for a specified module. A maximum of one module alias per slot is allowed.
sub-module *slot module*	Specifies the sub-module installed in its parent module expansion slot for which to display an alias. *slot* specifies the chassis slot the parent module is installed in. *module* specifies the sub-module ID.
powersupply *powersupply*	(Optional) Displays the alias set for a specified power supply. Valid values are **1** or **2**.
powersupply-slot *powersupply-slot*	(Optional) Displays an alias set for a specific power supply slot.
fan	(Optional) Displays the alias set for the fan tray.

fan-slot	(Optional) Displays an alias for the fan tray's slot.
port *port-string*	(Optional) Displays the alias set for a specified *port-string*. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.

Defaults

If no parameters are specified, all physical alias information will be displayed.

Mode

All command modes.

Example

This example shows how to display physical alias information for the chassis. In this case, the chassis entity is 1 and there is no alias currently set for the chassis:

```
S Chassis(rw)->show physical alias chassis
chassis-1           alias=<empty string> entity=1
S Chassis(rw)->
```

set physical alias

Use this command to set the alias, a text name, for a physical object.

Syntax

set physical alias {**chassis** *chassis* | **slot** *slot* | **backplane** *backplane* | **module** *module* | **sub-module** *slot module* | **powersupply** *powersupply* | **powersupply-slot** *powersupply-slot* | **fan** | **fan-slot** | **port** *port-string*} [*string*]

Parameters

chassis *chassis*	Sets an alias for the chassis.
slot *slot*	Sets an alias for a specific slot in the chassis.
backplane *backplane*	Sets an alias for the backplane. Valid values are **1** for FTM 1 and **2** for FTM 2.
module *module*	Sets an alias for a specific module. A maximum of one module per slot is allowed.
sub-module *slot module*	Specifies the sub-module installed in its parent module expansion slot for which to set an alias. *slot* specifies the chassis slot the parent module is installed in. *module* specifies the sub-module ID.
powersupply *powersupply*	Sets an alias for a specific power supply. Valid values are **1** or **2**.
powersupply-slot *powersupply-slot*	Sets an alias for a specific power supply slot.
fan	Sets an alias for the fan tray.
fan-slot	Sets an alias for the fan tray's slot.

port *port-string*	Sets an alias for a specific port. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.
string	(Optional) Assigns a text string alias to the specified physical object.

Defaults

If *string* is not specified, the alias of the type specified will be cleared.

Mode

All command modes.

Example

This example shows how to set the alias for the chassis to "chassisone":

```
S Chassis(rw)->set physical alias chassis chassisone
S Chassis(rw)->
```

clear physical alias

Use this command to reset the alias for a physical object to a zero-length string.

Syntax

clear physical alias {[**chassis** *chassis*] [**slot** *slot*] [**backplane** *backplane*] [**module** *module*] **sub-module** *slot module* | [**powersupply** *powersupply*] [**powersupply-slot** *powersupply-slot*] [**fan**] [**fan-slot**] [**port** *port-string*]}

Parameters

chassis *chassis*	Clears the chassis alias.
slot *slot*	Clears and alias for a specific slot.
backplane *backplane*	Clears and alias for a specific backplane. Valid values are **1** for FTM 1 and **2** for FTM 2.
module *module*	Clears an alias for a specific module.
powersupply *powersupply*	Clears an alias for a specific power supply. Valid values are **1** or **2**.
sub-module *slot module*	Specifies the sub-module installed in its parent module expansion slot for which to clear an alias. *slot* specifies the chassis slot the parent module is installed in. *module* specifies the sub-module ID.
fan	Clears the fan tray alias
port *port-string*	Clears an alias for a specific port. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set clear the alias set for the chassis:

```
S Chassis(rw)->clear physical alias chassis
S Chassis(rw)->
```

show physical assetid

Use this command to display the asset ID for a module.

Syntax

show physical assetid {**chassis** *chassis* | **module** *module* | **sub-module** *slot module* | **powersupply** *powersupply* | **poe-powersupply** *poe-powersupply* | **fan** *fan*}

Parameters

chassis *chassis*	Specifies the display of the chassis asset ID.
module *module*	Specifies the module for which to display the asset ID.
sub-module *slot module*	Specifies the sub-module installed in its parent module expansion slot for which to display an asset ID. *slot* specifies the chassis slot the parent module is installed in. *module* specifies the sub-module ID.
powersupply *powersupply*	Specifies the power supply for which to display the asset ID.
poe-powersupply *poe-powersupply*	Specifies the POE power supply for which to display the asset ID.
fan *fan*	Specifies the fan for which to display the asset ID.

Defaults

None.

Mode

All command modes.

Example

This example sets the **module 1** asset ID to **documentation** and shows how to display asset ID information for module 1:

```
S Chassis(rw)->set physical assetid module 1 documentation
S Chassis(rw)->show physical assetid module 1

Name                    AssetId                              Index
----------------------- -------------------------------- ----------
module-1                documentation                     10011001
S Chassis(rw)->
```

set physical assetid

Use this command to set the asset ID for a module.

Syntax

set physical assetid {**chassis** *chassis* | **module** *module* | **sub-module** *slot module* | **powersupply** *powersupply* | **poe-powersupply** *poe-powersupply* | **fan** *fan*} *string*

Parameters

chassis *chassis*	Sets an asset ID for this chassis.
module *module*	Sets an asset ID for a specific module.
sub-module *slot module*	Sets an asset ID for the sub-module installed in its parent module expansion slot. *slot* specifies the chassis slot the parent module is installed in. *module* specifies the sub-module ID.
powersupply *powersupply*	Sets an asset ID for the specified power supply.
poe-powersupply *poe-powersupply*	Sets an asset ID for the specified POE power supply.
fan *fan*	Sets an asset ID for the specified fan.
string	Specifies the asset ID.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the asset ID information for module 1 to "mod1":

```
S Chassis(rw)->set physical assetid module 1 mod1
S Chassis(rw)->
```

clear physical assetid

Use this command to reset the asset ID for a module to a zero-length string.

Syntax

clear physical assetid {**chassis** *chassis* | **module** *module* | **sub-module** *slot module* | **powersupply** *powersupply* | **poe-powersupply** *poe-powersupply* | **fan** *fan*}

Parameters

chassis	Clears an asset ID for this chassis.
module *module*	Clears an asset ID for a specific module.
sub-module *slot module*	Clears an asset ID for the sub-module installed in its parent module expansion slot. *slot* specifies the chassis slot the parent module is installed in. *module* specifies the sub-module ID.

powersupply *powersupply*	Clears an asset ID for the specified power supply.
poe-powersupply *poe-powersupply*	Clears an asset ID for the specified POE power supply.
fan *fan*	Clears an asset ID for the specified fan.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear the asset ID for module 1:

```
S Chassis(rw)->clear physical assetid module 1
S Chassis(rw)->
```

8

MAC Address Commands

This chapter provides detailed information for the MAC address set of commands. For information about configuring MAC address commands, refer to the "System Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show port mac	8-1
show mac	8-2
show mac agetime	8-4
set mac	8-5
clear mac	8-6
show newaddrtrap	8-7
set newaddrtrap	8-7
show movedaddrtrap	8-8
set movedaddrtrap	8-9

show port mac

Use this command to display the MAC address(es) for one or more ports.

Syntax

show port mac [*port-string*]

Parameters

port-string	(Optional) Displays MAC addresses for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, MAC addresses for all ports will be displayed.

Mode

All command modes.

Usage

These are port MAC addresses programmed into the device during manufacturing. To show the MAC addresses learned on a port through the switching process, use the **show mac** command as described in "show mac" on page 8-2.

Example

This example shows how to display the MAC address for ge.2.4:

```
S Chassis(rw)->show port mac ge.2.4

Port            MAC Address
------------  ----------------------
ge.2.4        00-01-F4-DA-32-FE
```

show mac

Use this command to display MAC addresses in the switch's filtering database.

Syntax

show mac [**address** *mac-address*] [**fid** *fid*] [**vlan-id** *vlan-id*] [**port-string** *port-string*] [**type** {**other** | **invalid** | **learned** | **self** | **mgmt**}] [**field-decode**] [**unicast-as-multicast**] [**-verbose**]

Parameters

address *mac-address*	(Optional) Displays a specific MAC address (if it is known by the device).
fid *fid*	(Optional) Displays MAC addresses for a specific filter database identifier.
vlan-id *vlan-id*	(Optional) Displays MAC addresses for a specific VLAN based on the VLAN ID, for static multicast entries only.
port-string *port-string*	(Optional) Displays MAC addresses for a specific port or range of ports. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
type other | **invalid** | **learned** | **self** | **mgmt**	(Optional) Display MAC addresses defined as **other**, **invalid**, **learned**, **self** or **mgmt** (management).
field-decode	(Optional) Display the meanings of the fields in the **show mac** command.
unicast-as-multicast	(Optional) Display matches of unlearned destination MAC address against the static multicast MAC entries.
-verbose	(Optional) Displays all MAC address information in detail.

Defaults

If no parameters are specified, all MAC addresses for the device will be displayed.

Mode

All command modes.

Usage

These are addresses learned on a port through the switching process or statically entered. To show port MAC addresses programmed into the device during manufacturing, use the **show port mac** command as described in "show port mac" on page 8-1.

Example

This example shows how to display MAC address information for port ge.1.1 with the meanings of field codes displayed:

```
S Chassis(rw)->show mac field-decode fid 1 port-string ge.1.1 -verbose


 Blank    = Not applicable
 Type:
  other   = Entry is other than below
  invalid = Entry is no longer valid, but has not been yet flushed-out
  learned = Entry has been learned and is currently used
  self    = Entry represents one of the device's address
  mgmt    = Entry represents a dot1qStaticUnicastAddress
  mcast   = Entry represents a dot1qStaticMulticastAddress
 Status:
  other   = Entry is other than below
  invalid = Entry shall be removed
  perm    = Entry is currently in use and shall remain so AFTER the next reset
            (permanent)
MAC Address       FID  Port          Type    Status
----------------- ---- ------------- ------- -------
00-00-5E-00-01-01 1    ge.1.1        learned
00-01-F4-00-70-1A 1    ge.1.1        learned
00-01-F4-2C-01-13 1    ge.1.1        learned
00-01-F4-5B-5F-A7 1    ge.1.1        learned
00-01-F4-5D-96-B4 1    ge.1.1        learned
00-03-47-93-7A-57 1    ge.1.1        learned
00-04-5A-79-40-73 1    ge.1.1        learned
00-06-1B-D9-2B-A9 1    ge.1.1        learned
.
.
.
00-E0-63-86-2B-BE 1    ge.1.1        learned
00-E0-63-86-3E-4D 1    ge.1.1        learned
S Chassis(rw)->
```

Table 8-1 provides an explanation of the command output.

Table 8-1 show mac Output Details

Output...	What it displays...
MAC Address	MAC addresses mapped to the port(s) shown.
FID	Filter database identifier.
Port	Port designation.
Type	Address type. Valid types are: • other - entry is other than below • invalid - entry is no longer valid, but has not been yet flushed-out • learned - entry has been learned and is currently used • self - entry represents one of the device's address • mgmt - entry represents a dot1qStaticUnicastAddress (manually entered MAC address) • mcast - entry represents a dot1qStaticMulticastAddress
Status	Address status. Valid types are: • other - entry is other than below • invalid - entry shall be removed • perm - entry is currently in use and shall remain so AFTER the next reset (permanent)

show mac agetime

Use this command to display the timeout period for aging learned MAC addresses.

Syntax

```
show mac agetime
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to display the MAC address timeout period:

```
S Chassis(rw)->show mac agetime
Aging time: 300 seconds
```

set mac

Use this command to set the timeout period for aging learned MAC entries, to define what ports a multicast address can be dynamically learned on or flooded to, and to make a static entry into the filtering database(s).

Syntax

```
set mac [agetime time] | [multicast mac-address vlan-id [port-string] {append |
clear}] | [unicast mac-address fid receive-port [ageable]] [unicast-as-multicast
{enable | disable}] [max-entries {64K | 128K}]
```

Parameters

agetime *time*	Specifies the timeout period in seconds for aging learned MAC addresses. Valid values are **10** to **65535**. Default: 300 seconds.
multicast *mac-address vlan-id* [*port-string*] {**append** | **clear**}]	This command allows you to limit specific layer two multicast addresses (mac-address) to specific ports (port-string) within a VLAN (vlan-id). You can later come back and append or clear ports from the list of ports the multicast MAC address is allowed to be dynamically learned on or flooded to.
unicast *mac-address fid receive-port* [**ageable**]	This command allows you to statically enter a unicast MAC address (*mac-address*) into a filtering database (*fid*) for a single port (*receive-port*). This entry will be either permanent or **ageable** where it will age out same as a dynamically learned MAC address.
unicast-as-multicast {**enable** | **disable**}	(Optional) **enable** - Enables treating static unicast MAC address as a multicast address by extending the search phase of layer 2 lookup to match the unlearned destination MAC address against the static Multicast MAC entries. **disable** - Treats static unicast MAC addresses as unicast addresses.
max-entries {**64K** | **128K**}	(Optional) Specifies the maximum number of MAC entries for the device. Valid values are **64K** (up to 65536) or **128K** (up to 131072). The default value is **64K**.

Defaults

- If port-string is not defined with the **set mac multicast** command, then it will apply to all ports.
- If the **set mac unicast** command is used without the **ageable** parameter, the entry will be permanent.
- The maximum number of MAC entries defaults to 65536.

Mode

All command modes.

Usage

A warning displays if a unicast MAC address is entered as part of a multicast command:

```
S Chassis(rw)->set mac multicast 00-02-ca-bb-cc-dd 2 ge.1.5
Warning: Unicast address converted to multicast 01-02-CA-BB-CC-DD
```

Examples

This example shows how to set the MAC timeout period to 600 seconds:

```
S Chassis(rw)->set mac agetime 600
```

This example shows how to enable the MAC for unicast-as-multicast:

```
S Chassis(rw)->set mac unicast-as-multicast enable
```

clear mac

Use this command to reset the timeout period for aging learned MAC entries to the default value of 300 seconds, or to clear MAC addresses out of the filtering database(s).

Syntax

clear mac {[**all**] | [**address** *address*] [**fid** *fid*] | [**vlan-id** *vlan-id*] | [**port-string** *port-string*] [**type** {**learned** | **mgmt**}]} | [**agetime**] [**unicast-as-multicast**]

Parameters

all	Clear all MAC address entries. This will even clear permanent entries.
address *address*	MAC address to clear (ex. 00-01-F4-56-78-90); if not specified, clear command shall be scoped to all MAC address.
fid *fid*	Filtering database id to clear; if not specified, clear command shall be scoped to all filtering database ids.
vlan-id *vlan-id*	Specify a VLAN ID from which to clear the MAC address for static multicast entries only.
port-string *port-string*	Single port to clear (ex. ge.1.1); if not specified, clear command shall be scoped to all ports.
type {**learned** | **mgmt**}	Status type to clear; if not specified, clear command shall be scoped to all 'learned' and 'mgmt' entries where mgmt refers to all statically entered MAC addresses.
agetime	(Optional) Clear timeout period to default value of 300 seconds.
unicast-as-multicast	(Optional) The layer 2 lookup to attempt to match the unlearned destination MAC address against the static multicast MAC entries cleared.

Parameters

None.

Defaults

None, except those noted above.

Mode

All command modes.

Examples

This example shows how to clear the MAC timeout period:

```
S Chassis(rw)->clear mac agetime
```

This example shows how to clear all the MAC addresses associated with port ge.1.3:

```
S Chassis(rw)->clear mac port-string ge.1.3
```

show newaddrtrap

Use this command to display the status of MAC address traps on one or more ports.

Syntax

show newaddrtrap [*port-string*]

Parameters

port-string	(Optional) Displays MAC address traps for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, MAC address traps for all ports will be displayed.

Mode

All command modes.

Example

This example shows how to display the status of MAC address traps on ge.1.1 through 3:

```
S Chassis(rw)->show newaddrtrap
New Address Traps Globally disabled

Port        Enable State
--------- ------------
ge.1.1    disabled
ge.1.2    disabled
ge.1.3    disabled
```

set newaddrtrap

Use this command to enable or disable SNMP trap messaging, globally and on one or more ports, when new source MAC addresses are detected.

Syntax

set newaddrtrap [*port-string*] {**enable** | **disable**}

Parameters

port-string	(Optional) Specifies the port(s) on which to enable or disable MAC address traps. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
enable | **disable**	Enables or disables SNMP trap messaging when new source MAC addresses are detected.

Defaults

If *port-string* is not specified, MAC address traps will be globally enabled or disabled.

Mode

All command modes.

Usage

MAC address traps must be enabled both globally and on affected ports as two separate entries.

Example

This example shows how to enable MAC address traps on ports **ge.1.4-8**:

```
S Chassis(rw)->set newaddrtrap enable
S Chassis(rw)->set newaddrtrap ge.1.4-8 enable
```

show movedaddrtrap

Use this command to display the status of SNMP trap messaging on one or more ports.

Syntax

show movedaddrtrap [*port-string*]

Parameters

port-string	(Optional) Displays MAC address traps for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, moved MAC address traps for all ports will be displayed.

Mode

All command modes.

Example

This example shows how to display the status of moved MAC address traps on ge.1.1 through 3:

```
S Chassis(rw)->show movedaddrtrap ge.1.1-3
Moved Address Traps Globally enabled

Port        Enable State
--------- ------------
ge.1.1     enabled
ge.1.2     enabled
ge.1.3     enabled
```

set movedaddrtrap

Use this command to enable or disable SNMP trap messaging, globally and on one or more ports, when moved source MAC addresses are detected.

Syntax

set movedaddrtrap [*port-string*] {**enable** | **disable**}

Parameters

port-string	(Optional) Specifies the port(s) on which to enable or disable MAC address traps. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
enable | **disable**	Enables or disables SNMP trap messaging when moved source MAC addresses are detected.

Defaults

If *port-string* is not specified, moved MAC address traps will be globally enabled or disabled.

Mode

All command modes.

Usage

The SNMP trap messaging when moved source MAC addresses are detected feature must be enabled both globally and on affected ports as two separate entries.

Example

This example shows how to enable SNMP trap messaging on ports **ge.1.4-8**:

```
S Chassis(rw)->set movedaddrtrap enable
S Chassis(rw)->set movedaddrtrap ge.1.4-8 enable
```

9

Telnet Commands

This chapter provides detailed information for the Telnet set of commands. Telnet command functionality includes enabling or disabling Telnet and starting a Telnet session to a remote host. The S-Series device allows a total of four inbound and/or outbound Telnet sessions to run simultaneously. For information about configuring Telnet, refer to the "System Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show telnet	9-1
set telnet	9-2
telnet	9-2

show telnet

Use this command to display the status of Telnet on the device.

Syntax

show telnet

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display Telnet status:

```
S Chassis(rw)->show telnet

Telnet inbound is currently: ENABLED
Telnet outbound is currently: ENABLED
```

set telnet

Use this command to enable or disable Telnet on the device.

Syntax

set telnet {**enable** | **disable**} {**all** | **inbound** |**outbound**}

Parameters

enable | **disable**	Enables or disables Telnet services.
all	Enables or disables both inbound and outbound Telnet services.
inbound	Enables or disables the ability for another device to Telnet to this device.
outbound	Enables or disables ability to Telnet to other devices from this device.

Defaults

None.

Mode

All command modes.

Example

This example shows how to disable inbound and outbound Telnet services:

```
S Chassis(rw)->set telnet disable all
S Chassis(rw)->
```

telnet

Use this command to start a Telnet connection to a remote host. The S-Series device allows a total of four inbound and / or outbound Telnet session to run simultaneously.

Syntax

telnet [**-s** *src-addr*] [**-4**] [**-6**] [**-vrf** *router*] [**-r**] {*host* [*port*]}

Parameters

host	Specifies the host name or IP address of the remote host this Telnet session is connecting to.
port	(Optional) Specifies the host port to connect to on the remote host. Default value: **23**.
-s *src-addr*	(Optional) Specifies the IP address to transmit from when there are multiple interfaces and or addresses.
-4	(Optional) Specifies that this session only supports IPv4 addressing.
-6	(Optional) Specifies that this session only supports IPv6 addressing.
-vrf *router*	(Optional) Specifies the router on which to source this SSH session. Valid values: **default**.

-r	(Optional) Specifies that normal routing table lookup should be bypassed and that the session request should be sent directly to a host on an attached network.

Defaults

- If not specified, the host Telnet default *port* number 23 will be used.
- If **-s** not specified, the source IP address is chosen by the system based upon the chosen route to the destination.
- If **-4** or **-6** is not specified, both IPv4 and IPv6 addressing is supported in this session.
- If **-vrf** is not specified, the router is inherited from the CLI context. The **default** router is used by this session.
- If **-r** is not specified, the standard host routing tables will be used for this session.

Mode

All command modes.

Usage

Any desired options must be entered on the command line prior to specifying the remote host and its optional port.

The **-4** and **-6** flags are used when the host is a domain name as opposed to a IPv4 or IPv6 address. A DNS server may return multiple responses, some of which may be IPv4 addresses and some of which may be IPv6 addresses. If the returned address type matters, then these flags let you choose which type will be accepted.

The **-s** and **-r** options are both intended for when the route table is invalid for some reason and you are using Telnet to debug it.

Example

This example shows how to start a Telnet session to a host at 10.21.42.13:

```
S Chassis(rw)->telnet 10.21.42.13
```

10

Secure Shell (SSH) Commands

This chapter provides detailed information for the Secure Shell (SSH) set of commands. For information about configuring SSH, refer to the "System Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show ssh state	10-1
set ssh	10-3
set ssh ciphers	10-3
clear ssh ciphers	10-4
set ssh client alive-interval	10-5
set ssh client alive-count	10-5
clear ssh client	10-6
set ssh hostkey	10-7
set ssh macs	10-7
clear ssh macs	10-8
set ssh reinitialize	10-9
set ssh server allowed-auth	10-9
show ssh authkey	10-10
set ssh server authkey	10-11
clear ssh server authkey	10-12
set ssh server pki trusted-ca-list	10-12
set ssh server pki authorized-cert-list	10-13
ssh	10-14

show ssh state

Use this command to display the current status of SSH on the device.

Syntax

```
show ssh state
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display SSH state and host key type for the device:

```
S Chassis(rw)->show ssh state
SSH Server:
 State: Enabled
 Host key type: RSA
Allowed Ciphers List (default):
  aes128-cbc,aes192-cbc,aes256-cbc,3des-cbc,blowfish-cbc,cast128-cbc,
  rijndael-cbc@lysator.liu.se
 Allowed MACs List (default):
  hmac-sha1-etm@openssh.com,hmac-md5-etm@openssh.com,
  hmac-ripemd160-etm@openssh.com,hmac-sha1-96-etm@openssh.com,
  hmac-md5-96-etm@openssh.com,hmac-sha1,hmac-md5,hmac-ripemd160,
  hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
 Allowed Authentication Methods:
  password: enabled
  pubkey:   enabled
 PKI Trusted CA List: JITC_CA
 PKI Authorized Cert List:
 Authorized User Public Keys:
  Username         Type Bits Public Key
  ---------------- ---- ---- ----------------------------------------------------
  admin            RSA  2048 AAAAB3NzaC1yc2EAAAADAQABAAABAQ...1pDucBQyCxXHAVFWTB
  locoJoe          RSA  2048 AAAAB3NzaC1yc2EAAAADAQABAAABAQ...1pDucBQyCxXHAVFWTB
  newUser          RSA  2048 AAAAB3NzaC1yc2EAAAADAQABAAABAQ...+M7MVJ40M/bXyNmEQ/
  rw               RSA  2048 AAAAB3NzaC1yc2EAAAADAQABAAABAQ...+M7MVJ40M/bXyNmEQ/

SSH Client:
 Client alive interval: 10
 Client alive count: 0
S Chassis(rw)->
```

set ssh

Use this command to enable, disable or reinitialize SSH server on the device.

Syntax

set ssh {**enable** | **disable** | **reinitialize**}

Parameters

enable | **disable**	Enables or disables the SSH server.
reinitialize	Reinitializes the SSH server.

Defaults

None.

Mode

All command modes.

Usage

This command only affects the SSH server on the device. The SSH device client is always enabled and is not configurable.

Example

This example shows how to disable SSH:

```
S Chassis(rw)->set ssh disable
```

set ssh ciphers

Use this command to list the allowed encryption ciphers in order of precedence from high to low.

Syntax

set ssh ciphers {[**aes128-cbc**][**aes192-cbc**] [**aes256-cbc**] [**3des-cbc**] [**blowfish-cbc**] [**cast128-cbc**] [**rijndael-cbc@lysator.liu.se**]}

Parameters

aes128-cbc	Specifies the AES in CBC mode, with 128-bit key cipher as a member of the allowed encryption ciphers list.
aes192-cbc	Specifies the AES in CBC mode, with 192-bit key cipher as a member of the allowed encryption ciphers list.
aes256-cbc	Specifies the AES in CBC mode, with 256-bit key cipher as a member of the allowed encryption ciphers list.
3des-cbc	Specifies the Three-key 3DES in CBC mode cipher as a member of the allowed encryption ciphers list.
blowfish-cbc	Specifies the Blowfish in CBC mode cipher as a member of the allowed encryption ciphers list. Not supported in FIPS mode.

cast128-cbc	Specifies the CAST-128 in CBC mode cipher as a member of the allowed encryption ciphers list. Not supported in FIPS mode.
rijndael-cbc@lysator.liu.se	Specifies the alias for the aes256-cbc cipher as a member of the allowed encryption ciphers list.

Defaults

None.

Mode

All command modes.

Usage

During the handshake between an SSH client and an SSH server, each side sends a proposal of cartographic Ciphers. This command sets the SSH ciphers applied to all new inbound (SSH server) and outbound (SSH client) SSH sessions. Existing sessions remain unchanged. Ciphers are entered in order of precedence from high to low. Applied SSH Ciphers default to all supported ciphers in the following order of precedence: aes128-cbc, aes192-cbc, aes256-cbc, 3des-cbc, blowfish-cbc, cast128-cbc, and rijndael-cbc@lysator. liu.se.

When in FIPS mode, only the following FIPS compliant Ciphers are allowed (listed in the default order of precedence from high to low): aes128-cbc, aes192-cbc, aes256-cbc, and 3des-cbc. If non-FIPS Ciphers are configured when booting in FIPS mode, SSH uses the default Cipher list.

Example

This example shows how to limit allowed SSH Ciphers in order of precedence from high to low to aes256-cbc and 3des-cbc:

```
S Chassis(rw)->set ssh ciphers aes256-cbc 3des-cbc
S Chassis(rw)->
```

clear ssh ciphers

Use this command to reset the allowed encryption ciphers in the default order of precedence.

Syntax

`clear ssh ciphers`

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

SSH Ciphers default to all supported ciphers in the following order of precedence: aes128-cbc, aes192-cbc, aes256-cbc, 3des-cbc, blowfish-cbc, and cast128-cbc, and rijndael-cbc@lysator. liu.se.

When in FIPS mode, only the following FIPS compliant Ciphers are allowed (listed in the default order of precedence from high to low): aes128-cbc, aes192-cbc, aes256-cbc, and 3des-cbc.

Example

This example shows how to reset SSH Ciphers allowed to the default in order of precedence:

```
S Chassis(rw)->clear ssh ciphers
S Chassis(rw)->
```

set ssh client alive-interval

Use this command to set the SSH server's client alive interval.

Syntax

set ssh client alive-interval *interval*

Parameters

interval	Sets the SSH client alive interval. Valid values are 0 - 2147483647 seconds. Default value is **30** seconds.

Defaults

30 seconds.

Mode

All command modes.

Usage

This command sets a timeout interval in seconds after which if no data has been received from the client, SSH sends a message through the encrypted channel to request a response from the client. Use the "set ssh client alive-count" on page 10-5 to set the number of times to repeat this procedure before the session is timed out.

If the SSH client alive interval is set to 0, no messages are sent to the client.

Example

This example shows how to set the SSH client keep alive interval to **40** seconds:

```
S Chassis(rw)->set ssh client alive-interval 40
```

set ssh client alive-count

Use this command to set the maximum number of times a client alive message is not acknowledged before the session times out.

Syntax

set ssh client alive-count *count*

Parameters

count	Sets the number of times a client alive message will be sent to the client before the session times out. Valid values are 0 - 2147483647. Default value is 5.

Defaults

5 seconds.

Mode

All command modes.

Usage

This command sets the maximum number of client alive messages which may be sent without SSH receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, SSH will disconnect the client, terminating the session.

Example

This example shows how to set the maximum number of client alive messages sent to the client to **6**:

```
S Chassis(rw)->set ssh client alive-count 6
```

clear ssh client

Use this command to reset the SSH client parameters to default values.

Syntax

clear ssh client {**alive-interval** | **alive-count**}

Parameters

alive-interval	Resets the SSH client alive interval to the default value of **30** seconds.
alive-count	Resets the SSH client alive count to the default value of **5**.

Defaults

alive-interval = **30** seconds.

alive-count = **5**.

Mode

All command modes.

Example

This example shows how to reset the SSH client keep alive interval to the default value of **30** seconds:

```
S Chassis(rw)->clear ssh client alive-interval
```

set ssh hostkey

Use this command to set or reinitialize new SSH authentication keys.

Syntax

```
set ssh hostkey [reinitialize] [type type]
```

Parameters

reinitialize	(Optional) Reinitializes the server host authentication keys.
type *type*	(Optional) Specify the hostkey type. Valid values are **dsa** or **rsa**. The default value is **rsa**.

Defaults

If **reinitialize** is not specified, the host key is set.

If **type** is not specified, the type is set to **rsa**.

Mode

All command modes.

Example

This example shows how to regenerate SSH keys:

```
S Chassis(rw)->set ssh hostkey reinitialize
```

set ssh macs

Use this command to list the allowed Message Authentication Code (MACs) in order of precedence from high to low.

Syntax

```
set ssh macs {[hmac-sha1-etm@openssh.com] [hmac-md5-etm@openssh.com]
[hmac-ripemd160-etm@openssh.com] [hmac-sha1-96-etm@openssh.com]
[hmac-md5-96-etm@openssh.com] [hmac-sha1] [hmac-md5] [hmac-ripemd160]
[hmac-ripemd160@openssh.com] [hmac-sha1-96] [hmac-md5-96]}
```

Parameters

hmac-sha1-etm @openssh.com	Specifies the SHA-1 with 20-byte digest and key length, encrypt-then-mac as a member of the allowed MAC list.
hmac-md5-etm @openssh.com	Specifies the MD5 with 16-byte digest and key length, encrypt-then-mac as a member of the allowed MAC list.
hmac-ripemd160-etm @openssh.com	Specifies the RIPEMD-160 algorithm with 20-byte digest length, encrypt-then-mac as a member of the allowed MAC list.
hmac-sha1-96-etm @openssh.com	Specifies the SHA-1 with 20-byte key length and 12-byte digest length, encrypt-then-mac as a member of the allowed MAC list.
hmac-md5-96-etm @openssh.com	Specifies the MD5 with 16-byte key length and 12-byte digest length, encrypt-then-mac, as a member of the allowed MAC list.

hmac-sha1	Specifies the SHA-1 with 20-byte digest and key length as a member of the allowed MAC list.
hmac-md5	Specifies the MD5 with 16-byte digest and key length as a member of the allowed MAC list.
hmac-ripemd160	Specifies the RIPEMD-160 algorithm with 20-byte digest length as a member of the allowed MAC list.
hmac-ripemd160 @openssh.com	Specifies the alias for hmac-ripemd160 MAC.
hmac-sha1-96	Specifies the SHA-1 with 20-byte key length and 12-byte digest length as a member of the allowed MAC list.
hmac-md5-96	Specifies the MD5 with 16-byte key length and 12-byte digest length as a member of the allowed MAC list.

Defaults

None.

Mode

All command modes.

Usage

During the handshake between an SSH client and an SSH server, each side sends a proposal of cryptographic MACs. MACs are entered in order of precedence from high to low. Applied MACs default to all supported MACs in the following order of precedence: hmac-sha1-etm@openssh.com, hmac-md5-etm@openssh.com, hmac-ripemd160-etm@openssh.com, hmac-sha1-96-etm@openssh.com, hmac-md5-96-etm@openssh.com, hmac-sha1, hmac-md5, hmac-ripemd160, hmac-ripemd160@openssh.com, hmac-sha1-96, and hmac-md5-96.

When in FIPS mode, only the following FIPS compliant MACs are allowed (listed in the default order of precedence from high to low): hmac-sha1 and hmac-sha1-96. If non-FIPS MACs are configured when booting in FIPS mode, SSH uses the default MACs list.

Example

This example shows how to limit allowed SSH MACs in order of precedence from high to low to hmac-sha1-etm@openssh.com and hmac-md5-96:

```
S Chassis(rw)->set ssh macs hmac-sha1-etm@openssh.com hmac-md5-96
S Chassis(rw)->
```

clear ssh macs

Use this command to reset the allowed MACs in the default order of precedence.

Syntax

clear ssh macs

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset SSH MACs allowed to the default in order of precedence:

```
S Chassis(rw)->clear ssh macs
S Chassis(rw)->
```

set ssh reinitialize

Use this command to reinitialize SSH authentication.

Syntax

set ssh reinitialize

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reinitialize SSH authentication:

```
S Chassis(rw)->set ssh reinitialize
```

set ssh server allowed-auth

Use this command to set the allowed authentication methods when connecting to the SSH server.

Syntax

set ssh server allowed-auth {[**password** {**enable** | **disable**}] [**pubkey** {**enable** | **disable**}]}

Parameters

password	Specifies that entering a password is an allowed or disallowed SSH server authentication method when connecting to this device. Enabled by default.
pubkey	Specifies that the public key SSH server authentication method is an allowed or disallowed SSH server authentication method when connecting to this device. Disabled by default.

Defaults

Password is enabled, pubkey is disabled.

Mode

All command modes.

Usage

During an SSH handshake the SSH server will advertise to the client a list of allowed authentication methods. The client then attempts authorization using one of the allowed methods. If the first attempt fails, the client may try subsequent attempts using the other allowed methods until either a method succeeds and the user is allowed to connect or all methods are exhausted.

Both the password and public key authentication methods are supported. The password authentication method is enabled by default. To use either method, SSH must be enabled on the device.

To use the public key authentication method:

- Enable the public key authentication method using this command
- Assure that at least one authkey is configured using "set ssh server allowed-auth" on page 10-9 or that PKI is configured

Example

This example shows how to set the password authentication method to disabled and the public key authentication method to enabled on this SSH server:

```
S Chassis(rw)->set ssh server allowed-auth password disable pubkey enable
```

show ssh authkey

Use this command to display the full user name and authkey data.

Syntax

`show ssh authkey`

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the full username and authkey data for the SSH server:

```
S Chassis(rw)->show ssh authkey
Authorized User Public Keys:
--------------------------------------------------------------------------------
```

```
Username:   testuser
Strength:   768 bits
Public Key: ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAYQDZoYlKuBueHbGWuqF4PcyiiVZQTJBEAaJUl2N8WfRYyGAFah7v
SmIoOIhEz1QSn47agV6z4LN8VCJcwfiiW2y7df/vppc0KVqx/zm1cD5luapTsmZ2ljAppNyNcEsw4LU=
S Chassis(rw)->
```

set ssh server authkey

Use this command to explicitly map a public key to a specific user.

Syntax

set ssh server authkey *username* {**ssh-dss** | **ssh-rsa**} *ssh-key* [**no-confirm**]

Parameters

username	Specifies the user to whom the public key belongs.
ssh-dss	Specifies DSA as the public key type.
ssh-rsa	Specifies RSA as the public key type.
ssh-key	Specifies the public key in OpenSSH format.
no-confirm	(Optional) Specifies that the key is accepted without prompting for confirmation.

Defaults

None.

Mode

All command modes.

Usage

This command assigns a single public key to a single user. The key must be of type DSA or RSA, and the key data must be in OpenSSH format (created by the OpenSSH command **ssh-keygen**).

Example

This example shows how to assign a created RSA public key to the user **testuser**:

```
S Chassis(rw)->set ssh server authkey testuser ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAYQDZoYlKuBueHbGWuqF4PcyiiVZQTJBEAaJUl2N8WfRYyGAFah7v
SmIoOIhEz1QSn47agV6z4LN8VCJcwfiiW2y7df/vppc0KVqx/zm1cD5luapTsmZ2ljAppNyNcEsw4LU=


Entered key for username "testuser" has the following attributes:
  Key Type: ssh-rsa
  Strength: 768 bits

Do you accept this public key (y/n) [n]?y
S Chassis(rw)->
```

clear ssh server authkey

Use this command to clear an SSH server authentication key.

Syntax

clear ssh server authkey [*username*] [**no-confirm**]

Parameters

username	(Optional) Specifies that the authentication key for the specified username is deleted.
no-confirm	(Optional) Specifies that the authentication key will be deleted without confirmation.

Defaults

If *username* is not specified, all authkeys are cleared.

If **no-confirm** is not specified, you are prompted to confirm the authkey deletion.

Mode

All command modes.

Example

This example shows how to clear the username **testuser** SSH server authentication public key:

```
S Chassis(rw)->clear ssh server authkey testuser
```

set ssh server pki trusted-ca-list

Use this command to establish the list of trusted CA certificates used during PKI authentication of a user's X.509 certificate.

Syntax

set ssh server pki trusted-ca-list *pki-cert-list*

Parameters

pki-cert-list	Specifies a named list of certificates using "set pki certificate" on page 5-5.

Defaults

None.

Mode

All command modes.

Usage

This command establishes the list of trusted CA certificates which are used during PKI authentication of a user's X.509 certificate. Any self-signed certificate in this list is considered

"trust anchor", meaning if a user certificate chain links back to one of these certificates, then the remote user is considered authenticated and is thus allowed to connect to the device.

PKI cryptographically binds public keys to usernames in what are called "Digital Certificates". The binding is performed by Certificate Authorities (CAs). A single CA may bind multiple user certificates. PKI asserts that if you trust a CA and you have that CA's certificate, then you can implicitly (rather than explicitly) trust all certificates issued by that CA.

In order for SSH to use PKI for public key authentication, the trusted-ca-list must be configured. Additionally, the device must have access to all certificates in a certificate chain. The user certificate in the chain is supplied by the SSH client during the handshake. Therefore all other certificates in the chain must be present in trusted-ca-list.

PKI verifies that every certificate in the chain was signed by its issuing CA, is currently valid (not expired), and has not been revoked (using the OCSP protocol, if enabled).

Example

This example shows how to set the trusted certificate authorization list to **myTrustedCAs**:

```
S Chassis(rw)->set ssh server pki trusted-ca-list myTrustedCAs
```

set ssh server pki authorized-cert-list

Use this command to require a user's certificate to be explicitly configured on the device.

Syntax

set ssh server pki authorized-cert-list *pki-cert-list*

Parameters

pki-cert-list	Specifies a named list of certificates and keys configured using "set pki certificate" on page 5-5.

Defaults

None.

Mode

All command modes.

Usage

By design, PKI authentication does not require a user's certificate to be configured on the device (explicitly trusted). However, if desired, you may impose an explicit trust requirement using this command.

If an authorized-cert-list is configured, any certificate presented by a user which is not on this list will be rejected. If the certificate is on the list, then normal PKI authentication will be performed.

If an authorized-cert-list is not configured, then user certificates are only subject to normal PKI verification using the CA certificate trust chain.

Example

This example shows how to require a user's certificate to be explicitly configured in the **myAuthCerts** authorized-cert-list:

```
S Chassis(rw)->set ssh server pki authorized-cert-list myAuthCerts
```

ssh

Use this command to start an SSH session to a remote host.

Syntax

ssh *hostname* [**-4** | **-6**] [**-b** *bind-address*] [**-c** *cipher-spec*] [**-e** *escape-char*] [**-l** *login-name*] [**-m** *mac-spec*] [**-p** *port*] [**-p**] [**-q**] [**-r**] [**-vrf** *router*]

Parameters

hostname	Specifies the host name or IP address of the remote host this SSH session is connecting to.
-4 | **-6**	(Optional) Specifies that SSH should use either IPv4 or IPv6 addresses, but not both.
-b *bind-address*	(Optional) Specifies the IP address to transmit from when there are multiple interfaces and or addresses.
-c *cipher-spec*	(Optional) Specifies a list of the cipher specifications that overrides the current cipher configuration for encrypting this session.
-e *escape-char*	(Optional) Sets the escape character for the session. Default value: **~**
-l *login-name*	(Optional) Specifies the user to login as on the remote host.
-m *mac-spec*	(Optional) Specifies the MAC algorithms used for data integrity protection.
-p *port*	(Optional) Specifies the host port to connect to on the remote host. Default value: **22**.
-q	(Optional) Specifies that the session will operate in quiet mode, causing all warning and diagnostic messages to be suppressed.
-r	(Optional) Specifies that normal routing table lookup should be bypassed and that the session request should be sent directly to a host on an attached network.
-vrf *router*	(Optional) Specifies the router on which to source this SSH session. Valid values: **default**.

Defaults

- If **-4** or **-6** are not specified, SSH will use IPv4 and IPv6 addresses for this session.
- If **-b** is not specified, the bind IP address is chosen by the system based upon the chosen route to the destination.
- If **-c** is not specified, the default cipher list is used.
- If **-e** is not specified, the default escape character **~** is used.
- If **-l** is not specified, no login name is sent with the session request.
- If **-m** is not specified, the default MAC algorithm list is used.

- If **-p** is not specified, the standard default SSH port 22 is used.
- If **-q** is not specified, warning and diagnostic messages are not suppressed for the session.
- If **-r** is not specified, normal host routing tables will be used for this session.
- If **-v** is not specified, SSH will not print debug messages for this session.
- If **-vrf** is not specified, the router is inherited from the CLI context. The **default** router is used by this session.

Mode

All command modes.

Usage

The SSH client application is always enabled.

The **-4** and **-6** flags are used when the host is a domain name as opposed to a IPv4 or IPv6 address. A DNS server may return multiple responses, some of which may be IPv4 addresses and some of which may be IPv6 addresses. If the returned address type matters, then these flags let you choose which type will be accepted.

The cipher specification list is a comma-separated list of ciphers listed in the order of preference. The specified cipher list overrides the current default configuration or the configuration specified in command "set ssh ciphers" on page 10-3.

The escape character is only recognized at the beginning of a line. The escape character followed by a dot (**~.**) closes the connection. The escape character followed by a CTRL-Z suspends the session. The escape character followed by itself (**~~**) sends a single escape character. Setting the escape character to **none** disables any escapes and makes the session fully transparent.

The *mac-spec* setting is a comma-separated list of MAC algorithms listed in the order of preference. The specified MAC list overrides the current default configuration or the configuration specified in command "set ssh macs" on page 10-7.

The **-r** option is intended for when the route table is invalid for some reason and you are using SSH to debug it.

Example

This example shows how to start an SSH session with host 10.20.10.2 with a login name of documentation and with warning and diagnostic messages suppressed:

```
S Chassis(rw)->ssh -l documentation -q 10.20.10.2
S Chassis(rw)->
```

11

Domain Name Server (DNS) Commands

This chapter provides detailed information for the Domain Name Server (DNS) set of commands. For information about configuring DNS, refer to the "System Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
set ip dns	11-1
set ip dns domain	11-2
clear ip dns domain	11-3
set ip dns server	11-3
clear ip dns server	11-4
set ip dns zone	11-4
clear ip dns zone	11-5
set ip dns port-number	11-6
clear ip dns port-number	11-6
set ip dns timeout	11-7
clear ip dns timeout	11-7
set ip dns query-retries	11-8
clear ip dns query-retries	11-9
clear ip dns all	11-9
clear ip dns status	11-10
show ip dns	11-10

set ip dns

Use this command to enable and disable DNS resolver.

Syntax

```
set ip dns {enable | disable}
```

Parameters

enable | **disable**	Enables or disables the DNS resolver function. Default value: **enabled**.

Defaults

None.

Mode

All command modes.

Example

This example disables the DNS resolver function on this system:

```
S Chassis(rw)->set ip dns disable
S Chassis(rw)->
```

set ip dns domain

Use this command to configure the DNS domain name.

Syntax

set ip dns domain *name*

Parameters

name	Specifies the DNS domain name where the device is located.

Defaults

None.

Mode

All command modes.

Usage

If the domain name is not set, all address lookups must provide fully qualified domains.

A “name” (Net, Host, Gateway, or Domain name) is a text string up to 24 characters drawn from the alphabet (A-Z), digits (0-9), minus sign (-), and period (.). Note that periods are only allowed when they serve to delimit components of “domain style names”. No blank or space characters are permitted as part of a name. No distinction is made between upper and lower case. The first character must be an alpha character. The last character must not be a minus sign or period. A host which serves as a GATEWAY should have “-GATEWAY” or “-GW” as part of its name. Hosts which do not serve as Internet gateways should not use “-GATEWAY” or “-GW” as part of their names. A host which is a TAC should have “-TAC” as the last part of its host name, if it is a DoD host. Single character names or nicknames are not allowed.

Example

This example sets the DNS domain name to **Enterprise-Services.Support**:

```
S Chassis(rw)->set ip dns domain Enterprise-Services.Support
S Chassis(rw)->
```

clear ip dns domain

Use this command to clear the configured DNS domain name.

Syntax

clear ip dns domain

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

If the domain name is not set, all address lookups must provide fully qualified domains.

Example

This example clears the currently configure DNS domain name for this system:

```
S Chassis(rw)->clear ip dns domain
S Chassis(rw)->
```

set ip dns server

Use this command to configure the IP address for the DNS server.

Syntax

set ip dns server *ip-address server*

Parameters

ip-address	Specifies the IPv4 or IPv6 address for the DNS server.
server	Specifies the server designation: • **primary** - Primary DNS server address • **secondary** - Secondary DNS server address • **tertiary** - Tertiary DNS server address • **quaternary** - Quaternary DNS server address

Defaults

None.

Mode

All command modes.

Examples

This example sets the IP address for this systems primary domain server to 20.20.0.1:

```
S Chassis(rw)->set ip dns server 20.20.0.1 primary
S Chassis(rw)->
```

This example sets the IP address for this systems primary domain server to **2001:11ac:dcaa::10**:

```
S Chassis(rw)->set ip dns server 2001:11ac:dcaa::10 primary
S Chassis(rw)->
```

clear ip dns server

Use this command to clear the specified server from the server pool.

Syntax

clear ip dns server [*server* | **all**]

Parameters

server	Specifies the server to clear: • **primary** - Primary DNS server address • **secondary** - Secondary DNS server address • **tertiary** - Tertiary DNS server address • **quaternary** - Quaternary DNS server address
all	Specifies that all DNS server addresses are cleared.

Defaults

If no option is specified, all DNS server addresses are cleared.

Mode

All command modes.

Example

This example clears the primary server for this system:

```
S Chassis(rw)->clear ip dns server primary
S Chassis(rw)->
```

set ip dns zone

Use this command to configure a non-default DNS zone for IPv4 or IPv6 address to name lookups.

Syntax

set ip dns zone {**ipv4** | **ipv6**} *zone-name*

Parameters

ipv4	Specifies an IPv4 or IPv6 DNS zone for IP address to name lookups.

ipv6	Specifies an IPv6 DNS zone.
zone-name	Specifies the IPv4 or IPv6 DNS zone for IP address to name lookups.

Defaults

None.

Mode

All command modes.

Usage

IPv4 and IPv6 DNS zones for IP address to domain name lookups default to:

- **ipv4** – in-addr.arpa
- **ipv6** – ip6.arpa

Use this command to set a non-default DNS zone. Use "show ip dns" on page 11-10 to determine the current DNS zone set for this device.

Example

This example sets the IPv4 DNS zone to **in-addr.arpa**:

```
S Chassis(rw)->set ip dns zone ipv4 in-addr.arpa
S Chassis(rw)->
```

clear ip dns zone

Use this command to clear the DNS zone for IP address to name lookups.

Syntax

clear ip dns zone [**ipv4** | **ipv6**]

Parameters

ipv4 | **ipv6**	(Optional) Specifies the IPv4 or IPv6 DNS zone to clear.

Defaults

If neither ipv4 or ipv6 are specified, both zones are returned to the default zone values.

Mode

All command modes.

Usage

Using this command resets the DNS zone for either IPv4, IPv6, or both to the default DNS zones. IP DNS zones default to:

- **ipv4** – in-addr.arpa
- **ipv6** – ip6.arpa

Use "show ip dns" on page 11-10 to determine the current IPv4 and IPv6 DNS zones set for this device.

Examples

This example clears the IPv4 DNS zone for this system:

```
S Chassis(rw)->clear ip dns zone ipv4
S Chassis(rw)->
```

This example clears both the IPv4 and IPv6 DNS zone for this system:

```
S Chassis(rw)->clear ip dns zone
S Chassis(rw)->
```

set ip dns port-number

Use this command to configure the port number the DNS resolver uses for DNS queries.

Syntax

set ip dns port-number *port-number*

Parameters

port-number	Specifies the port number the DNS resolver uses for DNS queries. Valid values: **0** - **65535**. Default value: **53**.

Defaults

None.

Mode

All command modes.

Example

This example sets the DNS port number to 5353 for this system:

```
S Chassis(rw)->set ip dns port-number 5353
S Chassis(rw)->
```

clear ip dns port-number

Use this command to reset the port number the DNS resolver uses for DNS queries to the default value.

Syntax

clear ip dns port-number

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

This command resets the port number the DNS resolver uses to the default value of port **53**.

Example

This example resets the DNS port number for this system to the default value:

```
S Chassis(rw)->clear ip dns port-number
S Chassis(rw)->
```

set ip dns timeout

Use this command to set the number of seconds before a DNS request is retried when the DNS server fails to respond.

Syntax

set ip dns timeout *seconds*

Parameters

seconds	Specifies the number of seconds to wait before a DNS request is retried when the DNS server fails to respond. Valid values: **1** - **100** seconds. Default value: **10** seconds.

Defaults

None.

Mode

All command modes.

Example

This example sets the DNS timeout value to 15 seconds:

```
S Chassis(rw)->set ip dns timeout 15
S Chassis(rw)->
```

clear ip dns timeout

Use this command to reset the number of seconds before a DNS request is retried when the DNS server fails to respond to the default value.

Syntax

clear ip dns timeout

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

This command resets the DNS timeout to the default value of **10** seconds.

Example

This example resets the DNS timeout to the default value:

```
S Chassis(rw)->clear ip dns timeout
S Chassis(rw)->
```

set ip dns query-retries

Use this command to configure the number of times to retry a lookup request to a DNS server that has failed to respond.

Syntax

set ip dns query-retries *retries*

Parameters

retries	Specifies the number of times to retry a lookup request to a DNS server that has failed to respond. Valid Values: **1**-**65535**. Default value: **2**.

Defaults

None.

Mode

All command modes.

Usage

The number of retries specified in this command is per name server. Each configured name server will be retried the number of times configured by this command before moving to the next configured server.

Example

This example sets the number server request retries for each name server to 4:

```
S Chassis(rw)->set ip dns query-retries 4
S Chassis(rw)->
```

clear ip dns query-retries

Use this command to reset the number of times to retry a lookup request to a DNS server that has failed to respond to its default value.

Syntax

clear ip dns query-retries

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

This command reset the number of times to retry a DNS lookup to the default value of **2**.

Example

This example resets the number of server request retries for each name server to the default value:

```
S Chassis(rw)->clear ip dns query-retries
S Chassis(rw)->
```

clear ip dns all

Use this command to reset all DNS configuration for this system to default values.

Syntax

clear ip dns all

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example sets all DNS configuration for this system to default values:

```
S Chassis(rw)->clear ip dns all
S Chassis(rw)->
```

clear ip dns status

Use this command to reset DNS state for this system to the default value.

Syntax

clear ip dns status

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

This command resets the DNS state to the default value of enabled. See “set ip dns” on page 11-1 for information on setting the DNS state to enabled or disabled. See show ip dns for information on determining whether DNS is currently enabled or disabled.

Example

This example sets DNS state on this system to the default value:

```
S Chassis(rw)->clear ip dns status
S Chassis(rw)->
```

show ip dns

Use this command to display DNS configuration for this system.

Syntax

show ip dns

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example displays DNS configuration for this system:

```
S Chassis(rw)->show ip dns
Current State:             Enabled
```

```
Default DNS domain name:
DNS zones:
  IPv4:                    in-addr.arpa
  IPv6:                    ip6.arpa

DNS port number:           53
DNS server timeout:        10 seconds
DNS query retries:         2
DNS Name servers                          Status
----------------------------------------  ----------
(No name servers configured)
S Chassis(rw)->
```

Table 11-1 provides an explanation of the command output.

Table 11-1 show ip dns Output Details

Output...	What it displays...
Current State	Specifies whether DNS is enabled or disabled for this system. Refer to "set ip dns" on page 11-1 for more information.
Default DNS Domain Name	Specifies the Default DNS Domain Name for this system. If the default domain name is not specified, lookups must provide fully qualified domains. Refer to "set ip dns domain" on page 11-2 for more information.
DNS Zones	Specifies the DNS Zones for IPv4 and IPv6 for IP address to name lookups. Refer to "set ip dns zone" on page 11-4 for more information.
DNS port number	Specifies the port DNS resolver uses for DNS queries on this system. Refer to "set ip dns port-number" on page 11-6.
DNS server timeout	Specifies the number of seconds before a DNS request is retried when the DNS server fails to respond. Refer to "set ip dns timeout" on page 11-7 for more information.
DNS query retires	Specifies the number of times to retry a lookup request to a DNS server that has failed to respond. Refer to "set ip dns query-retries" on page 11-8 for more information.
DNS Name servers	Lists all configured DNS name servers for this system. Refer to "set ip dns server" on page 11-3 for more information.
Status	Specifies whether DNS is enable or disabled on this server.

12

Node Alias Commands

This chapter provides detailed information for the node alias set of commands. For information about configuring node alias, refer to the "System Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show nodealias	12-1
show nodealias mac	12-3
show nodealias protocol	12-4
show nodealias config	12-5
set nodealias	12-6
set nodealias maxentries	12-8
clear nodealias	12-8
clear nodealias config	12-9

show nodealias

Use this command to display node alias properties for one or more ports.

Syntax

show nodealias [*port-string*]

Parameters

port-string	(Optional) Displays node alias properties for specific port(s).

Defaults

If *port-string* is not specified, node alias properties will be displayed for all ports.

Mode

All command modes.

Usage

Node aliases are dynamically assigned upon packet reception to ports enabled with an alias agent, which is the default setting on Extreme Networks S-Series devices. Node aliases cannot be

statically created, but can be deleted using the **clear node alias** command (“clear nodealias” on page 12-8).

Example

This example (a portion of the command output) shows how to display node alias properties for all ports:

```
S Chassis(rw)->show nodealias

Port:  ge.1.13   Time:   2008-12-19 14:03:46
-------------------------------------------------------
Alias ID         = 0              Active          = true
Vlan ID          = 1              MAC Address     = 00-ed-c0-00-00-1a
Protocol         = bpdu


Port:   ge.1.4   Time:   2008-12-19 14:03:52
-------------------------------------------------------
Alias ID         = 1              Active          = true
Vlan ID          = 1              MAC Address     = 00-01-f4-2b-3e-45
Protocol         = ospf


Port:   ge.1.4   Time:   2008-12-19 14:03:52
-------------------------------------------------------
Alias ID         = 2              Active          = true
Vlan ID          = 1              MAC Address     = 00-01-f4-2b-3e-45
Protocol         = ip             Source IP       = 110.1.1.110
```

Table 12-1 provides an explanation of the command output.

Table 12-1 show nodealias Output Details

Output...	What it displays...
Alias ID	Alias dynamically assigned to this port.
Active	Whether or not this node alias entry is active.
Vlan ID	VLAN ID associated with this alias.
MAC Address	MAC address associated with this alias.
Protocol	Networking protocol running on this port.
Address / Source IP	When applicable, a protocol-specific address associated with this alias.

show nodealias mac

Use this command to display node alias entries based on MAC address and protocol.

Syntax

show nodealias mac *mac-address* [*protocol*] [*port-string*]

Parameters

mac-address	Specifies a MAC address for which to display node alias entries. This can be a full or partial address.
protocol	(Optional) Displays node alias entries for one of the protocols listed in Table 12-2.
port-string	(Optional) Displays node alias properties for specific port(s).

Defaults

- If protocol is not specified, node alias entries for all protocols will be displayed.
- If *port-string* is not specified, node alias entries will be displayed for all ports.

Mode

All command modes.

Usage

Node alias entries can be displayed based upon the protocols listed in Table 12-2.

Table 12-2 Supported Node Alias Entry Protocols

Protocol Acronym	Description
ip	Internet Protocol version 4
apl	Appletalk
mac	Media Access Control
hsrp	Hot Standby Routing Protocol
dhcps	Dynamic Host Control Protocol Server
dhcpc	Dynamic Host Control Protocol Client
bootps	Boot Protocol Server
bootpc	Boot Protocol Client
ospf	Open Shortest Path First
vrrp	Virtual Router Redundancy Protocol
ipx	Internet Packet Exchange
xrip	IPX Routing Information Protocol
xsap	IPX Service Access Point
ipx20	IPX Protocol 20 packet
rtmp	Routing Table Maintenance Protocol
netBios	NetBIOS (raw)

Table 12-2 Supported Node Alias Entry Protocols

Protocol Acronym	Description
nbt	NetBIOS (over TCP/IP)
bgp	Border Gateway Protocol
rip	Routing Information Protocol
igrp	Interior Gateway Routing Protocol
dec	Digital Equipment Corporation
bpdu	Bridge Protocol Data Unit
udp	User Datagram Protocol
ipv6	Internet Protocol version 6

Example

This example shows how to display node alias entries for all traffic on MAC address **00-01-f4-2b-3e-45** (partial output shown here). Refer back to Table 12-1 for a description of the command output.

```
S Chassis(rw)->show nodealias mac 00-01-f4-2b-3e-45

Port: ge.1.2   Time: 20 days 20 hrs 50 mins 02 secs
-----------------------------------------------------
Alias ID         = 89              Active          = true
Vlan ID          = 1               MAC Address     = 00-01-f4-2b-3e-45
Protocol         = ip              Source IP       = 10.1.0.13


Port: ge.1.2   Time: 18 days 02 hrs 16 mins 00 secs
-----------------------------------------------------
Alias ID         = 75              Active          = true
Vlan ID          = 1               MAC Address     = 00-01-f4-2b-3e-45
Protocol         = ip              Source IP       = 10.1.2.164
```

show nodealias protocol

Use this command to display node alias entries based on protocol and protocol address.

Syntax

show nodealias protocol {*protocol*} [**ip_address** *ip-address*] [*port-string*]

Parameters

protocol	Specifies the protocol for which to display node alias entries. Refer to Table 12-2 on page 12-3 for a list and description of supported protocols.
ip-address *ip-address*	(Optional) Used for IP protocol only, displays node alias entries for a specific source address.
port-string	(Optional) Displays node alias entries for specific port(s).

Defaults

- If **ip_address** *ip-address* is not specified for the IP protocol, IP-related entries will be displayed from all source addresses.
- If *port-string* is not specified, node alias entries will be displayed for all ports.

Mode

All command modes.

Example

This example shows how to display node alias entries for IP traffic on ge.1.13. Refer back to Table 12-1 for a description of the command output.

```
S Chassis(rw)->show nodealias protocol ip ge.1.13

Port: ge.1.13   Time: 20 days 01 hrs 23 mins 47 secs
-------------------------------------------------------
Alias ID         = 84              Active           = true
Vlan ID          = 113             MAC Address      = 00-01-f4-5b-60-20
Protocol         = ip              Source IP        = 0.0.0.0


Port: ge.1.13   Time: 2 days 21 hrs 52 mins 28 secs
-------------------------------------------------------
Alias ID         = 39              Active           = true
Vlan ID          = 113             MAC Address      = 00-01-f4-5b-60-20
Protocol         = ip              Source IP        = 10.1.128.1
```

show nodealias config

Use this command to display node alias configuration settings on one or more ports.

Syntax

show nodealias config [*port-string*]

Parameters

port-string	(Optional) Displays node alias configuration settings for specific port(s).

Defaults

If *port-string* is not specified, node alias configurations will be displayed for all ports.

Mode

All command modes.

Example

This example shows how to display node alias configuration settings for port ge.1.1:

```
S Chassis(rw)->show nodealias config ge.1.1

Max Control Entries     = 44                  Active Entries = 44
Purge Time              = 01:16:09       State          = ready(2)

Port Number         Max Entries         Used Entries         Status
-----------         -----------         ------------         ----------
ge.1.1              44                  44                   Enabled
```

Table 12-3 provides an explanation of the command output.

Table 12-3 show nodealias config Output Details

Output...	What it displays...
Max Control Entries	Specifies the number of entries used across all ports.
Active Entries	Specifies the number of active entries across all ports.
Port Number	Port designation.
Max Entries	Maximum number of alias entries configured for this port. Set using “set nodealias maxentries” on page 12-8.
Used Entries	Number of alias entries (out of the maximum amount configured) already used by this port.
Status	Whether or not a node alias agent is enabled (default) or disabled on this port.

set nodealias

Use this command to enable, disable, or set maximum entries for a node alias agent on one or more ports.

Syntax

set nodealias {**enable** | **disable**} [**protocols** *protocols*] *port-string*

Parameters

enable | **disable**	Enables or disables a node alias agent. Default: **enable**.
protocols *protocols*	(Optional) Specifies the enabling or disabling of node alias captures on a protocol basis. Defaults to all protocols. Configurable protocols are: • **ip** – Internet Protocol Version 4 • **apl** – Appletalk • **mac** – Media Access Control • **hsrp** – Hot Standby Routing Protocol • **dhcps** – Dynamic Host Control Protocol Server • **dhcpc** – Dynamic Host Control Protocol Client • **bootps** – Boot Protocol Server • **bootpc** – Boot Protocol Client • **ospf** – Open Shortest Path First • **vrrp** – Virtual Router Redundancy Protocol • **ipx** – Internet Packet Exchange • **xrip** – IPX Routing Information Protocol • **xsap** – IPX Service Access Point • **ipx20** – IPX Protocol 20 packet • **rtmp** – Routing Table Maintenance Protocol • **netBios** – NetBIOS (raw) • **nbt** – NetBIOS (over TCP/IP) • **bgp** – Border Gateway Protocol • **rip** – Routing Information Protocol • **igrp** – Interior Gateway Routing Protocol • **dec** – Digital Equipment Corporation • **bpdu** – Bridge Protocol Data Unit • **udp** – User Datagram Protocol • **ipv6** – Internet Protocol Version 6
maxentries	Specifies the maximum number of entries the node alias agent will discover for the specified port(s).
port-string	If the **enable** or **disable** parameter is used, the port-string parameter specifies the port(s) on which to enable or disable a node alias agent. If the **maxentries** parameter is used, port-string specifies the port(s) on which to limit the maximum number of entries the node alias agent will discover.

Defaults

None.

Mode

All command modes.

Usage

Upon packet reception, node aliases are dynamically assigned to ports enabled with an alias agent, which is the default setting on Extreme Networks S-Series devices. Node aliases cannot be statically created, but can be deleted using "clear nodealias" on page 12-8.

Example

This example shows how to disable the node alias agent on ge.1.13:

```
S Chassis(rw)->set nodealias disable ge.1.13
```

set nodealias maxentries

Use this command to set the maximum number of node alias entries allowed for one or more ports.

Syntax

set nodealias maxentries *val port-string*

Parameters

val	Specifies the maximum number of alias entries. Valid values: **0** - **8192**. The default value is **69**.
port-string	Specifies the port(s) on which to set the maximum entry value.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the maximum node alias entries to 1000 on ge.1.13:

```
S Chassis(rw)->set nodealias maxentries 1000 ge.1.13
```

clear nodealias

Use this command to remove one or more node alias entries.

Syntax

clear nodealias {**port** *port-string* | **alias-id** *alias-id* | **protocol** *protocol*}

Parameters

port *port-string*	Specifies the port(s) on which to remove all node alias entries.
alias-id *alias-id*	Specifies the ID of the node alias to remove. This value can be viewed using "show nodealias" on page 12-1.

protocol *protocol*	Specifies a protocol to clear node alias capture entries for. See the **protocols** parameter for "set nodealias" on page 12-6 for a list of protocols to clear.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear all node alias entries on ge.1.13:

```
S Chassis(rw)->clear nodealias port ge.1.13
```

clear nodealias config

Use this command to reset node alias state to enabled and clear the maximum entries value.

Syntax

clear nodealias config *port-string*

Parameters

port-string	Specifies the port(s) on which to reset the node alias configuration.

Defaults

None.

Mode

All command modes.

Usage

This command resets the maximum entries value for the specified port to the default value of **69**.

Example

This example shows how to reset the node alias configuration on ge.1.3:

```
S Chassis(rw)->clear nodealias config ge.1.3
```

13

SNTP Commands

This chapter provides detailed information for the Simple Network Time Protocol (SNTP) set of commands. For information about configuring SNTP, refer to the "System Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show sntp	13-2
set sntp authentication mode	13-3
set sntp authentication key	13-4
set sntp authentication trust	13-5
clear sntp authentication	13-6
set sntp client	13-6
clear sntp client	13-7
set sntp server	13-7
clear sntp server	13-8
set sntp broadcastdelay	13-8
clear sntp broadcast delay	13-9
set sntp poll-interval	13-9
clear sntp poll-interval	13-10
set sntp poll-retry	13-10
clear sntp poll-retry	13-11
set sntp poll-timeout	13-11
clear sntp poll-timeout	13-12
show timezone	13-12
set timezone	13-13
clear timezone	13-13

show sntp

Use this command to display SNTP client settings.

Syntax

show sntp

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display SNTP client settings:

```
show sntp
SNTP Version: 4
Current Time: FRI MAY 06 15:33:53 2011
Timezone: 'EDT', offset from UTC is -4 hours and 0 minutes
Client Mode: unicast
Broadcast Delay: 3000 microseconds
Broadcast Count: 0
Poll Interval: 600 seconds
Poll Retry: 2
Poll Timeout: 5 seconds
SNTP Poll Requests: 2
Last SNTP Update: MON MAY 02 14:42:52 2011
Last SNTP Request: MON MAY 02 14:42:52 2011
Last SNTP Status: Enabled

SNTP Servers:

Status        Precedence     Key        SNTP-Server
------------------------------------------------------------------------
Active             1          1         10.21.1.100

SNTP Authentication: Enabled

Status        Key            Type         Trusted
------------------------------------------------------------------------
Active        1             MD5           Enabled
S Chassis(rw)->
```

Table 13-1 provides an explanation of the command output.

Table 13-1 show sntp Output Details

Output...	What it displays...
SNTP Version	SNTP version number.
Current Time	Current time on the system clock.
Timezone	Time zone name and amount it is offset from UTC (Universal Time). Set using "set timezone" on page 13-13.
Client Mode	Whether SNTP client is operating in unicast or broadcast mode. Set using "set sntp client" on page 13-6.
Broadcast Delay	Round trip delay for SNTP broadcast frames. Default of 3000 microseconds can be reset using "set sntp broadcastdelay" on page 13-8.
Broadcast Count	Number of SNTP broadcast frames received.
Poll Interval	Interval between SNTP unicast requests. Default of 512 seconds can be reset using "set sntp poll-interval" on page 13-9.
Poll Retry	Number of poll retries to a unicast SNTP server. Default of 1 can be reset using "set sntp poll-retry" on page 13-10.
Poll Timeout	Timeout for a response to a unicast SNTP request. Default of 5 seconds can be reset using "clear sntp poll-timeout" on page 13-12.
SNTP Poll Requests	Total number of SNTP poll requests.
Last SNTP Update	Date and time of most recent SNTP update.
Last SNTP Request	Date and time of most recent SNTP update.
Last SNTP Status	Whether or not broadcast reception or unicast transmission and reception was successful.
Status (SNTP Server)	Whether or not the SNTP server is active.
Precedence	Precedence level of SNTP server in relation to its peers. Highest precedence is 1 and lowest is 10. Default of 1 can be reset using "set sntp server" on page 13-7.
Key (SNTP Server)	The SNTP authentication key for this server.
SNTP-Server	IP address(es) of SNTP server(s).
SNTP Authentication	Whether SNTP authentication is enabled or not.
Status (SNTP Authentication)	Whether SNTP authentication is trusted or not
Key (SNTP Authentication)	SNTP authentication key configured for this client.
Type	SNTP authentication type configured for this client.

set sntp authentication mode

Use this command to enable or disable authentication for all SNTP client communications.

Syntax

```
set sntp authentication mode {enable | disable}
```

Parameters

enable | disable	Enables or disables authentication for all SNTP client communications. The default value is **disable**.

Defaults

None.

Mode

All command modes.

Usage

SNTP authentication mode is disabled by default.

Example

This example shows how to enable SNTP authentication mode:

```
S Chassis(rw)->set sntp authentication mode enable
```

set sntp authentication key

Use this command to create a new or modify an existing authentication key.

Syntax

set sntp authentication key *key-instance type password*

Parameters

key-instance	Specifies an SNTP authentication key instance. Up to 32 SNTP authentication key instances are supported.
type	Specifies an SNTP authentication type. Currently only MD5 authentication is supported. Valid value is **md5**.
password	Specifies an SNTP authentication key password value as either a string or the encrypted key in hexadecimal format. The maximum number of characters for the plain text string is 32. No space characters are allowed. The length of the encrypted hexidecimal value is dependent upon the initial plain text value.

Defaults

None.

Mode

All command modes.

Usage

This command creates a new or modifies an existing SNTP authentication key. The ID number is used to reference the instance of the key. The type ID specifies the encryption algorithm to use for authentication. MD5 is the supported encryption algorithm. The value is either a string of ASCII characters which are used to generate the encrypted key for the encryption algorithm or the

encrypted key itself in its raw hexadecimal format. The value string may not contain whitespaces. By default the new key is trusted.

Example

This example shows how to create SNTP authentication key instances 1 - 3:

```
S Chassis(rw)->set sntp authentication key 1 md5 foobaraboof
S Chassis(rw)->set sntp authentication key 2 md5 DEADBEAFCAFEBABEDEADBEAFCAFEBAE
S Chassis(rw)->set sntp authentication key 3 md5 01234567890123456789012345678890
```

set sntp authentication trust

Use this command to change the trust state of an existing SNTP authentication key.

Syntax

set sntp authentication trust *key-instance* {**enable** | **disable**}

Parameters

key-instance	Specifies the SNTP authentication key instance to modify the trust status for.
enable | disable	Enables or disables the trust status for the specified SNTP authentication key instance. The SNTP authentication trust status is disabled by default.

Defaults

None.

Mode

All command modes.

Usage

This command modifies the trust state of an existing SNTP authentication key. The key instance is used to reference the instance of the authentication key as configured in "set sntp authentication key" on page 13-4. If the key instance is a valid key, the trust state is modified as specified in the command. The authentication key trust flag must be enabled for SNTP authentication to occur between the SNTP client and server configured for that key instance.

Example

This example shows how to enable trust status for key instance 1 and disable the trust status for key instance 3:

```
S Chassis(rw)->set sntp authentication trust 1 enable
S Chassis(rw)->set sntp authentication trust 3 disable
```

clear sntp authentication

Use this command to clear SNTP authentication key configuration or reset the SNTP authentication mode to the default value.

Syntax

clear sntp authentication {**all** | **key** *key-instance* | **mode**}

Parameters

all	Clears all SNTP authentication keys and SNTP server key associations.
key *key-instance*	Removes the specified SNTP authentication key instance.
mode	Resets the SNTP authentication mode to the default value of disabled.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to clear SNTP authentication key instance 1:

```
S Chassis(rw)->clear sntp authentication key 1
```

This example shows how to reset the global SNTP authentication mode to the default value of disabled:

```
S Chassis(rw)->clear sntp authentication mode
```

set sntp client

Use this command to set the SNTP operation mode.

Syntax

set sntp client {**broadcast** | **unicast** | **disable**}

Parameters

broadcast	Enables SNTP in broadcast client mode.
unicast	Enables SNTP in unicast (point-to-point) client mode. In this mode, the client must supply the IP address from which to retrieve the current time.
disable	Disables SNTP.

Defaults

None.

Mode

All command modes.

Usage

The default SNTP operation mode is disabled.

Example

This example shows how to enable SNTP in broadcast mode:

```
S Chassis(rw)->set sntp client broadcast
```

clear sntp client

Use this command to clear the SNTP client's operational mode.

Syntax

clear sntp client

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

This command resets the SNTP client operation mode to the default value of disabled.

Example

This example shows how to clear the SNTP client's operational mode:

```
S Chassis(rw)->clear sntp client
```

set sntp server

Use this command to add a server from which the SNTP client will retrieve the current time when operating in unicast mode. Up to 10 servers can be set as SNTP servers.

Syntax

set sntp server {*ip-address* | *hostname*} [*precedence*][**key** *key-instance*]

Parameters

ip-address | *hostname*	Specifies the SNTP server's IPv4 or IPv6 address or hostname.
precedence	(Optional) Specifies this SNTP server's precedence in relation to its peers. Valid values are **1** (highest) to **10** (lowest).
key *key-instance*	(Optional) Specifies the authentication instance used by the client when requesting synchronization with the specified server.

Defaults

- If *precedence* is not specified, a precedence of **1** will be applied.
- If **key** *key-instance* is not specified, SNTP authentication will not occur on the server.

Mode

All command modes.

Example

This example shows how to set the server at IP address 10.21.1.100 as an SNTP server and to SNTP authenticate using authentication key instance 1:

```
S Chassis(rw)->set sntp server 10.21.1.100 key 1
```

clear sntp server

Use this command to remove one or all servers from the SNTP server list.

Syntax

clear sntp server {*ip-address* | *hostname* | **all**}

Parameters

ip-address | *hostname*	Specifies the IPv4 or IPv6 address or hostname of a server to remove from the SNTP server list.
all	Removes all servers from the SNTP server list.

Defaults

None.

Mode

All command modes.

Example

This example shows how to remove the server at IP address 10.21.1.100 from the SNTP server list:

```
S Chassis(rw)->clear sntp server 10.21.1.100
```

set sntp broadcastdelay

Use this command to set the round trip delay, in microseconds, for SNTP broadcast frames.

Syntax

set sntp broadcastdelay *time*

Parameters

time	Specifies broadcast delay time in microseconds. Valid values are **1** to **999999**. Default value is **3000** microseconds.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the SNTP broadcast delay to 12000 microseconds:

```
S Chassis(rw)->set sntp broadcastdelay 12000
```

clear sntp broadcast delay

Use this command to clear the round trip delay time for SNTP broadcast frames.

Syntax

clear sntp broadcastdelay

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

This command sets the SNTP broadcast delay to the default value of **3000** microseconds.

Example

This example shows how to clear the SNTP broadcast delay time:

```
S Chassis(rw)->clear sntp broadcastdelay
```

set sntp poll-interval

Use this command to set the poll interval between SNTP unicast requests.

Syntax

set sntp poll-interval *interval*

Parameters

interval	Specifies the poll interval in seconds. Valid values are **16** to **16284** seconds. The default value is **512** seconds.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the SNTP poll interval to 30 seconds:

```
S Chassis(rw)->set sntp poll-interval 30
```

clear sntp poll-interval

Use this command to clear the poll interval between unicast SNTP requests.

Syntax

clear sntp poll-interval

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

This command resets the SNTP poll interval to the default value of **512** seconds.

Example

This example shows how to clear the SNTP poll interval:

```
S Chassis(rw)->clear sntp poll-interval
```

set sntp poll-retry

Use this command to set the number of poll retries to a unicast SNTP server.

Syntax

set sntp poll-retry *retries*

Parameters

retries	Specifies the number of retries. Valid values are **0** to **10**. Default value is **1**.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the number of SNTP poll retries to 5:

```
S Chassis(rw)->set sntp poll-retry 5
```

clear sntp poll-retry

Use this command to clear the number of poll retries to a unicast SNTP server.

Syntax

clear sntp poll-retry

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

This command resets the number of SNTP poll retries to the default value of **1**.

Example

This example shows how to clear the number of SNTP poll retries:

```
S Chassis(rw)->clear sntp poll-retry
```

set sntp poll-timeout

Use this command to set the poll timeout (in seconds) for a response to a unicast SNTP request.

Syntax

set sntp poll-timeout *timeout*

Parameters

timeout	Specifies the poll timeout in seconds. Valid values are **1** to **30**. Default value is **5** seconds.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the SNTP poll timeout to 10 seconds:

```
S Chassis(rw)->set sntp poll-timeout 10
```

clear sntp poll-timeout

Use this command to clear the SNTP poll timeout.

Syntax

clear sntp poll-timeout

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

This command resets the SNTP poll timeout to the default value of **5** seconds.

Example

This example shows how to clear the SNTP poll timeout:

```
S Chassis(rw)->clear sntp poll-timeout
```

show timezone

Use this command to display SNTP time zone settings.

Syntax

show timezone

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display SNTP time zone settings:

```
S Chassis(rw)->show timezone
Admin Config timezone: '', offset from UTC is 5 hours and 0 minutes
Oper  Config timezone: '', offset from UTC is 5 hours and 0 minutes
```

set timezone

Use this command to set the SNTP time zone name and the hours and minutes it is offset from Coordinated Universal Time (UTC).

Syntax

set timezone *name* [*hours*] [*minutes*]

Parameters

name	Specifies the time zone name.
hours	(Optional) Specifies the number of hours this timezone will be offset from UTC. Valid values are minus 12 (**-12**) to **12**.
minutes	(Optional) Specifies the number of minutes this timezone will be offset from UTC. Valid values are **0** to **59**.

Defaults

If offset *hours* or *minutes* are not specified, none will be applied.

Mode

All command modes.

Example

This example shows how to set the time zone to EDT with an offset of minus 4 hours:

```
S Chassis(rw)->set timezone EDT -4 0
```

clear timezone

Use this command to remove SNTP time zone adjustment values.

Syntax

clear timezone

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to remove SNTP time zone adjustment values:

```
S Chassis(rw)->clear timezone
```

14

DHCP Commands

This chapter provides detailed information for the Dynamic Host Configuration Protocol (DHCP) set of commands. For information about configuring DHCP, refer to the "System Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
ip dhcp server	14-2
ipv6 dhcp server	14-3
ipv6 dhcp relay source-interface	14-3
ipv6 dhcp relay destination	14-4
show ip local pool	14-5
ip local pool	14-6
exclude	14-6
ip dhcp ping packets	14-7
ip dhcp ping timeout	14-8
ip dhcp pool	14-8
ipv6 dhcp pool	14-9
ip dhcp relay information option vpn	14-9
ip dhcp send-all-options	14-10
domain-name	14-11
dns-server	14-12
nis-domain-name	14-13
nis-server	14-13
nisp-domain-name	14-14
nisp-server	14-15
sip-domain-name	14-15
sip-server	14-16
sntp-server	14-17
unicast-server	14-17
information-refresh	14-18
netbios-name-server	14-19

For information about...	Refer to page...
netbios-node-type	14-20
default-router	14-20
bootfile	14-21
next-server	14-22
option	14-22
lease	14-23
host	14-24
client-class	14-24
client-identifier	14-25
client-name	14-26
hardware-address	14-26
show ip dhcp binding	14-27
clear ip dhcp binding	14-28
show ip dhcp server statistics	14-28
clear ip dhcp server statistics	14-29

ip dhcp server

Use this command to enable DHCP server features on a routing interface.

Syntax

```
ip dhcp server
no ip dhcp
```

Parameters

None.

Defaults

None.

Mode

Interface configuration command mode.

Usage

The “no” form of this command disables DHCP server features on a routing interface.

Example

This example shows how to enable DHCP server on VLAN 1:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip dhcp server
```

ipv6 dhcp server

Use this command to enable an DHCPv6 server pool to process requests from a client.

Syntax

ipv6 dhcp server *poolname*

no ipv6 dhcp server *poolname*

Parameters

poolname	Specifies the DHCPv6 pool used to process requests from a client

Defaults

None.

Mode

Interface configuration command mode.

Usage

The DHCPv6 server pool is created using "ipv6 dhcp pool" on page 14-9.

The "no" form of this command removes the DHCPv6 server pool configuration on the interface.

Example

This example shows how to enable the DHCPv6 server on VLAN **1** to process client requests using the **docPool** DHCPv6 server pool:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ipv6 dhcp server docPool
```

ipv6 dhcp relay source-interface

Use this command to specify the source interface of IPv6 DHCP relay forwarded messages.

Syntax

ipv6 dhcp relay source-interface *interface*

no ipv6 dhcp relay source-interface *interface*

Parameters

interface	Specifies the source interface of relayed messages. Defaults to the interface the DHCP relay is configured on.

Defaults

None.

Mode

Interface configuration.

Usage

You can configure a global source-interface for the device. The global source interface can be overridden at the interface level. Use the **ipv6 dhcp relay source-interface** command in global configuration mode to configure a global source interface or in interface configuration mode to override the global source interface configuration for the specified interface.

The **no ipv6 dhcp relay source-interface** command resets the source interface of IPv6 DHCP relay forwarded messages to the interface the DHCP relay is configured on.

Example

This example sets the source interface for IPv6 DHCP relayed messages to loopback interface 1:

```
S Chassis(su-config)->interface vlan 50
S Chassis(su-config-intf-vlan.0.50)->ipv6 dhcp relay source-interface lpbk.0.1
S Chassis(su-config-intf-vlan.0.50)->
```

ipv6 dhcp relay destination

Use this command to configure the IPv6 DHCP relay agent to forward an IPv6 DHCP request from a client or other relay agent to the destination server or relay agent address.

Syntax

ipv6 dhcp relay destination *ipv6-address* [*destination-interface*] [**global**] [**vrf** *vrf*]

no ipv6 dhcp relay destination *ipv6-address* [*destination-interface*] [**global**] [**vrf** *vrf*]

Parameters

ipv6-address	Specifies the DHCPv6 destination server address.
destination-interface	Optional, Specifies the destination interface when relaying link-local and multicast IPv6 addresses.
global	(Optional) Specifies that the default global forwarding table will be used for route lookup.
vrf *vrf*	(Optional) Specifies that the routing table of the specified VRF will be used for route lookup.

Defaults

If a destination interface is not specified, because the DHCPv6 server address is a global address, the interface is determined by a standard routing table lookup.

Mode

Interface configuration**.**

Usage

The DHCP Solicit message is a multicast message to the all DHCP server address (ff02::1:2). The all DHCP server address only crosses network segments when explicitly routed. If your network has multiple segments, you must configure a DHCP relay agent on the router interface for each segment, so that all DHCP solicit messages can be forwarded to your DHCP server.

The destination server interface must be specified when the DHCPv6 destination server address is either link-local or multicast IPv6. Specifying an interface is not required if the DHCPv6 destination server address is a global address.

The global address can be explicitly configured using the **global** option.

Use the VRF option to Specify a VRF routing table to use for route lookup.

The **no** option for this command removes the specified DHCPv6 destination server address.

Examples

This example sets the DHCPv6 destination server address to the link-local address fe80::21f:45ff:fe5b:f5cf and specifies VLAN 100 as the destination server interface:

```
S Chassis(su-config)->interface vlan 50
S Chassis(su-config-intf-vlan.0.50)->ipv6 dhcp relay destination
fe80::21f:45ff:fe5b:f5cf vlan.0.100
S Chassis(su-config-intf-vlan.0.50)->
```

This example sets the DHCPv6 destination server address to 2001:2010::00aa:

```
S Chassis(su-config)->interface vlan 50
S Chassis(su-config-intf-vlan.0.50)->ipv6 dhcp relay destination 2001:2010::00aa
S Chassis(su-config-intf-vlan.0.50)->
```

show ip local pool

Use this command to display IP local address pool statistics.

Syntax

show ip local pool [*pool*]

Parameters

pool	(Optional) Display the specified local address pool.

Defaults

If *pool* is not specified, information about all local address pools will be shown.

Mode

All command modes.

Example

This example shows statistics information for the configured local address pools on this device:

```
S Chassis(rw)->show ip local pool

-----------IP Pools Statistics-----------
Pool           Subnet          Mask            Free   In use Reserved Excluded
pool1          10.60.1.0       255.255.255.0   256    0      0        0
S Chassis(rw)->
```

ip local pool

Use this command to configure a local address pool. This defines a range of IP addresses which can be used by the DHCP server and enables IP local pool configuration mode.

Syntax

ip local pool *name subnet mask*

no ip local pool *name*

Parameters

name	Specifies a name for the local address pool.
subnet	Specifies an IP subnet for the local address pool.
mask	Specifies a subnet mask for the local address pool. Valid entries are of the form: x.x.x.x or /x.

Defaults

None.

Mode

Configuration command mode.

Usage

The “no” form of this command removes the local address pool.

Example

This example shows how to configure a local address pool called “localpool” on IP subnet 172.20.28.0/24 and enter configuration mode for that pool. Mask can also be expressed as 255.255.255.0:

```
S Chassis(rw-config)->ip local pool localpool 172.20.28.0/24
S Chassis(rw-config-dhcp-pool)->
```

exclude

Use this command to exclude one or more addresses from a DHCP local address pool.

Syntax

exclude *ip-address number*

no exclude *ip-address number*

Parameters

ip-address	Specifies the starting IP address to be excluded from this pool.
number	Specifies the number of addresses to be excluded. Valid values are **1** - **65535**.

Defaults

None.

Mode

Local pool configuration command mode.

Usage

Using the exclude command to add or delete addresses of an active pool (a pool is active if the **ip dhcp pool** command has been entered for that pool) will remove any active leases from the database as part of the underlying processing of recreating the DHCP pool.

The "no" form of this command removes the addresses from the list of addresses excluded from the local pool.

Example

This example shows how to exclude two IP addresses beginning with 172.20.28.253 from the "localpool" address pool (IP addresses 172.20.28.253 and 172.20.28.254 are excluded):

```
S Chassis(rw-config)->ip local pool localpool
S Chassis(rw-config-dhcp-pool)->exclude 172.20.28.253 2
```

ip dhcp ping packets

Use this command to specify the number of packets a DHCP Server sends to a pool address before assigning the address to a requesting client.

Syntax

ip dhcp ping packets *number*

no ip dhcp ping packets

Parameters

number	Specifies the number of ping packets to be sent. Valid values are **0** - **10**. Default is **2**.

Defaults

None.

Mode

Configuration command.

Usage

The "no" form of this command resets the number of ping packets to the default value.

A value of 0 prevents the server from pinging IP addresses.

Example

This example shows how to set the number of DHCP ping attempts to 6:

```
S Chassis(rw-config)->ip dhcp ping packets 6
```

ip dhcp ping timeout

Use this command to specify the amount of time the DHCP server will wait for a ping reply from an IP address before timing out.

Syntax

ip dhcp ping timeout *milliseconds*

no ip dhcp ping timeout

Parameters

milliseconds	Specifies the ping timeout in milliseconds. Valid values are **100** to **10000**. Default: **500** milliseconds.

Defaults

None.

Mode

Configuration command.

Usage

The "no" form of this command resets the ping timeout to the default value.

Example

This example shows how to set the DHCP ping timeout to 900 milliseconds:

```
S Chassis(rw-config)->ip dhcp ping timeout 900
```

ip dhcp pool

Use this command to assign a local pool of addresses as a DHCP pool, and to enable DHCP address pool configuration mode.

Syntax

ip dhcp pool *name*

no ip dhcp pool *name*

Parameters

name	Specifies a DHCP address pool name. **Note:** This must match the previously configured name assigned with the ip local pool command as described in "ip local pool" on page 14-6.

Defaults

None.

Mode

Configuration command mode.

Usage

The “no” form of this command deletes a DHCP address pool.

Example

This example shows how to assign the name “localpool” as a DHCP address pool, and enable configuration mode for that address pool:

```
S Chassis(rw-config)->ip dhcp pool localpool
S Chassis(rw-config-dhcp-pool)->
```

ipv6 dhcp pool

Use this command to configure a DHCPv6 server information pool and enter DHCP pool configuration mode to add DHCP information options.

Syntax

ipv6 dhcp pool *poolname*

no ipv6 dhcp pool *poolname*

Parameters

poolname	Specifies a name for the DHCPv6 server information options pool.

Defaults

None.

Mode

Configuration command mode.

Usage

The “no” form of this command removes the DHCPv6 server information pool.

Example

This example shows how to create the **docPool** DHCPv6 server information pool and enter DHCP pool configuration mode:

```
S Chassis(rw-config)->ipv6 dhcp pool docPool
S Chassis(rw-config-dhcp-v6-pool)->
```

ip dhcp relay information option vpn

Use this command to force the DHCP server to send the VPN option (82) to the client.

Syntax

ip dhcp relay information option vpn

no ip dhcp relay information option vpn

Parameters

None.

Defaults

None.

Mode

VRF Configuration command mode.

Usage

When forwarding the local UDP broadcasts from a VRF to a destination address on the global router or a different VRF, the DHCP relay agent must include information about itself that the DHCP server will forward to the client. Including Option 82 in the DHCP relay information provides the required DHCP relay information. Use the **ip dhcp relay information option vpn** command to include DHCP relay agent information in the packet sent to the client by the DHCP server. See “ip helper-address” on page 60-11 for details on changing the destination address for the forwarding of local UDP broadcasts.

The “no” form of this command removes the sending of Option 82 in the DHCP relay information.

Example

The following example:

- Enables IP forwarding for the UPD protocol on VRF “Alpha-Group”
- Enables DHCP/BOOTP relay on VLAN 10 of VRF “Alpha-Group” and sets the new destination address to 134.141.95.105 on VRF “Internet-Access”
- Configures the inclusion of DHCP relay agent information in the packet sent from the DHCP server to the client

```
S Chassis(su)->router Alpha-Group
S Chassis(su-*ha-Group)->configure
S Chassis(su-*ha-Group-config)->ip forward-protocol udp
S Chassis(su-*ha-Group-config)->interface vlan.0.10
S Chassis(su-*ha-Group-config-intf-vlan.0.10)->ip helper-address 134.141.95.105
vrf Internet-Access
S Chassis(su-*ha-Group-config-intf-vlan.0.10)->exit
S Chassis(su-*ha-Group-config)->ip dhcp relay information option vpn
S Chassis(su-*ha-Group-config)->
```

ip dhcp send-all-options

Use this command to force the DHCP server to send all configured options for this DHCP context to the client.

Syntax

ip dhcp send-all-options

no ip dhcp send-all-options

Parameters

None.

Defaults

None.

Mode

Configuration command mode.

Usage

Some clients do not have the ability to request all the options that might be configured in a DHCP context. This command provides for forcing the DHCP server to send out all the configured options for this DHCP context.

The "no" form of this command removes the sending of all configured options to the client by the DHCP server.

Example

This example shows how to configure VRF "Alpha-Group to force the DHCP server to send all configured options to the client:

```
S Chassis(su-*ha-Group-config)->ip dhcp send-all-options
S Chassis(su-*ha-Group-config)->
```

domain-name

Use this command to return one or more domain names when responding to a DHCP or DHCPv6 client request.

Syntax

domain-name *domain* [*domain2 ... domain8*]

no domain-name *domain* [*domain2 ... domain8*]

Parameters

domain	Specifies a domain name string.
[*domain2 ... domain8*]	(Optional) Specifies up to seven additional domain name strings separated by spaces.

Defaults

If additional optional domains are not specified, only the specified domain is configured.

Mode

DHCP address pool, class, or host configuration command mode for IPv4; DHCPv6 server information options pool configuration command mode for IPv6.

Usage

This command configures either the IPv4 DHCP option 15 in an IPv4 address DHCP server pool context or the DHCPv6 option 24 in an IPv6 information DHCP server pool context.

The “no” form of this command deletes the specified DHCP domain name(s).

Example

This example shows how to assign the **myEnterprise.com** domain name to the IPv4 **localpool** address pool:

```
S Chassis(rw-config)->ip dhcp pool localpool
S Chassis(rw-config-dhcp-v6-pool)->domain-name myEnterprise.com
```

This example shows how to assign the **myEnterprise.com** domain name to the **docPool** DHCPv6 server information options pool:

```
S Chassis(rw-config)->ipv6 dhcp pool docPool
S Chassis(rw-config-dhcp-pool)->domain-name myEnterprise.com
```

dns-server

Use this command to assign one or more DNS servers to DHCP or DHCPv6 clients.

Syntax

dns-server *address* [*address2...address8*]

no dns-server *address* [*address2...address8*]

Parameters

address	Specifies the IPv4 or IPv6 address of a DNS server.
address2... address8	(Optional) Specifies, in order of preference, up to 7 additional DNS server IPv4 or IPv6 address(es).

Defaults

If *address2...address8* is not specified, no additional addresses will be configured.

Mode

DHCP address pool, class, or host configuration command mode for IPv4; DHCPv6 server information options pool configuration command mode for IPv6.

Usage

This command configures either IPv4 DHCP option 6 or DHCPv6 option 23.

The “no” form of this command deletes the DNS servers.

Example

This example shows how to assign an IPv4 DNS server at address **11.12.1.99** to the **localpool** address pool:

```
S Chassis(rw-config)->ip dhcp pool localpool
S Chassis(rw-config-dhcp-pool)->dns-server 11.12.1.99
```

This example shows how to assign an IPv6 DNS server at addresses **1111::12**, **1111::13**, and **1111::14** to the **docPool** DHCPv6 server information options pool:

```
S Chassis(rw-config)->ipv6 dhcp pool docPool
S Chassis(rw-config-dhcp-v6-pool)->dns-server 1111::12 1111::13 1111::14
```

nis-domain-name

Use this command to return one or more Network Information Services (NIS) domain names when responding to a DHCPv6 client request.

Syntax

nis-domain-name *domain* [*domain2 ... domain8*]

no nis-domain-name *domain* [*domain2 ... domain8*]

Parameters

domain	Specifies a domain name string.
[*domain2 ... domain8*]	(Optional) Specifies up to seven additional domain name strings separated by spaces.

Defaults

If additional optional domains are not specified, only the specified domain is configured.

Mode

DHCPv6 server information options pool configuration command mode.

Usage

This command configures the DHCPv6 option 29 in an IPv6 information DHCPv6 server pool context.

The "no" form of this command deletes the specified NIS DHCPv6 domain name(s).

Example

This example shows how to assign the **myNisEnterprise.com** NIS domain name to the **docPool** DHCPv6 server information options pool:

```
S Chassis(rw-config)->ipv6 dhcp pool docPool
S Chassis(rw-config-dhcp-pool)->nis-domain-name myNisEnterprise.com
```

nis-server

Use this command to assign one or more Network Information Services (NIS) servers to DHCPv6 clients.

Syntax

nis-server *address* [*address2...address8*]

no nis-server *address* [*address2...address8*]

Parameters

address	Specifies the IPv6 address of a NIS server.
address2... address8	(Optional) Specifies, in order of preference, up to 7 additional DNS server IPv6 address(es).

Defaults

If *address2...address8* is not specified, no additional addresses will be configured.

Mode

DHCPv6 server information options pool configuration command mode.

Usage

This command configures DHCPv6 option 27.

The "no" form of this command deletes the DNS servers.

Example

This example shows how to assign an IPv6 NIS-DNS server at addresses **1111::12**, **1111::13**, and **1111::14** to the **docPool** DHCPv6 server information options pool:

```
S Chassis(rw-config)->ipv6 dhcp pool docPool
S Chassis(rw-config-dhcp-v6-pool)->nis-dns-server 1111::12 1111::13 1111::14
```

nisp-domain-name

Use this command to return one or more Network Information Services (NIS) version 2 domain names when responding to a DHCPv6 client request.

Syntax

nisp-domain-name *domain* [*domain2 ... domain8*]

no nisp-domain-name *domain* [*domain2 ... domain8*]

Parameters

domain	Specifies a domain name string.
[*domain2 ... domain8*]	(Optional) Specifies up to seven additional domain name strings separated by spaces.

Defaults

If additional optional domains are not specified, only the specified domain is configured.

Mode

DHCPv6 server information options pool configuration command mode.

Usage

This command configures the DHCPv6 option 30 in an IPv6 information DHCPv6 server pool context.

The "no" form of this command deletes the specified NISP DHCPv6 domain name(s).

Example

This example shows how to assign the **myNispEnterprise.com** NISP domain name to the **docPool** DHCPv6 server information options pool:

```
S Chassis(rw-config)->ipv6 dhcp pool docPool
S Chassis(rw-config-dhcp-pool)->nisp-domain-name myNispEnterprise.com
```

nisp-server

Use this command to assign one or more Network Information Services (NIS) version 2 servers to DHCPv6 clients.

Syntax

nis-server *address* [*address2...address8*]

no nis-server *address* [*address2...address8*]

Parameters

address	Specifies the IPv6 address of a NIS server.
address2... address8	(Optional) Specifies, in order of preference, up to 7 additional DNS server IPv6 address(es).

Defaults

If *address2...address8* is not specified, no additional addresses will be configured.

Mode

DHCPv6 server information options pool configuration command mode for IPv6.

Usage

This command configures DHCPv6 option 28.

The "no" form of this command deletes the NISP DNS servers.

Example

This example shows how to assign an IPv6 NIS-DNS server at addresses **1111::12**, **1111::13**, and **1111::14** to the **docPool** DHCPv6 server information options pool:

```
S Chassis(rw-config)->ipv6 dhcp pool docPool
S Chassis(rw-config-dhcp-v6-pool)->nis-dns-server 1111::12 1111::13 1111::14
```

sip-domain-name

Use this command to return one or more Session Initiation Protocol (SIP) domain names when responding to a DHCPv6 client request.

Syntax

sip-domain-name *domain* [*domain2 ... domain8*]

no sip-domain-name *domain* [*domain2 ... domain8*]

Parameters

domain	Specifies a domain name string.
[*domain2 ... domain*8]	(Optional) Specifies up to seven additional domain name strings separated by spaces.

Defaults

If additional optional domains are not specified, only the specified domain is configured.

Mode

DHCPv6 server information options pool configuration command mode.

Usage

This command configures the DHCPv6 SIP domain name option in an IPv6 information DHCPv6 server pool context.

The "no" form of this command deletes the specified SIP DHCPv6 domain name(s).

Example

This example shows how to assign the **mySipEnterprise.com** SIP domain name to the **docPool** DHCPv6 server information options pool:

```
S Chassis(rw-config)->ipv6 dhcp pool docPool
S Chassis(rw-config-dhcp-pool)->nisp-domain-name mySipEnterprise.com
```

sip-server

Use this command to assign one or more Session Initiation Protocol (SIP) servers to DHCPv6 clients.

Syntax

sip-server *address* [*address2...address8*]

no sip-server *address* [*address2...address8*]

Parameters

address	Specifies the IPv6 address of a SIP server.
address2... address8	(Optional) Specifies, in order of preference, up to 7 additional SIP server IPv6 address(es).

Defaults

If *address2...address8* is not specified, no additional addresses will be configured.

Mode

DHCPv6 server information options pool configuration command mode for IPv6.

Usage

This command configures DHCPv6 server option 22 in an IPv6 information DHCPv6 server pool context.

The “no” form of this command deletes the SIP servers.

Example

This example shows how to assign an IPv6 SIP server at addresses **1111::12**, **1111::13**, and **1111::14** to the **docPool** DHCPv6 server information options pool:

```
S Chassis(rw-config)->ipv6 dhcp pool docPool
S Chassis(rw-config-dhcp-v6-pool)->sip-dns-server 1111::12 1111::13 1111::14
```

sntp-server

Use this command to assign a Simple Network Time Protocol (SNTP) server to DHCPv6 clients.

Syntax

sntp-server *address*

no sntp-server *address*

Parameters

address	Specifies the IPv6 address of a SNTP server.

Defaults

None.

Mode

DHCPv6 server information options pool configuration command mode for IPv6.

Usage

This command configures DHCPv6 server option 31 in an IPv6 information DHCPv6 server pool context.

The “no” form of this command deletes the SNTP servers.

Example

This example shows how to assign an IPv6 SNTP server at address **1111::15** to the **docPool** DHCPv6 server information options pool:

```
S Chassis(rw-config)->ipv6 dhcp pool docPool
S Chassis(rw-config-dhcp-v6-pool)->sntp-server 1111::15
```

unicast-server

Use this command to assign a unicast server to DHCPv6 clients.

Syntax

unicast-server *address*

no unicast-server *address*

Parameters

address	Specifies the IPv6 address of a unicast server.

Defaults

None.

Mode

DHCPv6 server information options pool configuration command mode for IPv6.

Usage

This command configures DHCPv6 server option 12 in an IPv6 information DHCPv6 server pool context.

The "no" form of this command deletes the unicast server.

Example

This example shows how to assign an IPv6 unicast server at address **1111::15** to the **docPool** DHCPv6 server information options pool:

```
S Chassis(rw-config)->ipv6 dhcp pool docPool
S Chassis(rw-config-dhcp-v6-pool)->unicast-server 1111::15
```

information-refresh

Use this command to configure the amount of time a client should wait before refreshing information from the DHCPv6 server.

Syntax

information-refresh {**infinite** | *days* [[*hours*] [*minutes*]}

no information-refresh {**infinite** | *days* [[*hours*] [*minutes*]}

Parameters

infinite	Specifies that clients will not request an information refresh from the DHCPv6 server.
days	Specifies the number of days a client waits before requesting an information refresh from the DHCPv6 server. Valid values are 0 - 365.
hours	(Optional) Specifies the number of hours a client waits before requesting an information refresh from the DHCPv6 server. Valid values are **0** - **23**. Default value is **0**.
minutes	Specifies the number of minutes a client waits before requesting an information refresh from the DHCPv6 server. Valid values are **0** - **59**. Default value is **0**.

Defaults

Information refresh defaults to **1** day. If *hours* and *minutes* are not specified, the default is **0** in both cases.

Mode

DHCPv6 server information options pool configuration command mode for IPv6.

Usage

This command configures DHCPv6 server option 32 in an IPv6 information DHCP server pool context.

The “no” form of this command deletes the unicast server.

Example

This example shows how to configure the time the client will wait before requesting an information refresh from the DHCPv6 server to 12 hours:

```
S Chassis(rw-config)->ipv6 dhcp pool docPool
S Chassis(rw-config-dhcp-v6-pool)->information-refresh 0 12 0
```

netbios-name-server

Use this command to assign one or more NetBIOS WINS servers to DHCP clients.

Syntax

netbios-name-server *address* [*address2...address8*]

no netbios-name-server *address* [*address2...address8*]

Parameters

address	Specifies the IP address of a NetBIOS WINS server.
address2... address8	(Optional) Specifies, in order of preference, up to 7 additional NetBIOS WINS server IP address(es).

Defaults

If *address2...address8* is not specified, no additional addresses will be configured.

Mode

DHCP address pool, class, or host configuration command mode.

Usage

This command configures DHCP option 44.

The “no” form of this command deletes the NetBIOS WINS servers.

Example

This example shows how to assign a NetBIOS WINS server at 13.12.1.90 to the “localpool” address pool:

```
S Chassis(rw-config)->ip dhcp pool localpool
S Chassis(rw-config-dhcp-pool)->netbios-name-server 13.12.1.90
```

netbios-node-type

Use this command to assign a NetBIOS node (server) type to DHCP clients.

Syntax

netbios-node-type *type*

no netbios-node-type *type*

Parameters

type	Specifies the NetBIOS node type. Valid values and their corresponding types are: • **h-node** — hybrid (recommended) • **b-node** — broadcast • **p-node** — peer-to-peer • **m-mode** — mixed

Defaults

None.

Mode

DHCP address pool, class, or host configuration mode. Read-Write

Usage

This command configures DHCP option 46.

The “no” form of this command deletes the NetBIOS node type.

Example

This example shows how to specify hybrid as the NetBIOS node type for the “localpool” address pool:

```
S Chassis(rw-config)->ip dhcp pool localpool
S Chassis(rw-config-dhcp-pool)->netbios-node type h-node
```

default-router

Use this command to assign a default router list to DHCP clients.

Syntax

default-router *address* [*address2...address8*]

no default-router *address* [*address2...address8*]

Parameters

address	Specifies the IP address of a default router.
address2... address8	(Optional) Specifies, in order of preference, up to 7 additional default router IP address(es).

Defaults

If *address2...address8* is not specified, no additional addresses will be configured.

Mode

DHCP address pool, class, or host configuration command mode.

Usage

This command configures DHCP option 3.

The "no" form of this command deletes the default routers.

Example

This example shows how to assign a default router at 14.12.1.99 to the "localpool" address pool:

```
S Chassis(rw-config)->ip dhcp pool localpool
S Chassis(rw-config-dhcp-pool)->default-router 14.12.1.99
```

bootfile

Use this command to specify the default boot image for a DHCP client.

Syntax

bootfile *filename*

no bootfile *filename*

Parameters

filename	Specifies the boot image file name.

Defaults

None.

Mode

DHCP address pool, class, or host configuration command mode.

Usage

The "no" form of this command deletes the boot image association.

Example

This example shows how to specify "dhcpboot" as the boot image file in the "localpool" address pool:

```
S Chassis(rw-config)->ip dhcp pool localpool
S Chassis(rw-config-dhcp-pool)->bootfile dhcpboot
```

next-server

Use this command to specify the next server in the DHCP server boot process.

Syntax

next-server *ip-address*

no next-server *ip-address*

Parameters

ip-address	Specifies the next server in the boot process by IP address.

Defaults

None.

Mode

DHCP address pool, class, or host configuration command mode.

Usage

The next server is the server the client will contact for the boot file if the primary server is not able to supply it. A next server is usually specified in a manual DHCP binding configuration in order to provide an IP address to a BOOTP client and allow the client to receive the TFTP server address when downloading a boot file image.

The "no" form of this command removes the next server.

Example

This example shows how to specify 192.168.42.13 as the next server in the boot process:

```
S Chassis(rw-config)->ip dhcp pool localpool
S Chassis(rw-config-dhcp-pool)->next-server 192.168.42.13
```

option

Use this command to configure DHCP options.

Syntax

option *code* [**instance** *number*] {**ascii** *string* | **hex** *string* | **ip** *address*}

no option *code* [**instance** *number*] {**ascii** *string* | **hex** *string* | **ip** *address*}

Parameters

code	Specifies a DHCP option code. Valid Values: **0** - **254**.
instance *number*	(Optional) Assigns an instance number to this option. Valid values are **0** to **255**. The default instance is **0**.
ascii *string* | **hex** *string* | **ip** *address*	Specifies a *code* parameter. An ASCII character string containing a space must be enclosed in quotations.

Defaults

If **instance** is not specified, the default instance of **0** is applied.

Mode

DHCP address pool, class, or host configuration command mode.

Usage

These configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message to network hosts. Several commonly-used options may also be configured using dedicated commands: “domain-name” on page 14-11, “dns-server” on page 14-12, “netbios-name-server” on page 14-19, “netbios-node-type” on page 14-20, and “default-router” on page 14-20.

The parameter format of a site-specific option must be either ascii or hex.

The “no” form of this command deletes a configured DHCP option.

Examples

This example shows how to configure DHCP option 19, which specifies whether the client should configure its IP layer for packet forwarding. In this case, IP forwarding is enabled with the 01 value:

```
S Chassis(rw-config)->ip dhcp pool localpool
S Chassis(rw-config-dhcp-pool)->option 19 hex 01
```

This example shows how to configure DHCP option 72, which assigns one or more Web servers for DHCP clients:

```
S Chassis(rw-config)->ip dhcp pool localpool
S Chassis(rw-config-dhcp-pool)->option 72 ip 168.24.3.252
```

lease

Use this command to specify the duration of the lease for an IP address assigned by a DHCP server to a client.

Syntax

lease {*days* [*hours*] [*minutes*]}

no lease {*days* [*hours*] [*minutes*]}

Parameters

days	Specifies the number of days an address lease will remain valid.
hours	(Optional) When a *days* value has been assigned, specifies the number of hour an address lease will remain valid.
minutes	(Optional) When a *days* value has been assigned, specifies the number of minutes an address lease will remain valid.

Defaults

If *hours* or *minutes* are not specified, no values will be configured for the hours and minutes, and only the days value will apply.

Mode

DHCP address pool or class configuration command mode.

Usage

The “no” form of this command resets the lease duration to the default value of 1 day (24 hours).

Example

This example shows how to set a one-hour lease to the “localpool” address pool:

```
S Chassis(rw-config)->ip dhcp pool localpool
S Chassis(rw-config-dhcp-pool)->lease 0 1
```

host

Use this command to specify an IP address and network mask for manual DHCP binding.

Syntax

host *address* [*mask* | *prefix-length*]

no host *address* [*mask* | *prefix-length*]

Parameters

address	Specifies the IP address of the DHCP client.
mask | *prefix-length*	(Optional) Specifies a network mask or prefix for the IP address.

Defaults

If not specified, DHCP server will examine its defined IP address pools for a *mask* or *prefix-length*.

Mode

DHCP address pool configuration command mode.

Usage

The “no” form of this command removes the client IP address.

Example

This example shows how to set 15.12.1.99 255.255.248.0 as the IP address and subnet mask of a client in the “localpool” address pool:

```
S Chassis(rw-config)->ip dhcp pool localpool
S Chassis(rw-config-dhcp-pool)->hardware-address 0e-fd-04-20-00-01
S Chassis(rw-config-dhcp-host)->host 15.12.1.99 255.255.248.0
```

client-class

Use this command to identify a DHCP client class.

Syntax

client-class *name*

no client-class *name*

Parameters

name	Specifies a name for a DHCP client class.

Defaults

None.

Mode

DHCP address pool configuration command mode.

Usage

By giving a set of client class properties a name, using this command allows you to assign properties to all DHCP clients within the class rather than configuring each client separately. This command also enables DHCP class configuration mode.

The "no" form of this command deletes a client class name.

Example

This example shows how to assign "clientclass1" as a client class name in the "localpool" address pool:

```
S Chassis(rw-config)->ip dhcp pool localpool
S Chassis(rw-config-dhcp-pool)->client-class clientclass1
S Chassis(rw-config-dhcp-class)->
```

client-identifier

Use this command to enable DHCP host configuration mode and optionally associate a client class with a DHCP client.

Syntax

client-identifier *unique-identifier* [**client-class** *name*]

no client-identifier *unique-identifier*

Parameters

unique-identifier	Specifies the client's unique-identifier.
client-class *name*	(Optional) Specifies the class to which this client will be assigned. Must be configured using the client-class name as described in "client-class" on page 14-24.

Defaults

If **client-class** is not specified, none will be assigned.

Mode

DHCP address pool configuration command mode.

Usage

The "no" form of this command deletes a client identifier.

Example

This example shows how to create a client-identifier with an identifier of 010e.fd04.2000.01 and assign the client-class clientclass1 to it:

```
S Chassis(rw-config)->ip dhcp pool localpool
S Chassis(rw-config-dhcp-pool)->client-identifier 010e.fd04.2000.01 client-class
clientclass1
S Chassis(rw-config-dhcp-host)->
```

client-name

Use this command to assign a name and optionally associate a client class with a DHCP client.

Syntax

client-name *name* [**client-class** *name*]

no client-name *name*

Parameters

name	Specifies a name for a DHCP client. **Note:** The client name should not include the domain name.
client-class *name*	(Optional) Specifies the class to which this client will be assigned. Must be configured using the client-class name as described in "client-class" on page 14-24.

Defaults

If **client-class** is not specified, none will be assigned.

Mode

DHCP host configuration command mode.

Usage

The "no" form of this command deletes a client name.

Example

This example shows how to assign "soho1" as a client name in "clientclass1":

```
S Chassis(rw-config)->ip dhcp pool localpool
S Chassis(rw-config-dhcp-pool)->client-identifier 010e.fd04.2000.01 client-class
clientclass1
S Chassis(rw-config-dhcp-host)->client-name soho1 client-class clientclass1
```

hardware-address

Use this command to specify parameters for a new DHCP client address.

Syntax

hardware-address *hardware-address* [*type*]

no hardware-address *hardware-address* [*type*]

Parameters

hardware-address	Specifies the MAC address of the client's hardware platform.
type	(Optional) Specifies a hardware protocol or client class name. Valid values and their corresponding meanings are: • **1** or **ethernet** - 10Mb Ethernet • **6** or **ieee802** - IEEE 802 networks • **client-class** *name* - Client class (configured as described in "client-identifier" on page 14-25).

Defaults

If *type* is not specified, Ethernet will be applied.

Mode

DHCP address pool configuration command mode.

Usage

This command also enables DHCP host configuration mode.

The "no" form of this command removes the hardware address.

Example

This example shows how to specify 0001.f401.2710 as an Ethernet MAC address for the "localpool" address pool:

```
S Chassis(rw-config)->ip dhcp pool localpool
S Chassis(rw-config-dhcp-pool)->hardware-address 0001.f401.2710 ethernet
S Chassis(rw-config-dhcp-host)->
```

show ip dhcp binding

Use this command to display information about one or all DHCP address bindings.

Syntax

show ip dhcp binding [*ip-address*]

Parameters

ip-address	(Optional) Displays bindings for a specific client IP address.

Defaults

If *ip-address* is not specified, information about all address bindings will be shown.

Mode

All command modes.

Example

This example shows how to display the DHCP binding address parameters, including an associated Ethernet MAC addresses, lease expiration dates, type of address assignments, and whether the lease is active:

```
S Chassis(rw-config-dhcp-pool)->show ip dhcp binding 172.28.1.249

IP address       Hardware address    Lease expiration       Type       Act.
172.28.1.249     00a0.c976.6d38      Infinite               Automatic  Y
S Chassis(rw-config-dhcp-pool)->
```

clear ip dhcp binding

Use this command to delete one or all automatic DHCP address bindings.

Syntax

clear ip dhcp binding {*address* | *****}

Parameters

address | *****	Specifies an automatic address binding to be deleted, or that all automatic bindings will be deleted (*).

Defaults

None.

Mode

Configuration command mode.

Example

This example shows how to delete the address binding 18.12.22.99 from the DHCP server bindings database:

```
S Chassis(rw-config)->clear ip dhcp binding 18.12.22.99
```

show ip dhcp server statistics

Use this command to display DHCP server statistics.

Syntax

show ip dhcp server statistics

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display DHCP server statistics:

```
S Chassis(su-router-#)->show ip dhcp server statistics

Message                Received
BOOTREQUEST            0
DHCPDISCOVER           0
DHCPREQUEST            646
DHCPDECLINE            0
DHCPRELEASE            0
DHCPINFORM             0

Message                Sent
BOOTREPLY              0
DHCPOFFER              0
DHCPACK                646
DHCPNAK                0
```

clear ip dhcp server statistics

Use this command to reset all DHCP server counters.

Syntax

clear ip dhcp server statistics

Parameters

None.

Defaults

None.

Mode

Configuration command mode.

Example

This example shows how to reset all DHCP server counters:

```
S Chassis(su-config)->clear ip dhcp server statistics
```

15

License Commands

This chapter provides detailed information for the license set of commands. To enable advanced features, such as the removal of per-port user restrictions, advanced redundant management, routing protocols, and extended ACLs on an S-Series device, you must purchase and activate a license key. For information about configuring licenses, refer to the "System Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

You must purchase a license for each S-Series module or chassis, as applicable, on which you want to activate a license. For example, if you want to activate the port capacity license (S-EOS-PPC) on all three access modules in an S3 chassis, you must purchase three S-EOS-PPC licenses.

For information about...	Refer to page...
set license	15-1
show license	15-2
clear license	15-3

set license

When you have purchased a license, use this command to activate licensed features. If you have activated a license on your S-Series device, a unique license key will display in the **show license** command output.

Syntax

set license {**port-capacity** | **user-capacity** | **l3-s150** | **l3-s130**} *license-key* [{**slot** | **chassis**} *value*]

Parameters

port-capacity	Removes the per-port user restrictions on the module or SSA. The port capacity license (S-EOS-PPC) applies to the S130 Class modules and S130 Class SSA only; it does not apply to the S150 Class modules or S150 Class SSA.
user-capacity	Sets the user capacity feature key.
2x-user-capacity	Sets the user capacity feature key.
l3-s150	Sets the S150 Class advanced routing feature key for an S-Series chassis. These routing features are in the S-EOS-L3-S150 license.
l3-s130	Sets the S130 Class advanced routing feature key for an S-Series chassis. These routing features are in the S-EOS-L3-S130 license.

license-key	Specifies your unique license key, in ASCII.
slot | **chassis** *value*	(Optional) Specifies the S-Series S130 Class module or SSA or the S-Series chassis on which the port capacity license (S-EOS-PPC) it will be activated. If you are activating the port capacity license on an SSA, use 1 as the slot number.

Defaults

If the **slot** option is not specified, the license is applied to all slots in the system.

Usage

The S-EOS-L3-S130 license is required to run VRF on the S130 class of fabrics or in the S3 chassis with S130 class I/O module installed. In a mixed chassis of S150 and S130 fabrics, the feature entitlement will revert to the S130 feature set and therefore a license would be required to run VRF in this mixed environment.

The S-EOS-L3-S150 license is not currently available. This license is reserved for future routing enhancements on the S150 class of fabrics.

S-Series license keys can contain white spaces; therefore, you should enclose your license key in double quotation marks.

Mode

All command modes.

Example

This example shows how to set the port capacity on the modules in slots 1 and 2:

```
S Chassis(rw)->set license port-capacity "0001:S-EOS-PPC:2:12345678:0:Enterprise
Name:0:abcdefgh:abcdefghijklmnopqrstuvwxyz123456" slot 1
```

```
S Chassis(rw)->set license port-capacity "0001:S-EOS-PPC:1:12345678:0:Enterprise
Name:0:abcdefgh:abcdefghijklmnopqrstuvwxyz123456" slot 2
```

This example shows how to set the enhanced access routing on an S-130 class fabric:

```
S Chassis(rw)->set license l3-s130 "0001:S-EOS-L3-S130:0:abcdefg:0:Extreme
Networks SQA:0:00000000:abcdefghij+abcdefghijklmnopqrst/abcdefghijklmnopqrstuv
/1234567890abcdefghijklmno/12345=="
```

show license

If you have activated a license on your S-Series device, use this command to display your license keys.

Syntax

```
show license
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

```
S Chassis(rw)->show license

License Type      Location  Status      Key
----------------  --------  ----------  ----------------------------------------
port-capacity     slot 1    active      0001:S-EOS-PPC:A:BCDEFGHI:0:Enterprise
Name:0:12345678:abcdefghijklmnopqrstuvwxyz123456
port-capacity     slot 2    active      0001:S-EOS-PPC:1:BCDEFGHI:0:Enterprise
Name:0:12345678:abcdefghijklmnopqrstuvwxyz123456
port-capacity     slot 3 active      0001:S-EOS-PPC:0:BCDEFGHI:0:Enterprise
Name:0:12345678:abcdefghijklmnopqrstuvwxyz123456
l3-s130          chassis   active     0001:S-EOS-L3-S130:0:abcdefg:0:Enterprise
Name:0:00000000:abcdefghij+abcdefghijklmnopqrst/abcdefghijklmnopqrstuv/123456789
0abcdefghijklmno/12345==
```

clear license

Use this command to clear license key settings.

Syntax

clear license {**port-capacity** | **user-capacity** | **l3-s150** | **l3-s130**} *license-key* [{**slot** | **chassis**} *value*]

Parameters

port-capacity	Clears the port capacity feature key from an S-Series S130 Class module or S130 Class SSA.
l3-s150	Clears the S150 Class advanced routing feature key from the S-Series chassis.
l3-s130	Clears the S130 Class advanced routing feature key from the S-Series chassis.
all	Clears all licenses.
slot | **chassis** *value*	Specifies the S-Series S130 Class module or S130 Class SSA from which the port capacity license will be cleared. If you are clearing the port capacity license on an SSA, use 1 as the slot number.

Defaults

None.

Mode

All command modes.

Example

This example clears the port-capacity license from slot 1 for the S-Series device:

```
S Chassis(rw)->clear license port-capacity slot 1
```

16

Power over Ethernet (PoE) Commands

Important Notice

This section applies only to PoE-equipped S-Series devices. Consult the *Hardware Installation Guide* or *Quick Reference* shipped with your product to determine if it is PoE-equipped.

This chapter provides detailed information for the Power over Ethernet (PoE) set of commands. PoE functionality includes: reviewing and setting PoE parameters, including the power available to the chassis, the usage threshold for each module, whether or not SNMP trap messages will be sent when power status changes, and per-port PoE settings. For information about configuring PoE, refer to the "Power over Ethernet Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show inlinepower	16-2
set inlinepower mode	16-3
clear inlinepower mode	16-3
set inlinepower available	16-4
clear inlinepower available	16-4
set inlinepower powertrap	16-5
clear inlinepower powertrap	16-5
set inlinepower assigned	16-6
clear inlinepower assigned	16-6
set inlinepower threshold	16-7
clear inlinepower threshold	16-7
set inlinepower management	16-8
clear inlinepower management	16-8
set inlinepower psetrap	16-9
clear inlinepower psetrap	16-10
show port inlinepower	16-10
set port inlinepower	16-11
clear port inlinepower	16-12

show inlinepower

Use this command to display device PoE properties.

Syntax

show inlinepower

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

The show inlinepower output will display eight powersupply status lines regardless of the number of bays in the PoE power shelf. It a power supply bay does not exist or there is no power supply installed, the status will read “not installed.”

Example

This example shows how to display PoE properties for this chassis.

```
S Chassis(rw)->show inlinepower
Total Power Detected    : 2400 Watts
Total Power Available   : 2400 Watts (100% of Total Power Detected)
Total Power Assigned    : 0 Watts
Power Allocation Mode   : auto
Power Trap Status       : disabled
Power Redundancy Status : not supported
Power Supply 1 Status   : installed and operating
Power Supply 2 Status   : not installed
Power Supply 3 Status   : not installed
Power Supply 4 Status   : installed and operating
Power Supply 5 Status   : not installed
Power Supply 6 Status   : not installed
Power Supply 7 Status   : not installed
Power Supply 8 Status   : not installed

Slot Oper   Power Power    Power     Class  Power Usage Usage PSE      Mgmt
     Status Limit Assigned Available Budget Usage       Trhld Trap     Mode
            (W)   (W)      (W)       (W)    (W)   (%)   (%)   Status
---- ------ ----- -------- --------- ------ ----- ----- ----- -------- ---------
1    on     1632  0        563              2     0     75    disabled real-time
2                 0
3                 0
```

```
4                 0
5                 0
6    on     2040  0        704              3     0     75    disabled real-time
7    on     1632  0        563              2     0     75    disabled real-time
8    off    1632  0        564              0     0     75    disabled real-time
```

set inlinepower mode

Use this command to set the chassis power allocation mode.

Syntax

set inlinepower mode {**auto** | **manual**}

Parameters

auto	Assigns automatic mode to chassis power allocation.
manual	Assigns manual mode to chassis power allocation. This setting allows the values configured with the **set inlinepower assigned** command (“set inlinepower assigned” on page 16-6) to be applied to PoE modules.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the chassis power allocation mode to manual:

```
S Chassis(rw)->set inlinepower mode manual
```

clear inlinepower mode

Use this command to reset chassis power allocation to the default mode of auto.

Syntax

clear inlinepower mode

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the chassis power allocation mode to auto:

```
S Chassis(rw)->clear inlinepower mode
```

set inlinepower available

Use this command to set the percentage of total power available that a chassis can use from the total power detected.

Syntax

set inlinepower available *max-percentage*

Parameters

max-percentage	Specifies the maximum PoE power available to this chassis as a percentage of the total installed PoE power. Valid values are **0–100**.

Defaults

None.

Mode

All command modes.

Usage

If the total power wattage value set with the **set inlinepower assigned** command ("set inlinepower assigned" on page 16-6) is greater than the maximum power percentage specified with this command, a warning will display.

Example

This example shows how to set the maximum inline power available to the chassis to 70 percent:

```
S Chassis(rw)->set inlinepower available 70
```

clear inlinepower available

Use this command to reset the percentage of the total inline power available to a chassis to the default value of 100.

Syntax

clear inlinepower available

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the maximum inline power available to the chassis to 100 percent:

```
S Chassis(rw)->clear inlinepower available
```

set inlinepower powertrap

Use this command to disable or enable the sending of an SNMP trap message whenever status changes occur in the chassis PoE power supplies or the PoE system redundancy.

Syntax

set inlinepower powertrap {**disable** | **enable**}

Parameters

disable | **enable**	Disables or enables trap messaging for the chassis PoE power supplies.

Defaults

None.

Mode

All command modes.

Example

This example shows how to enable a chassis power supplies trap:

```
S Chassis(rw)->set inlinepower powertrap enable
```

clear inlinepower powertrap

Use this command to reset chassis power trap messaging back to the default state of disabled.

Syntax

clear inlinepower powertrap

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset chassis power trap messaging to disabled:

```
S Chassis(rw)->clear inlinepower powertrap
```

set inlinepower assigned

Use this command to manually assign Power Sourcing Equipment (PSE) power to a module in the chassis.

Syntax

set inlinepower assigned *power-value slot-number*

Parameters

power-value	Specifies a power value in watts.
slot-number	Specifies a module slot location for the power assignment. If you are configuring this value on an SSA, use 1 as the slot number.

Defaults

None.

Mode

All command modes.

Usage

If the total power wattage value set with this command is greater than the maximum power percentage specified with the **set inlinepower available** command (“set inlinepower available” on page 16-4), a warning will display. If you execute these parameters, a ratio of assigned power is applied to each module.

Example

This example shows how to assign 200 watts of power to the module in slot 1:

```
S Chassis(rw)->set inlinepower assigned 200 1
```

clear inlinepower assigned

Use this command to clear the power value manually assigned to one or more modules.

Syntax

clear inlinepower assigned [*slot-number*]

Parameters

slot-number	(Optional) Clears the power assignment from a specific module. If you are clearing the assigned value on an SSA, use 1 as the slot number. If *slot-number* is not specified, power value assignments will be cleared from all modules.

Defaults

If *slot-number* is not specified, power value assignments will be cleared from all modules.

Mode

All command modes.

Example

This example shows how to clear power assignments to all modules in the chassis:

```
S Chassis(rw)->clear inlinepower assigned
```

set inlinepower threshold

Use this command to set the PoE usage threshold on a specified module.

Syntax

set inlinepower threshold *usage-threshold module-number*

Parameters

usage-threshold	Specifies a PoE threshold as a percentage of total system power usage. Valid values are **1–99**.
module-number	Specifies the module on which to set the PoE threshold. If you are configuring this value on an SSA, use 1 as the module number.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the PoE threshold to 50 on module 1:

```
S Chassis(rw)->set inlinepower threshold 50 1
```

clear inlinepower threshold

Use this command to reset the PoE usage threshold on a specified module to the default value of 75 percent.

Syntax

clear inlinepower threshold *module-number*

Parameters

module-number	Specifies the module on which to reset the PoE threshold. If you are clearing the threshold value on an SSA, use 1 as the module number.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the PoE threshold to 75 on module 1:

```
S Chassis(rw)->clear inlinepower threshold 1
```

set inlinepower management

Use this command to set the PoE management mode on a specified module.

Syntax

set inlinepower management {**realtime** | **class**} *module-number*

Parameters

realtime	Manages power based on the actual power consumption of the ports.
class	Manages power based on the IEEE 802.3af definition of the class upper limit.
module-number	Specifies the module on which to set the PoE management mode. If you are configuring this value on an SSA, use 1 as the module number.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the PoE management mode to “class” on module 1:

```
S Chassis(rw)->set inlinepower management class 1
```

clear inlinepower management

Use this command to reset the PoE management mode on a specified module back to the default setting of “realtime”.

Syntax

clear inlinepower management *module-number*

Parameters

module-number	Specifies the module on which to reset the PoE management mode. If you are clearing the management value on an SSA, use 1 as the module number.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the PoE management mode to "realtime" on module 1:

```
S Chassis(rw)->clear inlinepower management 1
```

set inlinepower psetrap

Use this command to enable or disable the sending of an SNMP trap message for a module whenever the status of its ports changes, or whenever the module's PoE usage threshold is crossed.

Syntax

set inlinepower psetrap {**disable** | **enable**} *module-number*

Parameters

disable | **enable**	Disables or enables PoE trap messaging.
module-number	Specifies the module on which to disable or enable trap messaging. If you are configuring this value on an SSA, use 1 as the module number.

Defaults

Disabled.

Mode

All command modes.

Usage

The module's PoE usage threshold must be set using the **set inlinepower threshold** command as described in "set inlinepower threshold" on page 16-7.

Example

This example shows how to enable PoE trap messaging on module 1:

```
S Chassis(rw)->set inlinepower psetrap enable 1
```

clear inlinepower psetrap

Use this command to reset PoE trap messaging for a module back to the default state of disabled.

Syntax

clear inlinepower psetrap *module-number*

Parameters

module-number	Specifies the module on which to clear PoE trap messaging. If you are clearing this value on an SSA, use 1 as the module number.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset PoE trap messaging for module 1 to disabled:

```
S Chassis(rw)->clear inlinepower psetrap 1
```

show port inlinepower

Use this command to display all ports supporting PoE.

Syntax

show port inlinepower *port-string*

Parameters

port-string	Displays information for specific PoE port(s).

Defaults

If not specified, information for all PoE ports will be displayed.

Mode

All command modes.

Example

This example shows how to display PoE information for Gigabit Ethernet port 1 on an SSA:

```
S Chassis(su)->show port inlinepower ge.1.1

Port    Type          Oper             Admin  Priority Class Power Power PD
        (truncated)   Status           Status                Limit Usage Type
                                                             (mW)  (mW)
------- ------------- ---------------- ------ -------- ----- ----- ----- -------
ge.1.1                other fault      auto   low      0     15400 0     other
```

set port inlinepower

Use this command to configure PoE parameters on one or more ports.

Syntax

set port inlinepower *port-string* {[**admin** {**off** | **auto**}] [**priority** {**critical** | **high** | **low**}] [**type** *type*] [**powerlimit** *powerlimit*] [**capability** *capability*]}

Parameters

port-string	Specifies the ports on which to configure PoE.
admin off | **auto**	Sets the PoE administrative state to off (disabled) or auto (on).
priority critical | **high** | **low**	Sets the ports priority for the PoE allocation algorithm to critical (highest), high or low.
type *type*	Specifies a string describing the type of device connected to a port.
powerlimit *powerlimit*	Sets the maximum power allowed on this port in watts. Valid values are 0–15400 for PoE 802.3af or 0–34000 for PoE 802.3at.
capability *capability*	Sets the PoE mode for the port. • 8023af—The port is running is 802.3af PoE mode (15.4W maximum power) • 8023at—The port is running in 802.3at PoE mode (34.0W maximum power)

Defaults

None.

Mode

All command modes.

Usage

To support 802.3at PDs, set **powerlimit** to the appropriate value in the 802.3at range and set **capability** to 8023at.

Example

This example shows how to enable 802.3at PoE on port ge.1.1:

```
S Chassis(rw)->set port inlinepower ge.1.1 admin auto powerlimit 34000 capability
8023at
```

clear port inlinepower

Use this command to reset PoE parameters on one or more ports to default values.

Syntax

clear port inlinepower *port-string* {[**admin**] [**priority**] [**type**] [**powerlimit**] [**capability**]}

Parameters

port-string	Specifies the port(s) on which to reset PoE.
admin	Resets the PoE administrative state to **auto** (on).
priority	Resets the port(s) priority for the PoE allocation algorithm to **low**.
type	Resets the port type to an empty string.
powerlimit	Resets the maximum power to 15400 watts.
capability	Resets the PoE mode to 802.3af (15.4W maximum power).

Defaults

None.

Mode

All command modes.

Example

This example shows how to rest the PoE priority on port ge.3.1 to low:

```
S Chassis(rw)->clear port inlinepower ge.3.1 priority
```

17

Configuration and Image File Management Commands

For information about...	Refer to page...
General Configuration and Image File Management Commands	17-1
Restore Point Commands	17-24

General Configuration and Image File Management Commands

This section provides detailed information for the general configuration and image file management set of commands. Configuration and image file management functionality includes viewing, managing and executing configuration and image files. For information about configuration and image file management, refer to the "Image Configuration and File Management" chapter of the *Extreme Networks S-Series Configuration Guide*. For information about configuring high availability firmware upgrades, refer to the "High Availability Firmware Upgrade (HAU) Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
dir	17-2
show boot system	17-5
set boot system	17-6
show boot high-availability	17-8
set boot high-availability group	17-11
clear boot high-availability group	17-12
set boot high-availability delay	17-13
clear boot high-availability delay	17-13
set boot high-availability default-mode	17-14
clear boot high-availability default-mode	17-15
set boot high-availability force-complete	17-15
show file	17-16
show config	17-18
configure	17-20
copy	17-21

For information about...	Refer to page...
delete	17-22
script	17-23

dir

Use this command to list files stored in the file system, on a particular slot, or on a USB device plugged into one of the USB ports.

Syntax

dir [*slotN* | *slotN/usbN*] [**images**] [*filename*]

Parameters

slotN | *slotN/usbN*	(Optional) Specifies the slot or USB subdirectory for which you want to list files. See the Usage information below for supported slot numbers and USB numbers for your chassis.
images	(Optional) Specifies that information for all images on the system will display.
filename	(Optional) Specifies the file, in the root directory or a subdirectory (slot or USB device directory), to list.

Defaults

If none of the optional parameters are specified, all files in the system will be displayed.

Mode

All command modes.

Usage

If you specify a specific slot with the **dir** command (for example, **dir slot2**), the output will list all files on the slot and any USB devices on the slot.

If you specify a specific USB device with the **dir** command (for example, **dir slot2/usb2**), the output will list only the files on the USB device on the slot.

The S-Series supports 2 USB ports. usb1 is the console port. usb2 is a port on a supported slot. USB ports are supported on the following slots, by chassis:

- **SSA** – slot 1
- **S3** chassis – slots 1, 2, and 3
- **S4** chassis – slots 3 and 4
- **S6** chassis – slots 3, 4, and 5
- **S8** chassis – slots 3, 4, and 5

More output detail is available for images on the system when specifying a particular image to view or using the **images** option to display detail for all images on the system.

If C2 security mode is enabled, the Secure directory, including all secure logs, can not be accessed while in Read-Write or Read-Only user modes.

Examples

This example shows how to list all the files in the system:

```
S Chassis(su)->dir
Images:
================================================================================
Filename:      S-76101-0002
Version:       07.61.01.0002
Size:          10845980 (bytes)
Date:          THU DEC 08 18:28:18 2011

Filename:      S-76101-0003 (Active) (Boot)
Version:       07.61.01.0003T
Size:          10846108 (bytes)
Date:          TUE DEC 13 18:27:22 2011

Files:
================================================================================
slot2:
AUG 22 2011  15:08:22           37332 ipstrc.log.gz
DEC 08 2011  14:50:54 <DIR>     16384 cores
NOV 04 2011  11:02:42            9759 031611
AUG 19 2011  08:28:08 <DIR>     16384 logs
DEC 02 2011  13:19:56           13090 120211
DEC 06 2011  11:06:56           14866 120611
DEC 13 2011  18:28:34           16577 121311

slot3:
OCT 20 2011  17:28:28 <DIR>     16384 cores
AUG 11 2011  14:27:00 <DIR>     16384 logs
JUL 08 2011  09:31:56 <DIR>     16384 secure
NOV 16 2011  15:47:10           10318 111611

slot4:
AUG 22 2011  15:08:38 <DIR>     16384 cores
JUN 29 2011  18:49:22 <DIR>     16384 logs
JUL 08 2011  09:31:58 <DIR>     16384 secure
```

This example shows how to list information about a specific file:

```
S Chassis(su)->dir  S-76101-0002
Filename:      S-76101-0002
Version:       07.61.01.0002
Size:          10845980 (bytes)
Date:          THU DEC 08 18:28:18 2011
CheckSum:      8101e4f14a13cc4d3a691fb8a5fac161
HAU Key:       a40dc8ca42102b7db12aeeae5f5d91a964a588a0 (HAU compatible)
```

```
Location:      slot2, slot3, slot4
Compatibility: Sx0000-0000, ST4106-0248, ST1206-0848, SG4101-0248, SG1201-0848,
               SK1008-0816, ST4106-0348-F6, ST1206-0848-F6, ST5206-0848-F6,
               SG1201-0848-F6, SG5201-0848-F6, SK1208-0808-F6, SK5208-0808-F6,
               SSA-T4068-0252, SSA-T1068-0652, SSA-T5068-0652, SSA-G1018-0652,
               SSA-G5018-0652
```

This example shows how to list information for all system images:

```
S Chassis(su)->dir images
Images:
================================================================================
Filename:      S-76101-0002
Version:       07.61.01.0002
Size:          10845980 (bytes)
Date:          THU DEC 08 18:28:18 2011
CheckSum:      8101e4f14a13cc4d3a691fb8a5fac161
HAU Key:       a40dc8ca42102b7db12aeeae5f5d91a964a588a0 (HAU compatible)
Location:      slot2, slot3, slot4
Compatibility: Sx0000-0000, ST4106-0248, ST1206-0848, SG4101-0248, SG1201-0848,
               SK1008-0816, ST4106-0348-F6, ST1206-0848-F6, ST5206-0848-F6,
               SG1201-0848-F6, SG5201-0848-F6, SK1208-0808-F6, SK5208-0808-F6,
               SSA-T4068-0252, SSA-T1068-0652, SSA-T5068-0652, SSA-G1018-0652,
               SSA-G5018-0652

Filename:      S-76101-0003 (Active) (Boot)
Version:       07.61.01.0003
Size:          10846108 (bytes)
Date:          TUE DEC 13 18:27:22 2011
CheckSum:      2c53ef3cb66010944fd93193f1a95a6f
HAU Key:       a40dc8ca42102b7db12aeeae5f5d91a964a588a0 (active image)
Location:      slot2, slot3, slot4
*Active:       slot2, slot3, slot4
Compatibility: Sx0000-0000, ST4106-0248, ST1206-0848, SG4101-0248, SG1201-0848,
               SK1008-0816, ST4106-0348-F6, ST1206-0848-F6, ST5206-0848-F6,
               SG1201-0848-F6, SG5201-0848-F6, SK1208-0808-F6, SK5208-0808-F6,
               SSA-T4068-0252, SSA-T1068-0652, SSA-T5068-0652, SSA-G1018-0652,
               SSA-G5018-0652
```

Table 17-1 provides an explanation of the command output.

Table 17-1 dir Output Details

Output...	What it displays...
Images	Lists all the images resident in the chassis and information about each.

Table 17-1 dir Output Details (continued)

Output...	What it displays...
Filename	Name of the image file stored in the local file system. Flags may be listed after the filename: • (Active) — Indicates this image is currently running. • (Boot) — Indicates this image is selected to boot on the next reset.
Version	Firmware version of the image.
Size	Size of image file in the local file system.
Date	Date of image file in the local file system.
CheckSum	MD5 checksum calculated across the entire image file, used for image identity and verification.
HAU Key	The High Availability key used to determine HAU compatibility between images. If the image is HAU compatible with the active image, The phrase “(HAU compatible)” is appended to the key information.
Location	Modules on which this image resides. The system automatically mirrors all images to all other compatible modules in the system. A user cannot selectively add or remove images from individual modules while they reside in the same chassis.
Compatibility	Module types on which this image is qualified to run. Attempting to run an incompatible image on a given module will not succeed.
Files	User maintained files, such as CLI configuration files. For details on working with configuration files, refer to **show config** (“show config” on page 17-18) and **configure** (“configure” on page 17-20.)
slotN	Lists user maintained files on a slot. If a USB device is connected to the USB port associated with the slot, the files on the USB device are also listed.
slotN/usbN	Lists user maintained files on a USB device connected to the USB port associated with a slot.

show boot system

Use this command to display the firmware image the system will load at the next system reset.

Syntax

```
show boot system
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

The system must be reset by software for the new boot image to take effect at startup. If the chassis is powered OFF and then back ON, the current active image will reload at startup.

The **dir** command, as described in "dir" on page 17-2, displays additional information about boot image files. "Active" indicates the image that is currently running, and "Boot" indicates the image that is currently scheduled to boot next. The **set boot system** command ("set boot system" on page 17-6) will move the boot designation from the current running image, but will allow the active image to stay where it is until after the reset, when that image has actually been booted.

Example

This example shows how to display the switch's boot firmware image:

```
S Chassis(rw)->show boot system
Current system image to boot: bootfile
```

set boot system

Use this command to set the firmware image the switch loads at startup or when performing a standard or high availability firmware upgrade (HAU).

Syntax

set boot system *filename* [standard | high-availability]

Parameters

filename	Specifies the name of the firmware image file.
standard	(Optional) Specifies that the next system reset will result in a standard (non-HAU) upgrade. The entire system will be reset and all modules will load the new image.
high-availability	(Optional) Specifies that the next system reset will attempt to initiate a High-Availability upgrade. If all HAU preconditions are not met, the upgrade will not be performed. See the usage section below for HAU precondition details.

Defaults

If no option is specified, the upgrade method for the new firmware image is determined by the default mode setting using "set boot high-availability default-mode" on page 17-14. The HAU default mode defaults to **never** which is the same as specifying the **standard** system boot method.

Mode

All command modes.

Usage

There are two methods for loading a system firmware image:

- Standard – The specified image is loaded after a system reset
- High Availability – Provides a rolling firmware upgrade

Setting a system boot method over-rides the HAU default mode set using "set boot high-availability default-mode" on page 17-14.

Using the standard method, the image is loaded automatically after the system has been reset. Although it is not necessary to choose to reset the system and activate the new boot image immediately, the CLI will prompt you whether or not you want to do so. You can choose "Yes" at the question prompt to have the system reset and load the new boot image immediately, or choose "No" to load the new boot image at a later scheduled time, by issuing one of the following commands: **clear config**, **reset**, or **configure**. The new boot setting will be remembered through resets and power downs, and will not take effect until the **clear config**, **reset**, or **configure** command is given.

The high availability upgrade method provides for loading new system firmware without resetting the entire system at once. HAU groups made up of one or more slots are upgraded one HAU group at a time rather than simultaneously. This process of staggering slot upgrades allows slots that do not belong to the HAU group that is currently being upgraded to continue normal operation, providing a high-degree of system availability during the upgrade process.

During a high availability upgrade each group slot will be temporarily unavailable while it is being upgraded, causing every physical port to experience an interruption during the upgrade process. These interruptions can be mitigated by a redundant network architecture, using Link Aggregation Groups (LAG) which span multiple slots. A properly configured LAG can continue to operate even when one or more of its component links are temporarily unavailable.

The following preconditions must be met for a high availability upgrade to occur:

- **HAU Compatibility Key** - The target image must have the same HAU Compatibility Key as the active image. To display the HAU key, use the **dir** command, specifying the image to display, or use the **image** option to display all images. The HAU key field in the display specifies whether the image displayed is compatible with the current image. If "HAU compatible" is appended to the key field, an HA firmware update can be performed between the displayed image and the current image.
- **Configuration restore-points** - Configuration restore-points may be set, but must not be configured. A configured restore-point would cause upgraded slots to boot with different configuration data, and all slots must be running the same configuration data.
- **Upgrade Groups** - At least two upgrade groups are required, and each group must contain at least one operational module at the start of HA Upgrade.
- **Platform** – S-Series S4, S6, and S8 platforms require the presence of at least 2 fabric modules in the system. See the following bullet for an exception to this rule.
- **Virtual Switch Bonding (VSB)** – HAU is not allowed if the reset of any single upgrade group would break all VSB interconnect bond links. An exception to this rule:
  - HAU is allowed in any bonded system including those that would would break either the two fabric module restriction or the all VSB interconnect links restrictions, if:
    - There is one and only one HAU group configured for each chassis
    - All slots in a chassis belong to the same HAU group

If any of these preconditions are not met when attempting a high availability upgrade, no upgrade takes place. Should you wish a standard upgrade to automatically take place when an HAU precondition is not met:

- Do not specify a system boot method when entering this command
- Set the HAU default mode to **if-possible** using the "set boot high-availability default-mode" on page 17-14.

Examples

This example shows how to set the boot firmware image file to “newimage” and reset the system with the new image loaded immediately using the standard method:

```
S Chassis(rw)->set boot system newimage standard
This command can optionally reset the system to boot the new image.
Do you want to reset now (y/n) [n]?y
Resetting system ...
```

This example shows how to set the boot firmware image file to “haimage” and to immediately start the HA Upgrade:

```
S Chassis(rw)->set boot system haimage high-availability
This command can optionally start a High-Availability Upgrade.
Do you want to do this now (y/n) [n]?y
Starting High-Availability Upgrade ...
```

This example shows how to set the boot firmware image file to “haimage” and set the high availability upgrade to pending. The **reset system** command starts the high availability upgrade:

```
S Chassis(rw)->set boot system haimage high-availability
This command can optionally start a High-Availability Upgrade.
Do you want to do this now (y/n) [n]?n

High-Availability Upgrade has been enabled and is now pending.
The next system reset will start the upgrade.
S Chassis(rw)->
S Chassis(rw)->reset system
A High-Availability Upgrade is pending.  If you proceed then the upgrade
will start now and modules will be reset sequentially.  Your CLI session
will be disconnected sometime during this upgrade.
Do you want to continue (y/n) [n]?y
Starting High-Availability Upgrade ...
```

show boot high-availability

Use this command to display HAU boot configuration and state settings.

Syntax

show boot high-availability

Parameters

None.

Defaults

None.

Mode

All command modes.

Examples

This example shows HAU configuration and state settings display when HAU is disabled:

```
S Chassis(rw)->show boot high-availability

There is currently no High Availability Upgrade running or pending.

Status:            disabled
Default Mode:      never
Inter Group Delay: 0
Previous Image:
Target Image:
Start Time:        Unknown
Finish Time:       Unknown
Duration:          Unknown

                          Slots
-----------------------+---------+
Groups                 | 1  2  3 |
-----------------------+---------+
  1                    | X  .  . |
  2                    | .  X  . |
  3                    | .  .  X |
-----------------------+---------+
Status                 | 1  2  3 |
-----------------------+---------+
 Currently Present     | X  X  X |
 Currently Operational | X  X  X |
-----------------------+---------+

S Chassis(rw)->
```

This example shows HAU configuration and state settings display when HAU is running:

```
show boot high-availability

There is currently a High Availability Upgrade in progress.

Status:            running
Default Mode:      never
Inter Group Delay: 0
Previous Image:    07.61.01.0004
Target Image:      07.61.01.0005
Start Time:        TUE DEC 27 20:32:23 2011
Finish Time:       Unknown
Duration:          89 seconds
```

```
                          Slots
----------------------+---------+
Groups                | 1  2  3 |
----------------------+---------+
  1                   | X  .  . |
  2                   | .  X  . |
  3                   | .  .  X |
----------------------+---------+
Status                | 1  2  3 |
----------------------+---------+
 Initially Present    | X  X  X |
 Currently Present    | X  X  X |
 Currently Operational| X  X  X |
 Upgrade Pending      | X  .  . |
 Upgrade In Progress  | .  X  . |
 Upgrade Complete     | .  .  X |
 Error Condition      | .  .  . |
----------------------+---------+
```

Table 17-1 provides an explanation of the command output.

Table 17-2 show boot high-availability Output Details

Output...	What it displays...
Status	The status of HAU for this device: • **Disabled** – HAU is not enabled. • **Pending** – HAU is enabled and will be initiated by the next system reset. • **Running** – HAU is in progress. • **Success** – HAU completed successfully and entity is running the target version of firmware. • **Error** – A failure occurred during upgrade. • **ForceComplete** – HAU was forced to complete early. The device is running the target version of firmware, but the high availability aspect of the upgrade may have been compromised.
Default Mode	The default mode of the HAU for the device (See "set boot high-availability default-mode" on page 17-14): **Never** – HAU is never performed; a standard upgrade is always performed. **IfPossible** – A high availability upgrade is performed whenever possible based upon the HAU pre-conditions listed in the usage section of "set boot system" on page 17-6. If all pre-conditions are not met a standard upgrade is performed. **Always** – Always attempt to perform a high availability upgrade. If a compatible image is not available, do not perform any upgrade. Specifying a system boot method using "set boot system" on page 17-6 overrides the default mode setting.

Table 17-2 show boot high-availability Output Details (continued)

Output...	What it displays...
Inter Group Delay	The duration, in seconds, that the HAU process will wait between the successful upgrade of a just completed HAU group and the upgrade start of the next HAU group. See "set boot high-availability delay" on page 17-13.
Previous Image	The release and version of the firmware the device is upgrading from.
Target Image	The release and version of the firmware the device is upgrading to.
Start Time	The date and time when the most recent HAU was started.
Finish Time	The date and time when the most recent HAU was completed.
Duration	The duration of the most recent HAU in centiseconds.
Status	Displays slot status. When HAU status is disabled or pending: • **Currently Present** – A module is present in any slot with an "X" present • **Currently Operational** – A module is operational in any slot with an "X" present. When HAU is running: • **Initially Present** - The module was present at the start of HAU. • **Upgrade Pending** - The module is still running the original image. • **Upgrade In Progress** - The module has been reset and should reboot to the target image. • **Upgrade Complete** - The module has rebooted to the target image. • **Error Condition** - The initially present module is no longer present, no longer operational, or did not boot to the target image.
Groups	Lists the default or configured HAU groups for the device. See "set boot high-availability group" on page 17-11 for HAU group configuration details.
Slots	The slot to which a group belongs or to which a status is indicated, represented by an "X".

set boot high-availability group

Use this command to configure an HAU group.

Syntax

set boot high-availability group *group-id slot(s)*

Parameters

group-id	Specifies an HAU group. Valid values are **1** — **128**.
slot(s)	Specifies one or more group member slots. Multiple slots are delineated by a comma (,) or a range by hyphen (-). Valid values are **1** — maximum number of supported device slots.

Defaults

HAU groups default to one group per slot.

Mode

All command modes.

Usage

The HAU group feature provides for the simultaneous upgrade of all modules within a group. This capability provides the benefit of minimizing total upgrade time for the system.

All essential system capabilities on the device should be configured across multiple groups. For example, all LAGs configured on the device should provide sufficient redundancy for packets to continue forwarding on the LAG using slots belonging to an HAU group that is not upgrading.

Example

This example shows how to configure HAU group 1 for slots 1 and 4:

```
S Chassis(rw)->set boot high-availability group 1 1,4
S Chassis(rw)->
```

clear boot high-availability group

Use this command to reset configured HAU groups to the default HAU group configuration.

Syntax

clear boot high-availability group

Parameters

None.

Defaults

By default, each occupied system slot belongs to a separate HAU group.

Mode

All command modes.

Usage

This command resets any HAU group configuration to the default value with each occupied system slot belonging to its own HAU group.

Example

This example shows how to reset HAU group configuration to the default of each occupied slot belonging to its own HAU group:

```
S Chassis(rw)->clear boot high-availability group
S Chassis(rw)->
```

set boot high-availability delay

Use this command to set a delay between the completion of one upgrade group and the beginning of another.

Syntax

set boot high-availability delay *delay*

Parameters

delay	Specifies a delay in seconds between the upgrade completion of one HAU group and the beginning of another. Valid values are **0** - **600** seconds. The default value is **0** seconds.

Defaults

0 seconds (no delay).

Mode

All command modes.

Usage

If it is determined that certain features, functions or protocols in a particular network have an adverse reaction to the multiple slot resets which are a necessary part of HA Upgrades, it is possible to slow the pace of the upgrade process. Inserting extra delay between resets may allow those protocols to reach a stable state before the next reset begins.

Under normal operation there is an approximately 5 second delay between the completion of one HAU group upgrade and the start of the next group upgrade. Use the HAU delay to assure that the just completed HAU group is fully operational before beginning the next HAU group upgrade.

Example

This example shows how to set the delay between the upgrade completion of one HAU group and the beginning of another to 15 seconds:

```
S Chassis(rw)->set boot high-availability delay 15
S Chassis(rw)->
```

clear boot high-availability delay

Use this command to reset the HAU delay to its default setting.

Syntax

clear boot high-availability delay

Parameters

None.

Defaults

0 seconds (no delay).

Mode

All command modes.

Usage

Using this command sets the HAU delay to 0 seconds. Setting HAU delay to 0 seconds could result in the next HAU group upgrade beginning before some system applications such as OSPF and IGMP multicast being fully operational on the just completed HAU group modules.

Example

This example shows how to reset the delay between the upgrade completion of one HAU group and the beginning of another to 0 seconds:

```
S Chassis(rw)->clear boot high-availability delay
S Chassis(rw)->
```

set boot high-availability default-mode

Use this command to configure an HAU default mode for the device.

Syntax

```
set boot high-availability default-mode {never | if-possible | always}
```

Parameters

never	Specifies that a standard non-HA firmware upgrade is always performed. The default HAU default-mode is **never**.
if-possible	Specifies that a high availability upgrade will only be performed if HAU preconditions such as HAU image compatibility are met. Otherwise, a non-HA standard firmware upgrade is performed. See the "set boot system" on page 17-6 usage section for HAU precondition details.
always	Specifies that a high availability upgrade will be performed if all HAU preconditions are met. Otherwise, no firmware upgrade is performed. See the "set boot system" on page 17-6 usage section for HAU precondition details.

Defaults

The HAU default mode defaults to **never**. The **standard** system boot mode is used.

Mode

All command modes.

Usage

This command sets the HA firmware upgrade default mode for the device. By default, the standard system boot upgrade method is used.

Note: Specifying a boot mode option (**standard** or **high-availability**), using the "set boot system" on page 17-6, overrides any HAU default mode setting. If the boot mode option is set to **standard**, HAU boot behavior is the same as the **never** default mode setting. If the boot mode option is set to **high-availability**, HAU boot behavior is the same as the **always** default mode setting.

When the **if-possible** default mode is set, a firmware upgrade will always be performed. If all HAU preconditions are met, a high availability upgrade is performed, otherwise a non-HA standard upgrade is performed. See the usage section of "set boot system" on page 17-6 for HAU precondition details.

When the **always** default mode is set, a firmware upgrade is only performed if all HAU preconditions are met. This setting assures that if a firmware upgrade can be performed, it will always be an HA upgrade. This setting prevents your system from being taken down by a standard system upgrade.

Example

This example shows how to set the HAU default mode to **always**:

```
S Chassis(rw)->set boot high-availability default-mode always
S Chassis(rw)->
```

clear boot high-availability default-mode

Use this command to reset the HAU default mode for the device to the default value.

Syntax

clear boot high-availability default-mode

Parameters

None.

Defaults

The HAU default mode defaults to **never**.

Mode

All command modes.

Example

This example shows how to reset the HAU default mode to the default value of **never**:

```
S Chassis(rw)->clear boot high-availability default-mode
S Chassis(rw)->
```

set boot high-availability force-complete

Use this command to force the firmware upgrade to simultaneously upgrade all remaining HAU groups.

Syntax

set boot high-availability force-complete

Parameters

None.

Defaults

None

Mode

All command modes.

Usage

Once HAU is started, it cannot be cancelled or aborted. However, it is possible to force a running HAU to complete immediately. This command causes the immediate and simultaneous upgrade of all slots which have yet to be upgraded. Although all slots in the system are upgraded to the target image, the force complete action compromises the high availability aspect of the upgrade and should only be used when there is good reason to complete the upgrade as quickly as possible.

Example

This example shows how to force all remaining non-upgraded HAU groups to simultaneously upgrade:

```
S Chassis(rw)->set boot high-availability force-complete

This command will force immediate completion of the in-progress
High-Availability Upgrade by simultaneously resetting all pending
and failed slots. This will compromise the high-availability
aspect of the upgrade.
Do you want to do this now (y/n) [n]?y
Forcing High-Availability Upgrade Completion ...
```

show file

Use this command to display the contents of a configuration file.

Syntax

show file *filename*

Parameters

filename	Specifies the file, in the root directory or a subdirectory (slot or USB device directory), to display.

Defaults

None.

Mode

All command modes.

Usage

If C2 security mode is enabled, encrypted passwords are cloaked while in Read-Write or Read-Only user mode.

Example

This example shows how to display the contents of a configuration file named sample.cfg:

```
S Chassis(rw)->show file slot1/sample.cfg
#BEGIN:  07.00.00.0061

begin
!
# ***** NON-DEFAULT CONFIGURATION *****
!
!
# Chassis Firmware Revision:  07.00.00.0061
!
!
#  SLOT   TYPE
#  ___    _________________
!
#   1     SSA-T4068-0252
!
!
# router configuration
!
# **** VRF default (default) ****
configure terminal
!
 interface vlan.0.4000
  ip address 192.168.100.20 255.255.255.0
  no shutdown
  exit
!
# Static routes configured on routed interfaces
 ip route 10.0.0.0/8 192.168.100.1 interface vlan.0.4000 1
 ip route 134.0.0.0/8 192.168.100.1 interface vlan.0.4000 1
!
# Static routes configured on non-routed interfaces
!
exit
!
# ip dns
!
# ip interface
set ip interface vlan.0.4000 default
!
# authentication
!
```

```
.
.
.!
# vlan
set vlan create 2-5,4000
clear vlan egress 1 ge.1.47
set vlan egress 2 ge.1.1-2 tagged
set vlan egress 3 ge.1.1-2 tagged
set vlan egress 4 ge.1.1-2 tagged
set vlan egress 5 ge.1.1-2 tagged
set vlan egress 4000 host.0.1 tagged
set vlan egress 4000 ge.1.47 untagged
!
# vlanauthorization
!
# webview
!
# width
!
end

#END: e2bf4471a3b8c59203b277f35859a68d
```

show config

Use this command to display the system configuration or write the current configuration to a file.

Syntax

show config [**all**] [*facility*] [**outfile** *outfile*]

Parameters

all	(Optional) Displays default and non-default configuration settings.
facility	(Optional) Displays the configuration for a specific facility.
outfile *outfile*	(Optional) Specifies a file in which to store the configuration. You can store this file in the root directory or a subdirectory (slot or USB device directory).

Defaults

If no parameters are specified, only non-default system configuration settings will be displayed.

Mode

All command modes.

Usage

If C2 security mode is enabled, encrypted passwords are cloaked while in Read-Write or Read-Only user mode.

Example

This example shows how to display the current non-default device configuration and write the output to file **config08222010.txt** on slot **1**:

```
S Chassis(su)->show config outfile slot1/config08222010.txt
This command shows non-default configurations only.
Use 'show config all' to show both default and non-default configurations.


begin
!
# ***** NON-DEFAULT CONFIGURATION *****
!
!
# Chassis Firmware Revision: 07.00.00.0061T
!
# router configuration
!
# **** VRF default (default) ****
configure terminal
!
 interface loop.0.1
  ip address 172.16.3.1 255.255.255.252
  no shutdown
  exit
 interface loop.0.2
  ip address 172.16.3.5 255.255.255.252
  no shutdown
  exit
.
.
.
# vlan
set vlan create 13,23,1010,1020,1030,1040,4024
clear vlan egress 1 lag.0.1;ge.1.1-24
set vlan egress 1 ge.1.1 tagged
set vlan egress 13 lag.0.1;ge.1.21 untagged
set vlan egress 23 ge.1.22 tagged
set vlan egress 1010 ge.1.1 untagged
set vlan egress 1020 ge.1.2 untagged
set vlan egress 1030 ge.1.3 untagged
set vlan egress 1040 ge.1.4 tagged
```

```
set vlan egress 4024 ge.1.24 untagged
!
# vlanauthorization
!
# webview
!
# width
set width 160 default
!
end
```

configure

Use this command to execute a previously downloaded configuration file stored on the device.

Syntax

configure *filename* [**append**] [**chassis-id** *chassis-id*]

Parameters

filename	Specifies the path and file name of the configuration file to execute.
append	(Optional) Executes the configuration as an appendage to the current configuration. This is equivalent to typing the contents of the config file directly into the CLI and can be used, for example, to make incremental adjustments to the current configuration.
chassis-id	(Optional) Specifies the replacement chassis ID in the VSB system the configuration file is being applied to. The original chassis ID was set using "set bonding chassis" on page 18-4.

Defaults

If **append** is not specified, the current running configuration will be replaced with the contents of the configuration file, which will result in an automatic reset of the chassis.

If **chassis-id** is not specified for a VSB system, see the usage section below for a discussion of chassis ID precedence rules.

Mode

All command modes.

Usage

If C2 security mode is enabled, a non-append version of the **configure** command can not be accessed while in Read-Write or Read-Only user mode.

The **configure** command is not allowed if an HA upgrade is pending.

A VSB configuration file contains chassis specific information such as the chassis serial-number. When configuring a replacement VSB chassis with an already existing VSB configuration file, you must specify the chassis ID of the replacement chassis so that chassis specific information on the specified chassis will be ignored and replaced in the configuration file with the correct chassis settings. Use the **chassis-id** option to specify a replacement VSB system chassis.

There are four rules of chassis ID precedence that determine the chassis ID selection when applying a configuration file to a VSB system (from high precedence to low precedence):

1. If bonding is already enabled, and the chassis is active, the active chassis ID is used
2. The chassis ID specified using the **configure** command **chassis-id** option is used
3. The chassis ID specified in the configuration file that contains a serial-number matching the device serial number is used
4. The lowest chassis ID specified in the configuration file is used

Examples

This example shows how to execute the “myconfig” file on the USB device connected to the USB port associated with the module in slot 1:

```
S Chassis(rw)->configure slot1/usb2/myconfig
```

This example shows how to execute the “myconfig” file on the USB device connected to the USB port associated with a replacement chassis 2 in a VSB system:

```
S Chassis(rw)->configure slot1/usb1/myconfig chassis-id 2
```

copy

Use this command to upload or download an image or a CLI configuration file.

Syntax

copy *source destination*

Parameters

source	Specifies location and name of the source file to copy. Options are a local file path (valid directories are the images/ directory, the slotN/ directory, and the slotN/usbN directory), or the URL of an FTP, TFTP, or SCP server.
destination	Specifies location and name of the destination where the file will be copied. Options are a slot location and file name, or the URL of an FTP, TFTP, or SCP server.

Defaults

None.

Mode

All command modes.

Usage

The S-Series module to which a configuration file is downloaded must have the same hardware configuration as the S-Series module from which it was uploaded.

The **copy** command supports URLs:

- FTP – File Transfer Protocol
- TFTP – Trivial File Transfer Protocol
- SCP – SecureCopy File transfers tunneled through SSH

For reasons of security, passwords are not allowed in **copy** command URLs. A password prompt displays upon entering a **copy** command. For example:

```
S Chassis(rw)->copy slot3/docconfig1 scp://doc@10.21.1.180/docconfig1
Password:
###########
S Chassis(rw)->
```

Examples

This example shows how to download an image via TFTP:

```
S Chassis(rw)->copy tftp://134.141.89.34/ets-mtxe7-msi newimage
```

This example shows how to download an image via Anonymous FTP:

```
S Chassis(rw)->copy ftp://134.141.89.34/ets-mtxe7-msi newimage
```

This example shows how to download an image via FTP with user credentials:

```
S Chassis(rw)->copy ftp://user:passwd@134.141.89.34/ets-mtxe7-msi newimage
```

This example shows how to download a configuration file via TFTP to the slot 3 directory:

```
S Chassis(rw)->copy tftp://134.141.89.34/myconfig slot3/myconfig
```

This example shows how to download a configuration file via SCP

```
S Chassis(rw)->copy scp://doc@banshee.extremenetworks.com:22/docconfig1
slot3/docconfig1
```

This example shows how to upload a configuration file via Anonymous FTP from the module in slot 3:

```
S Chassis(rw)->copy slot3/myconfig ftp://134.141.89.34/myconfig
```

This example shows how to upload a file using SCP from the module in slot 3 to the server:

```
S Chassis(rw)->copy slot3/myconfig scp//doc@10.21.1.180:/myconfig
```

This example shows how to copy a configuration file from the slot 3 directory to the slot 5 directory:

```
S Chassis(rw)->copy slot3/myconfig slot5/myconfig
```

delete

Use this command to remove an image or a CLI configuration file from the S-Series system.

Syntax

delete *filename*

Parameters

filename	Specifies the local path name to the file. Valid directories are the images/ directory, the slotN/ directory, and the slotN/usbN directory.

Defaults

None.

Mode

All command modes.

Usage

Use the **show config** command as described in "show config" (page 17-18) to display current image and configuration file names.

Examples

This example shows how to delete the "myconfig" configuration file from slot 3:

```
S Chassis(rw)->delete slot3/myconfig
```

This example shows how to delete the "010300" image file:

```
S Chassis(rw)->delete images/010300
```

This example shows how to delete the "myconfig" configuration file from the USB device connected to the USB port associated with slot 1:

```
S Chassis(rw)->delete slot1/usb2/myconfig
```

script

Use this command to execute a script file.

Syntax

script *filename* [*arg1*] [*arg2*] [*arg3*] [*arg4*] [*arg5*] [*arg6*] [*arg7*]

Parameters

filename	Specifies the local path name to the file. Valid directories are the images/ directory, the slotN/ directory, and the slotN/usbN directory.
arg1 through *arg7*	Specifies up to seven arguments to the script.

Defaults

None.

Mode

All command modes.

Usage

The script file must first be created on a PC and copied to the S-Series device using the **copy** command ("copy" on page 17-21) before the script can be executed. The file can contain any number of switch commands, up to a maximum file size of 128 kilobytes. Router commands cannot be included in the file. Scripts cannot be nested within the file. Note that the **history** command will not reflect the execution of commands within a script file.

If C2 security mode is enabled, access to secure logs using the **script** command is not supported while in Read-Write or Read-Only user modes.

Example

This example uses the **copy** command to copy the script file named "setport.scr" from IP address 10.1.221.3 to slot 4. Next, the contents of the file is displayed with the **show file** command. The

script file requires two arguments, a port string (%1) and a VLAN id (%2). Finally, the script is executed, by specifying ge.1.1 as the first argument and 100 as the second argument.

```
S Chassis(rw)->copy tftp://10.1.221.3/setport.scr slot4/setport.scr


S Chassis(rw)->show file slot4/setport.scr
set port alias %1 script_set_port
set port vlan %1 %2 modify-egress
set port jumbo enable %1
set port disable %1
set port lacp port %1 disable


S Chassis(rw)->script slot4/setport.scr ge.1.1 100
```

When the **script** command parses the file and performs the command line argument substitution, the commands are converted to the following:

```
set port alias ge.1.1 script_set_port
set port vlan ge.1.1 100 modify-egress
set port jumbo enable ge.1.1
set port disable ge.1.1
set port lacp port ge.1.1 disabled
```

The converted strings are then executed by the CLI engine and the **script** command returns.

Restore Point Commands

This section provides detailed information about the restore point set of commands. Configuration of restore point functionality includes the display and setting restore points, which allows the configuration to be restored, up to the restore point, if necessary. For information about configuring restore points, refer to the “Image Configuration and File Management” chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
set config restore-point	17-24
show config restore-point	17-25
clear config restore-point	17-26
configure restore-point	17-26

set config restore-point

Use this command to create a restore point of the current configuration.

Syntax

set config restore-point *description*

Parameters

description	A description of the configuration restore point.

Defaults

None.

Mode

All command modes.

Usage

If the *description* contains spaces, enclose the description in double quotes (“”).

Any additional configuration settings that you change after creating a restore point will not be included when the restore point configuration is applied, such as when the system reboots. Currently, you can configure only one restore point.

Example

```
S Chassis(rw)-> set config restore-point 25June2009_0800
```

show config restore-point

Use this command to display the index, creation date, and description of the currently configured restore point.

Syntax

show config restore-point

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

If “(Boot)” is listed after the index entry, this restore point will be used when the system reboots next.

Example

```
S Chassis(rw)->show config restore-point

 Index:          1245935343 (Boot)
 Creation Date:  THU JUN 25 13:09:03 2009
 Description:    test
```

If no restore point is configured, the CLI displays the following message:

```
S Chassis(rw)->show config restore-point

 No restore-point configured.
```

clear config restore-point

Use this command to delete the current restore point.

Syntax

clear config restore-point *index*

Parameters

index	The index number of the restore point. Use the **show config restore-point** command to view the index number.

Defaults

None.

Mode

All command modes.

Usage

Because the system currently supports only one restore point, you must delete the current restore point before creating a new one.

Example

```
S Chassis(rw)-> clear config restore-point 1245935343
```

configure restore-point

Use this command to indicate whether the restore point will be applied when the system reboots.

Syntax

configure restore-point *index* [**none**]

Parameters

index	The index number of the restore point. Use the **show config restore-point** command to view the index number.
none	(Optional) Indicates that the restore point will not be applied when the system reboots.

Defaults

None.

Mode

All command modes.

Usage

If the restore point is applied when the system reboots, any configuration changes made after the restore point was set will be lost.

This command is not allowed if an HA upgrade is pending.

Example

This examples shows how to not apply restore point **1245935343** when the system reboots:

```
S Chassis(rw)-> configure restore-point 1245935343 none
```

18

Virtual Switch Bonding Commands

This chapter provides detailed information for the Virtual Switch Bonding (VSB) set of commands. For information about configuring VSB, refer to the "Virtual Switch Bonding (VSB) Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show bonding	18-1
set bonding chassis	18-4
clear bonding chassis	18-5
set bonding enable	18-5
set bonding disable	18-6
set bonding lfr	18-7
clear bonding lfr	18-8
set bonding port enable	18-8
set bonding port disable	18-9
set bonding mac	18-10
clear bonding mac	18-11
set bonding mode	18-11
clear bonding mode	18-12
show lacp outportLocalPreference	18-13
set lacp outportLocalPreference	18-13
clear lacp outportLocalPreference	18-14
set license vsb	18-15

show bonding

Use this command to display VSB information for this device.

Syntax

```
show bonding
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example displays VSB information for an S4 chassis VSB configuration using hardware bonding ports:

```
S Chassis(rw)->show bonding
Global Bonding State    : enabled
Bonding Mode            : hardware
Max Bonded Chassis      : 2
Max Bonded System Slot  : 8
Slots active in System  : 1-6,8
Bonding Admin System MAC: 00-00-90-00-00-90
Bonding Oper System MAC : 00-00-90-00-00-90
Link Failure Response   : enabled

Chassis: 1
        System Identifier: 999
            Serial Number: 13035251635Y
                   Status: up
  Slots active in Chassis: 1-4
            Shared Secret: yes
             LFR priority: 90

Chassis: 2
        System Identifier: 999
            Serial Number: 13085590635Y
                   Status: up
  Slots active in Chassis: 5-6,8
            Shared Secret: yes
             LFR priority: 100

Port          Admin    Partner       Oper     Oper
              Status   Port          Mode     Status
------------- -------- ------------- -------- ----------------
vsb.2.1       enabled  vsb.8.4       bonding  up
vsb.2.2       enabled  vsb.6.1       bonding  up
vsb.2.3       enabled  vsb.6.3       bonding  up
vsb.2.4       enabled  vsb.8.2       bonding  up
vsb.3.1       enabled  vsb.8.1       bonding  up
vsb.3.2       enabled  vsb.8.3       bonding  up
```

```
vsb.6.1       enabled  vsb.2.2       bonding  up
vsb.6.3       enabled  vsb.2.3       bonding  up
vsb.8.1       enabled  vsb.3.1       bonding  up
vsb.8.2       enabled  vsb.2.4       bonding  up
vsb.8.3       enabled  vsb.3.2       bonding  up
vsb.8.4       enabled  vsb.2.1       bonding  up
S Chassis(rw)->
```

Table 18-1 provides an explanation of the command output.

Table 18-1 show bonding Output Details

Output...	What it displays...
Global Bonding State	Specifies whether VSB is globally enabled or disabled for the device.
Max Bonded Chassis	Specifies the non-configurable maximum number of supported physical chassis that can be bonded into a single VSB system. Current maximum bonded chassis value is 2.
Max Bonded System Slot	Specifies the maximum number of slots supported in the VSB system.
System Slot List	Specifies all active and enabled slots in the system.
Bonding Admin System MAC	Specifies the administratively configured system MAC address for use with VSB.
Bonding Oper System MAC	Specifies the operational system MAC currently used by VSB system.
Link Failure Response	Specifies whether the Link Failure Response (LFR) protocol is enabled or disabled for the system. See “set bonding lfr” on page 18-7.
Chassis	Specifies the Chassis ID for each physical chassis in the VSB. “set bonding chassis” on page 18-4.
System Identifier	Specifies the System ID assigned to the physical chassis. “set bonding chassis” on page 18-4.
Serial Number	Specifies the serial number of the physical chassis.
Status	Specifies the status of the chassis in the VSB system: • **Up** = Chassis is active in VSB system • **Down** = Chassis is not present in a VSB system • **Incomplete** = Chassis is not bonded to all VSB members • **Inactive** = Indicates the chassis is present but not active in the VSB system
Slots active in Chassis	Specifies the active and enabled slots in the chassis.
Shared Secret	Specifies whether a shared secret has been configured for the chassis. See “set bonding chassis” on page 18-4.
LFR priority	Specifies the LFR priority configured for this device. Defaults to 10 times the VSB chassis ID. See “set bonding chassis” on page 18-4.
Port	Specifies a Port ID belonging to the VSB. See “set bonding enable” on page 18-5.
Admin Status	Specifies the configured VSB state for the port (enabled/disabled).
Partner Port	Specifies the VSB interconnect port that this port is connected to.
Oper Mode	Specifies the VSB operational state for this VSB interconnect port.

Table 18-1 show bonding Output Details (continued)

Output...	What it displays...
Oper Status	Specifies the current operational state for a VSB port. • **up** = Port is up and operational for VSB • **down** = port is operationally down

set bonding chassis

Use this command to set VSB configuration on the physical chassis.

Syntax

set bonding chassis *chassis-id* {**system-id** *system-id* | **secret** *secret* | **lfr-priority** *priority*}

Parameters

chassis-id	Sets the physical chassis ID. Valid values are **1** — **2**.
system-id *system-id*	Sets the system ID for the VSB. Valid values are **1** - **18446744073709551615**.
secret *secret*	Configures a shared encrypted secret between VSB chassis for extra security. Valid values are up to 32 printable characters. If a space is used, secret must be enclosed in double quotes (“).
lfr-priority *priority*	Sets an LFR priority for this chassis. Valid values are 1 - 255. The default value is 10 times the VSB chassis-ID.

Defaults

The **lfr-priority** *priority* defaults to 10 times the chassis ID. All other parameters default to none.

Mode

All command modes.

Usage

Each VSB chassis has its own ID (**1** or **2**) and belongs to a VSB system. A VSB system forms a virtual chassis made up of two VSB chassis.

Note: It is possible to configure the same system ID for multiple VSB systems, but for management purposes it is highly recommended that each VSB system be configured with a unique ID.

Chassis belonging to a VSB system must be of the same platform and model.

LFR priority is used to determine which chassis is taken out of operation should all VSB interconnect links go down. Setting the LFR priority to the same value for both chassis in the VSB system is not allowed.

A shared secret may be configured before or after VSB is enabled. The secret may be changed at anytime without clearing the secret first.

Example

This example configures the chassis with VSB chassis ID **2** for VSB system **1**:

```
S Chassis(rw)->set bonding chassis 2 system-id 1
```

clear bonding chassis

Use this command to clear the VSB chassis ID and VSB system ID if the chassis has not yet been VSB enabled globally.

Syntax

clear bonding chassis *chassis-id* [**secret**] [**lfr-priority**]

Parameters

chassis-id	Specifies the chassis ID of the chassis to clear from the VSB system. Valid values are **1**-**2**.
secret	(Optional) Clears any shared secret configuration.
lfr-priority	(Optional) Resets the LFR priority to the default of 10 times the VSB chassis ID.

Defaults

- If only the *chassis-id* is specified, all VSB chassis configuration is cleared for this physical chassis.
- If the **secret** option is specified, any configured secret is cleared.
- If the **lfr-priority** option is specified, the LFR priority is reset to the default value of 10 times the chassis ID.

Mode

All command modes.

Example

This example clears the chassis ID and associated system ID for chassis 2:

```
S Chassis(rw)->clear bonding chassis 2
```

set bonding enable

Use this command to globally enable VSB.

Syntax

set bonding enable

Parameters

None.

Defaults

Bonding is globally disabled.

Mode

All command modes.

Usage

Before globally enabling VSB on your VSB configured chassis you must:

- Configure chassis IDs and the VSB system ID using “set bonding chassis” on page 18-4
- Enable at least one interconnect link between the two VSB chassis using “set bonding port enable” on page 18-8
- Assure that any required licenses are activated using “set license vsb” on page 18-15
- Optionally, assign a new MAC address using “set bonding mac” on page 18-10, if a non-default MAC address will be used

VSB is globally disabled by default.

A solid blue system CPU LED signifies a bonded enabled system.

Example

This example shows how to configure VSB on a chassis by: configuring chassis **1** for VSB system **1**, enabling VSB on ports **1** and **2**, and globally enabling VSB on the chassis.

```
S Chassis(rw)->set bonding chassis 1 system-id 1
S Chassis(rw)->set bonding port tg.1.1-2 enable
S Chassis(rw)->set bonding enable
S Chassis(rw)->
```

set bonding disable

Use this command to globally disable VSB.

Syntax

```
set bonding disable
```

Parameters

Bonding is globally disabled.

Defaults

None.

Mode

All command modes.

Usage

Note: Globally disabling VSB resets the chassis and clears the configuration on both physical chassis when the VSB system is in a bonded state.

VSB chassis and system ID configuration persists after globally disabling VSB. Use "clear bonding chassis" on page 18-5 to clear VSB chassis and system ID configuration when VSB is not globally enabled.

Example

This example shows how to globally disable VSB on this chassis.

```
S Chassis(rw)->set bonding disable
S Chassis(rw)->
```

set bonding lfr

Use this command to enable Link Failure Response (LFR) on the physical chassis.

Syntax

set bonding lfr {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables LFR on the physical chassis. Default value is **disable**.

Defaults

LFR is globally Disabled.

Mode

All command modes.

Usage

This command provides for enabling and disabling the LFR protocol on the physical chassis.

The LFR protocol determines which chassis will be brought down should all VSB interconnect links between the VSB chassis go down, and it is determined that both VSB chassis are operational.

The LFR protocol allows:

- 1GbE ports, when using software bonded ports
- 1 and 10GbE ports, when using hardware bonded ports

to be designated as VSB monitor links that operate in a standby mode to the primary VSB bond ports. The VSB monitor link provides dedicated redundant control plane connectivity and is used only as a backup communication path between two bonded chassis in the unlikely event that all of the primary VSB links fail or become unavailable. When the primary VSB ports are down, the VSB monitor links facilitate a communications path to allow the physical chassis with highest LFR priority in the bonded pair to remain active while placing the chassis with the lower priority into a dormant state.

The LFR protocol must be enabled on each VSB chassis in the VSB system for LFR monitoring to occur.

Example

This example enables the LFR protocol on the VSB chassis:

```
S Chassis(rw)->set bonding lfr enable
```

clear bonding lfr

Use this command to reset the Link Failure Response (LFR) configuration to disabled on the physical chassis.

Syntax

clear bonding lfr

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example resets the LFR protocol state to disabled on the VSB chassis:

```
S Chassis(rw)->clear bonding lfr
```

set bonding port enable

Use this command to enable a VSB interconnect or LFR monitor port.

Syntax

set bonding port *port-string* **enable**

Parameters

port-string	Enable VSB for the specified port.

Defaults

Bonding is disabled on ports.

Mode

All command modes.

Usage

Use this command to enable VSB ports for VSB chassis interconnection or Link Failure Response (LFR) monitoring.

VSB interconnect ports are the GbE ports interconnecting the VSB chassis that make up the VSB system. The chassis must be configured for VSB using “set bonding chassis” on page 18-4 before enabling VSB interconnect ports.

VSB LFR ports are GbE ports used to monitor a partner VSB chassis. In the case of a failure of all VSB interconnectivity, if LFR monitoring determines that both VSB chassis are operational, the VSB chassis with the highest LFR priority is allowed to remain operational. The chassis with the lower LFR priority is placed in a dormant mode.

VSB interconnect and LFR monitor ports can be provisioned before VSB is enabled.

VSB supports enabling up to a combined total of 32 VSB connectivity and LFR monitor links (32 ports per chassis).

Note: Interconnect link support depends upon whether the platform has dedicated VSB hardware ports present. If present, only VSB hardware ports are supported for VSB interconnect links. If not present, 10GbE ports enabled for VSB are supported for VSB interconnect links. 1GbE software ports enabled for VSB are LFR ports..

When first configuring VSB (chassis has not yet been globally enabled), ports are specified as they would be for a non-VSB system: **tg.***x***.***y* (where *x* specifies the slot of the non-VSB system and *y* specifies the port).

In a VSB globally enabled system:

- Chassis 1 slots are numbered the same as in a non-VSB system
- Chassis 2 begins slot numbering at the maximum number of supported chassis 1 slots plus 1.

  For example, in a VSB enabled system with two S3 chassis, chassis 1 slots are numbered **1** - **3** and chassis 2 slots are numbered **4** - **6**.

When modifying interconnect ports in a globally enabled VSB system, use the globally enabled port designation to specify ports.

Example

This example shows how to configure VSB on a chassis by: configuring chassis **1** for VSB system **1**, and enabling VSB interconnection on 10GbE slot **1** ports **1** and **2** and enabling VSB LFR on 1GbE slot **1** ports **5** and **6**.

```
S Chassis(rw)->set bonding chassis 1 system-id 1
S Chassis(rw)->set bonding port tg.1.1-2 enable
S Chassis(rw)->set bonding port ge.1.5-6 enable
S Chassis(rw)->
```

set bonding port disable

Use this command to disable a VSB interconnect or LFR monitor port.

Syntax

set bonding port *port-string* **disable**

Parameters

port-string	Disable VSB on the specified port.

Defaults

Bonding is disabled on ports.

Mode

All command modes.

Usage

When disabling a VSB interconnect or LFR monitor port, with no intention of reenabling it for VSB, be sure to disable both sides of the interconnect link.

Example

This example shows how to disable VSB interconnection on port **tg.1.1**. and LFR on port **ge.1.5**

```
S Chassis(rw)->set bonding port tg.1.1 disable
S Chassis(rw)->set bonding port ge.1.5 disable
S Chassis(rw)->
```

set bonding mac

Use this command to set the VSB system MAC address.

Syntax

set bonding mac *mac-address*

Parameters

mac *mac-address*	Specifies the MAC address for the VSB system. The supported MAC address formats are: • HH-HH-HH-HH-HH-HH • HH:HH:HH:HH:HH:HH • HHHH.HHHH.HHHH

Defaults

VSB MAC address defaults to an internal MAC address associated with VSB chassis **1**.

Mode

All command modes.

Usage

By default, VSB sets the VSB system MAC address to an internal MAC address associated with VSB chassis 1. Use this command to manually set a MAC address for the VSB system. Set the MAC address to the same value on both chassis before globally enabling VSB. Locally administered MAC addresses create the possibility for duplicate MAC addresses on the network. Be sure that the MAC address assigned using this command does not duplicate an already existing MAC address on the network.

Note: The VSB system MAC address can not be changed while VSB is globally enabled on the system. You must disable VSB using “set bonding disable” on page 18-6 before attempting to manually change the VSB system MAC address.

Example

This example manually sets the MAC address for the VSB system to a2f4:1234:dbc3:

```
S Chassis(rw)->set bonding mac a2f4.1234.dbc3
```

clear bonding mac

Use this command to reset the VSB system MAC address to its default value.

Syntax

clear bonding mac

Parameters

None.

Defaults

VSB MAC address defaults to an internal MAC address associated with VSB chassis **1**.

Mode

All command modes.

Usage

This command resets a manually configured MAC address to the default MAC address for the VSB system. By default, VSB sets the VSB system MAC address to an internal MAC address associated with VSB chassis 1.

Note: Once a VSB system has been globally enabled using the **set bonding enable** command, the VSB system MAC address can not be modified. The **clear bonding mac** command can only be used prior to globally enabling VSB on the system.

Example

This example clears the manually configured MAC address for the pre-globally enabled VSB system:

```
S Chassis(rw)->clear bonding mac
```

set bonding mode

Use this command to set the VSB interconnect port bonding mode.

Syntax

set bonding mode {**hard** | **soft**}

Parameters

hard	Specifies that the interconnect port used is an S180 dedicated hardware VSB fabric extended interconnect port.
soft	Specifies that the interconnect port used is a standard software assisted Ethernet data port. (Default)

Defaults

The default bonding mode is **soft**.

Mode

All command modes.

Usage

Newer version modules have either built in or the ability to install an option module that contains dedicated hardware VSB interconnect ports. Ports used for VSB interconnection for S-Series modules that do not have this capability are standard software assisted Ethernet data ports. The bonding mode specifies whether the interconnect port used for the VSB configuration is hardware or software.

The VSB system must operating in the V2 compatibility mode to use the S180 dedicated hardware VSB interconnect ports. Refer to "set chassis compatibility-mode" on page 7-3 for compatibility mode command details.

Use the **hard** keyword when interconnecting VSB chassis using dedicated hardware interconnect ports. Use the **soft** keyword when interconnecting VSB chassis using standard Ethernet data ports.

Example

This example sets the VSB bonding mode to hard for an S180 using the dedicated VSB hardware interconnect port for interconnection between VSB bonded chassis:

```
S Chassis(rw)->set bonding mode hard
```

clear bonding mode

Use this command to reset the VSB bonding mode to the default value.

Syntax

clear bonding mode

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example resets the VSB bonding mode to the default value of **soft**:

```
S Chassis(rw)->clear bonding mode
```

show lacp outportLocalPreference

Use this command to display the current LACP outport local preference status.

Syntax

```
show lacp outportLocalPreference
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

This command displays the current setting for LACP outport local preference, which determines the likelihood of a packet that ingresses the local chassis egressing the VSB system using a local chassis LAG port. See “set lacp outportLocalPreference” on page 18-13 for setting details.

Example

This example shows how to display the current LACP output local preference for the chassis:

```
S Chassis(rw)->show lacp outportLocalPreference
Outport local chassis preference set to strong
```

set lacp outportLocalPreference

Use this command to set the LACP outport local preference for the VSB system.

Syntax

```
set lacp outportLocalPreference {none | weak | strong | all-local}
```

Parameters

none	Specifies that no preference for outport local preference is configured for this chassis. **none** is the default setting.
weak	Specifies that some preference will be given to the likelihood that a packet will egress the VSB system using a LAG port on the local chassis. The resulting preference will be greater than none and less than strong.
strong	Specifies that a strong preference will be given to the likelihood that a packet will egress the VSB system using a LAG port on the local chassis. The resulting preference will be greater than weak and less than all-local.
all-local	Specifies that all packets will be forced to use local chassis LAG ports if resources are available.

Defaults

LACP outport local preference defaults to **none**.

Mode

All command modes.

Usage

The LACP outport local preference setting determines the likelihood of a packet that ingresses the local chassis egressing the VSB system using a local chassis LAG port. There are four outport local preference levels. If set to **none**, the outport local preference feature has no impact on packet egress for the VSB system. The **weak**, **strong**, and **all-local** outport local preference settings provide an increasing likelihood that the packet will egress the VSB system using a LAG port on the local chassis if resources are available. The degree of likelihood is from a somewhat greater likelihood in the case of **weak**, to an attempt to force all packets to use a local chassis LAG port in the case of **all-local**.

Outport local preference may be configured or cleared at any time. If you configure this feature prior to globally enabling VSB, configure both chassis with the same value. Setting or changing the parameter in a globally enabled system affects both chassis.

Outport local preference defaults to **none**.

Note: Local chassis outport LAG preference is a VSB-only feature. The outport LAG preference setting is only in affect when VSB is globally enabled on the system.

Example

This example shows how to set the LACP outport local preference to strong for this VSB system:

```
S Chassis(rw)->set lacp outportLocalPreference strong
```

clear lacp outportLocalPreference

Use this command to reset LACP outport local preference to the default value.

Syntax

clear lacp outportLocalPreference

Parameters

LACP outport local preference defaults to **none**.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the LACP outport local preference to the default value of **none**:

```
S Chassis(rw)->clear lacp outportLocalPreference
```

set license vsb

Use this command to activate a VSB license on each bonded chassis.

Syntax

set license vsb *license-key* {**slot** *slot* | **chassis** *chassis*}

Parameters

license-key	Specifies a unique VSB license key, in ASCII, and enclosed in double quotes (“”).
slot *slot*	Specifies the chassis slot the license is applied to.
chassis *chassis*	Specifies the chassis the license is applied to.

Defaults

If no option is specified, the license is applied to the chassis.

Mode

All command modes.

Usage

VSB is supported by default on the S155 module. A license is required when globally enabling VSB on chassis containing S130 and S150 modules. When a VSB enabled S155 module is hot swapped with an S130 or S150 module or a license expires, VSB is not disabled on the new or license expired module. An error message will display every five minutes until a valid license is configured on the module.

The displayed error message will be similar to:

```
System[2]Virtual Switch Bonding (VSB) is enabled on chassis-2 without a valid
license. This message will continue until the license is configured or VSB is
disabled.
System[1]Virtual Switch Bonding (VSB) is enabled on chassis-1 without a valid
license. This message will continue until the license is configured or VSB is
disabled.
```

A feature entitlement verification check occurs when attempting to enable VSB globally. If modules other than S155s are installed in the system, you must activate a VSB license on each chassis in the system before attempting to globally enable VSB.

Entering a **clear config all** or a **set bonding disable** command does not remove a VSB license. Use the **clear license vsb** command to clear a VSB license.

Example

This example sets the VSB license for both chassis 1 and chassis 2, enables VSB globally, and displays the vsb license information for the system:

Chassis 2

```
S Chassis(rw)->set license vsb "YYYYYYYYYYYYYYYYYYYYYYYYYYYYYY" chassis 2
```

Chassis 1

```
S Chassis(rw)->set license vsb "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX" chassis 1
S Chassis(rw)->set bonding enable
```

```
S Chassis(rw)->show license
License Type      Location    Status      Key
----------------  ----------  ----------  ------------------------------------------------
vsb               chassis 1   active      XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
vsb               chassis 2   active      YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY
S Chassis(rw)->
```

19

Network Diagnostics

This chapter provides detailed information for the network diagnostics set of commands. Network diagnostics functionality includes ping, traceroute, and name server lookup. For information about configuring network diagnostics, refer to the "Network Monitoring Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
ping	19-1
traceroute	19-3
nslookup	19-5

ping

Use this command to determine the availability of another node on the network by sending the node an ICMP echo-request packet and receiving an ICMP echo-reply back.

Syntax

```
ping  [-s bytes] [-c count] [-n] [-p pattern] [-t milliseconds] [-I interface]
[-S ip-address] [-Q service-type] [-r] [-i milliseconds] [-v {4 | 6}] [-V router]
host
```

Parameters

-s *bytes*	(Optional) Specifies the number of data bytes to be sent. The default value is **56**, which translates into 64 ICMP/ICMP6 data bytes when combined with the 8 bytes of ICMP/ICMP6 header data. The maximum data size for IPv4 is **65507** bytes. The maximum data size for IPv6 is **65487** bytes.
-c *count*	(Optional) Number of ping packets. The default value is **4**.
-n	(Optional) Avoids any communications with nameservers. An IP address has to be supplied as a hostname if this option is used.
-p *pattern*	(Optional) Specify up to a 16 bit hexadecimal pattern to fill outgoing packet with (ex. -p ff).
-t *hops*	(Optional) Specifies the maximum number of hops for the ping. Time To Live (TTL) for IPv4; Hop Limit (HL) for IPv6. The default value for both Time TTL and HL is **64**.
-I *interface*	(Optional) Source IP Interface. Valid values are IP interfaces, for example vlan.0.5 for VLAN 5.

-S *ip-address*	(Optional) Source IP address.
-Q *service-type*	(Optional) Specifies the Type of Service in the IPv4 header or the traffic class in the IPv6 header. Valid Range: **0** - **255**. The default value is **0**.
-r	(Optional) Bypass the normal routing tables and send directly to a host on an attached network.
-i	(Optional) Specifies the time in milliseconds to wait for ping timeouts and between sending ping packets. The default value is **1** second.
-v	(Optional) Forces ping to a specific ip version. Valid Values: **4**: Use IPv4 ping, **6**: Use IPv6 ping. The default value is auto-detect. Auto-detect is not configurable.
-V *router*	(Optional) Specify a virtual router name for this ping. The default value is **0** (**default** router).
host	Specifies the IP address or a hostname of the receiving device.

Defaults

- If **-s** is not specified, the number of data bytes sent is **56**.
- If **-c** is not specified, the number of ping packets is **4**.
- If **-I** is not specified, the route table chooses the source IP interface.
- If **-n** is not specified, communication with name servers is not avoided.
- If **-p** is not specified, no hexadecimal pattern is used to fill the outgoing packet.
- If **-t** is not specified, the maximum number of hops for the ping is **64**.
- If **-S** is not specified the source IP address is the address belonging to the management interface.
- If **-Q** is not specified, the type of service or traffic class is **0**.
- If **-r** is not specified, the routing tables are not bypassed when forwarding to a host on an attached network.
- If **-S** is not specified, the route table chooses the source IP address.
- If **-i** is not specified, the ping timeout and time between pings is **1** second.
- If **-v** is not specified, the IP version is auto-detected (not configurable).
- If **-V** is not specified, the virtual router to forward the ICMP echo-reply to is **0** (**default** router).

Mode

All command modes.

Example

This example shows how to ping IP address 127.0.0.1 with 10 packets:

```
S Chassis(rw)->ping -c 10 127.0.0.1
PING 127.0.0.1 (localhost) 64 bytes of data.
64 bytes from 127.0.0.1 (localhost): icmp_seq=0 ttl=64 time=1.58 ms
64 bytes from 127.0.0.1 (localhost): icmp_seq=1 ttl=64 time=1.52 ms
64 bytes from 127.0.0.1 (localhost): icmp_seq=2 ttl=64 time=1.57 ms
64 bytes from 127.0.0.1 (localhost): icmp_seq=3 ttl=64 time=2.26 ms
64 bytes from 127.0.0.1 (localhost): icmp_seq=4 ttl=64 time=1.42 ms
```

```
64 bytes from 127.0.0.1 (localhost): icmp_seq=5 ttl=64 time=2.44 ms
64 bytes from 127.0.0.1 (localhost): icmp_seq=6 ttl=64 time=1.61 ms
64 bytes from 127.0.0.1 (localhost): icmp_seq=7 ttl=64 time=1.40 ms
64 bytes from 127.0.0.1 (localhost): icmp_seq=8 ttl=64 time=2.32 ms
64 bytes from 127.0.0.1 (localhost): icmp_seq=9 ttl=64 time=1.54 ms

--- 127.0.0.1 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 8997 ms
rtt min/avg/max = 1/1/2 ms
S Chassis(rw)->
```

traceroute

Use this command to display a hop-by-hop path through an IP network from the device to a specific destination host.

Syntax

traceroute [-d *ip-address*] **[-F] [-f** *first_ttl*] **[-I] [-i** *interface*] **[-m** *max_ttl*] **[-n] [-p** *port*] **[-q** *nqueries*] **[-r] [-s** *source-address*] **[-t** *tos*] **[-v {4 | 6}] [-V** *router*]**[-w** *waittime*] **[-x]** *host*

Parameters

-d *ip-address*	(Optional) Performs a reverse lookup (finds a hostname that matches the specified IP address).
-F	(Optional) Specifies that the traceroute packet should not be fragmented.
-f *first-TTL*	(Optional) Specifies the maximum Time-To-Live (TTL) used in the first outgoing probe packets. Default value: **1**.
-I	(Optional) Specifies that ICMP echo requests should be used instead of UDP datagrams.
-i *source-interface*	(Optional) Specifies the IP source interface (for example vlan.0.5 for VLAN 5).
-m *max-ttl*	(Optional) Specifies the maximum Time-To-Live (TTL) for outgoing packets. Default value: **30**.
-n host-ip-address	(Optional) Specifies that name server contact should be avoided. All hops are listed numerically.
-p *udp-dest-port*	(Optional) Specifies the initial UDP destination port. For each sent probe the UDP destination port is increased by one. Valid values: **1**-**65535**. Default value: **33434**.
-q *number-of-probes*	(Optional) Specifies the number of probes to send out for each hop. Valid values: **1** - **255**. Default value: **3**.
-r	(Optional) Specifies that normal host routing tables should be bypassed.
-s *source-ip-address*	(Optional) Specifies the source IP address for the traceroute probes.
-t *tos*	(Optional) Specifies the Type-of-Service (ToS) for IPv4 or the traffic class for IPv6. Valid Values **0** - **255**. Default value: **0**.

-v *version*	(Optional) Forces traceroute to use either IPv4: **4** or IPv6: **6**. The IP version is auto-detected by default (not configurable).
-V *router*	(Optional) Specifies the virtual router to use for this traceroute. The default value is **0** (**default** router).
-w *period*	(Optional) Specifies the time in seconds to wait for a response to a probe. Valid values: **0** - **255**. Default value: **5**.
-x	(Optional) Specifies that traceroute should not calculate checksum.
host *host*	Specifies an IP address or a host to find a route to.

Defaults

- If **-d** is not specified, a reverse lookup is not performed.
- If **-F** is not specified, the traceroute will be fragmented if necessary.
- If **-f** is not specified, the maximum TTL in the first probe packet is set to **1**.
- If **-i** is not specified, the route table chooses the source IP interface.
- If **-I** is not specified, UDP datagrams are used.
- If **-m** is not specified, the maximum TTL in outgoing probes is **30**.
- If **-n** is not specified, name server contacts are not avoided.
- If **-p** is not specified, the initial UDP destination port is set to **33434**.
- If **-q** is not specified, the number of probes sent out for each hop is set to **3**.
- If **-r** is not specified, host routing tables are not bypassed.
- If **-s** is not specified, the route table chooses the source IP address.
- If **-t** is not specified, the ToS or traffic class is set to **0**.
- If **-v** is not specified, the IP version is set to **auto-detect**.
- If **-V** is not specified, virtual router 0 (**default**) is used.
- If **-w** is not specified, the time to wait for a probe response is set to **5** seconds.
- If **-x** is not specified, the traceroute calculates the checksum.

Mode

All command modes.

Usage

Possible annotations returned after the probe response time (**-w**) are:

- **!H** - host is unreachable
- **!N** - network is unreachable
- **!P** - protocol is unreachable
- **!S** - source route failed
- **!F**-<pmtu> - fragmentation needed; the RFC1191 Path MTU Discovery value is dis-played
- **TOS=***value***!** - TOS has been altered in the path to <value>
- **!X** - communication administratively prohibited
- **!V** - host precedence violation

- **!C** - precedence cutoff in effect
- **!***num* - ICMP unreachable code *num*

These annotations are defined by RFC1812 which supersedes RFC1716. If almost all the probes result in an unreachable device or type, traceroute will give up and exit.

Example

This example shows how to use traceroute to display a round trip path to host 192.167.252.17. In this case, hop 1 is the Extreme Networks S-Series switch, hop 2 is 14.1.0.45, and hop 3 is back to the host IP address. Round trip times for each of the three UDP probes are displayed next to each hop:

```
S Chassis(rw)->traceroute 192.167.252.17
traceroute to 192.167.252.17 (192.167.252.17), 30 hops max, 40 byte packets
  1  matrix.extremenetworks.com (192.167.201.40)  20.000 ms  20.000 ms  20.000 ms
  2  14.1.0.45 (14.1.0.45)  40.000 ms  10.000 ms  20.000 ms
  3  192.167.252.17 (192.167.252.17)  50.000 ms  0.000 ms  20.000 ms
```

nslookup

Use this command to query name servers, translating hostnames to IP addresses or IP addresses to hostnames.

Syntax

nslookup [**-x**] [**-v** {**4** | **6**}] *host*

Parameters

-x	(Optional) Specifies that a reverse lookup should be performed. If this parameter is used, then you must specify an IP address as the *host* variable.
-v {**4** | **6**}	(Optional) Specifies the IP version for this name server lookup. Auto-detect (non-configurable) is used for a reverse lookup.
host	Specifies the host name, or an IP address, in the case of a reverse lookup.

Defaults

- If reverse lookup is not specified, the lookup is a name lookup.
- If **-v** not specified, the IP version is autodetected.

Mode

All command modes.

Usage

A reverse lookup provides the endpoint IP address and returns the hostname.

Example

The following example performs a reverse lookup providing the host name for IP address 127.0.0.1:

```
S Chassis(su)->nslookup -x 127.0.0.1
Name: localhost
Address: 127.0.0.1
```

20

Discovery Protocol Commands

This chapter provides detailed information for the discovery protocol set of commands. For information about configuring discovery protocol, refer to the "Discovery Protocol Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
Displaying Neighbors	20-1
Extreme Networks Discovery Protocol	20-8
Cisco Discovery Protocol	20-13
Link Layer Discovery Protocol and LLDP-MED	20-19

Displaying Neighbors

This section describes how to display neighbors discovered by all support discovery protocols.

For information about...	Refer to page...
show neighbors	20-1

show neighbors

Use this command to display Network Neighbor Discovery information from all supported discovery protocols.

Syntax

show neighbors [*protocol*] [**-verbose**] [*port-string*] [**wide**]

Parameters

protocol	(Optional) Specifies the protocol type to display for the neighbor. Valid values are: • **cdp** – Displays CDP neighbor information • **ciscodp** – Displays CiscoDp neighbor information • **lldp** – Displays LLDP neighbor information • **lldp-med** – Displays LLDP-MED neighbor information • **lldp-dcb** – Displays LLDP data center bridging neighbor information
-verbose	(Optional) Displays a detailed level of information.

wide	(Optional) Displays a 123 character single line per port summary of Network Neighbor Discovery information.
port-string	(Optional) Displays Network Neighbor Discovery information for a specific port. For a detailed description of possible port-string values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If an optional parameter is not specified, a standard level of all Network Neighbor Discovery information will be displayed.

Mode

All command modes.

Examples

This example shows how to display Network Neighbor Discovery information for port **ge.2.1**:

```
S Chassis(rw)->show neighbors ge.2.1
TYPES:   LL = LLDP         Ct = CtronDp        Ci = CiscoDp

Port      Device ID         Port ID   Ty Network Address
-------------------------------------------------------------------------------
ge.2.1    00-11-88-fe-52-8c ge.1.2    LL 12.10.1.18
ge.2.1    00-11-88-fe-52-8c ge.1.2    Ct 12.10.1.18
ge.2.1    00-11-88-fe-52-8c ge.1.2    Ci 12.10.1.18
```

This example shows how to display protocol type CDP Network Neighbor Discovery information for ports **ge.2.1** and **ge.2.2**:

```
S Chassis(rw)->show neighbors cdp ge.2.1-2
TYPES:   LL = LLDP         Ct = CtronDp        Ci = CiscoDp

Port      Device ID         Port ID   Ty Network Address
-------------------------------------------------------------------------------
ge.2.1    00-11-88-fe-52-8c ge.1.2    Ct 12.10.1.18
ge.2.2    00-1f-45-62-99-24 ge.1.1    Ct 12.10.1.15
```

This example show how to display a verbose level of Network Neighbor Discovery information for port **ge.2.1**:

```
S Chassis(rw)->show neighbors ge.2.1-2 -verbose
Port ge.2.1
  Neighbor                : 00-11-88-fe-52-8c
  Description             : Chassis 1
  Port                    : ge.1.2
  MTU                     : 0
  Last Update             : THU JAN 14 08:11:37 2010
  LLDP
    Chassis Id            : 00-11-88-fe-52-8c
    Port                  : ge.1.2
```

```
    Support               :
    Enabled               :
  CDP
    Neighbor IP           : 12.10.1.18
    Chassis IP            : 12.10.1.18
    Chassis MAC           : 00-11-88-fe-52-8c
    Device Type           : dot1qSwitch
    Support               : ieee8021q, gvrp, igmpSnoop
  CiscoDP
    Device Id             : 00-11-88-fe-52-8c
    Address               : 12.10.1.18
    Port                  : ge.1.2
    Version               : 2
    Primary Management    : 12.10.1.18
    Duplex                : Full Duplex
    Power                 : 0 milliwatts
    Support               : 0x00022

Port ge.2.2
  Neighbor                : 00-1f-45-62-99-24
  Description             : Chassis 1
  Port                    : ge.1.1
  MTU                     : 0
  Last Update             : THU JAN 14 08:11:41 2010
  LLDP
    Chassis Id            : 00-1f-45-62-99-24
    Port                  : ge.1.1
    Support               :
    Enabled               :
  CDP
    Neighbor IP           : 12.10.1.15
    Chassis IP            : 12.10.1.15
    Chassis MAC           : 00-1f-45-62-99-24
    Device Type           : dot1qSwitch
    Support               : ieee8021q, gvrp, igmpSnoop
  CiscoDP
    Device Id             : 00-1f-45-62-99-24
    Address               : 12.10.1.15
    Port                  : ge.1.1
    Version               : 2
    Primary Management    : 12.10.1.15
    Duplex                : Full Duplex
    Power                 : 0 milliwatts
    Support               : 0x00022
S Chassis(rw)->
```

This example show how to display a wide single line summary of Network Neighbor Discovery information for port **ge.2.1**:

```
S Chassis(rw)->show neighbors wide ge.2.1
Port      Device ID                      Port ID                        Type    Network Address
-------------------------------------------------------------------------------------------------
ge.2.1    00-11-88-fe-52-8c              ge.1.2                         LLDP    12.10.1.18
ge.2.1    00-11-88-fe-52-8c              ge.1.2                         CtronDp 12.10.1.18
ge.2.1    00-11-88-fe-52-8c              ge.1.2                         CiscoDp 12.10.1.18
```

Neighbor Warning Detection

This section describes how to set and display protocol checking for port mis-configuration with its neighbor.

For information about...	Refer to page...
set neighbors warning-detection	20-4
clear neighbors warning-detection	20-5
show neighbors warnings	20-6
show neighbors warning-detection	20-7

set neighbors warning-detection

Use this command to enable protocol checking for port mis-configuration (warning detection) with its neighbor.

Syntax

set neighbors warning-detection *warning-type* [*port-string*] {enable | disable}

Parameters

warning-type	The following warning types are supported: • **ciscodp-duplex** – Detect neighbor differences in duplex; defaults to disabled. • **ciscodp-max-frame** – Detect neighbor differences in MTU; defaults to disabled. • **lldp-v2-mac-phy** – Detect neighbor differences in speed and duplex; defaults to enabled. • **lldp-v2-power-via-mdi** – Detect neighbor differences in power class; defaults to enabled. • **lldp-v2-max-frame** – Detect neighbor differences in MTU; defaults to enabled • **lldp-v2-lacp** – Detect neighbor differences in LACP status; defaults to disabled. • **lldp-v2-pfc** – Detect neighbor differences in PFC status; defaults to disabled.
port-string	(Optional) Enables neighbor warning detection on the specified or range of ports. For a detailed description of possible port-string values, refer to the *Extreme Networks S-Series Configuration Guide*.

enable	Enables the protection of neighbor configuration differences for the specified warning type.
disable	Disables the protection of neighbor configuration differences for the specified warning type.

Defaults

- If *port-string* is not specified, neighbor warning detection is enabled on all ports for the specified warning type.
- **ciscodp-duplex** defaults to disabled.
- **ciscodp-max-frame** defaults to disabled.
- **lldp-v2-mac-phy** defaults to enabled.
- **lldp-v2-power-via-mdi** defaults to enabled.
- **lldp-v2-max-frame** defaults to enabled
- **lldp-v2-lacp** defaults to disabled.
- **lldp-v2-pfc** defaults to disabled.

Mode

All command modes.

Usage

Use "show neighbors warning-detection" on page 20-7 to display the state of each warning type on a port basis.

Use "show neighbors warnings" on page 20-6 to display any warnings generated on all or a specified port.

Examples

This example shows how to enable the detect neighbor differences in MTU neighbor warning on all ports:

```
S Chassis(rw)->set neighbor warning-detection lldp-v2-max-frame enable
```

clear neighbors warning-detection

Use this command to reset a warning detection warning type to the default setting for all or specified ports.

Syntax

clear neighbors [*port-string*] **warning-detection** *warning-type*

Parameters

port-string	(Optional) disables neighbor warning detection on the specified or range of ports. For a detailed description of possible port-string values, refer to the *Extreme Networks S-Series Configuration Guide*.

warning-type	The following warning types are supported: • **ciscodp-duplex** – Detect neighbor differences in duplex • **ciscodp-max-frame** – Detect neighbor differences in MTU • **lldp-v2-mac-phy** – Detect neighbor differences in speed and duplex • **lldp-v2-power-via-mdi** – Detect neighbor differences in power class • **lldp-v2-max-frame** – Detect neighbor differences in MTU • **lldp-v2-lacp** – Detect neighbor differences in LACP status • **lldp-v2-pfc** – Detect neighbor differences in PFC status

Defaults

- If *port-string* is not specified, neighbor warning detection is reset to the default value on all ports for the specified warning type.
- **ciscodp-duplex** defaults to disabled.
- **ciscodp-max-frame** defaults to disabled.
- **lldp-v2-mac-phy** defaults to enabled.
- **lldp-v2-power-via-mdi** defaults to enabled.
- **lldp-v2-max-frame** defaults to enabled
- **lldp-v2-lacp** defaults to disabled.
- **lldp-v2-pfc** defaults to disabled.

Mode

All command modes.

Examples

This example shows how to disable the detect neighbor differences in MTU warning type on all ports:

```
S Chassis(rw)->set neighbor warning-detection lldp-v2-max-frame
```

show neighbors warnings

Use this command to display neighbors with warnings due to enabled warning detection hits on the port.

Syntax

show neighbors warnings [*warning-type*] [*port-string*]

Parameters

warning-type	(Optional) Specifies the warning type to display for the neighbor. Valid values are: • **lldp-v2-mac-phy** – Neighbor differences in speed and duplex • **lldp-v2-power-via-mdi** – Neighbor differences in power class • **lldp-v2-max-frame** – Neighbor differences in MTU • **lldp-v2-lacp** – Neighbor differences in LACP status • **lldp-v2-pfc** – Neighbor differences in PFC status
port-string	(Optional) Displays warnings that have been generated for a specific port. For a detailed description of possible port-string values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If an optional parameter is not specified, all generated warnings for all ports display.

Mode

All command modes.

Examples

This example shows how to display neighbor warnings generated for port **ge.1.17**:

```
S Chassis(rw)->show neighbors warnings ge.1.17
Port:                        ge.1.17
Connection Index:            2
Remote Chassis Type:         chasIdMacAddress
Remote Chassis Description: 00-1f-45-5b-f4-f7
Configuration mismatch:
  Local duplex is full, but is half on peer with MAC address 00-1f-45-5b-f5-0a.
```

show neighbors warning-detection

Use this command to display the status of each neighbors warning type for all or specified ports.

Syntax

show neighbors warning-detection [*port-string*]

Parameters

port-string	(Optional) Displays the status of each neighbor warning type for the specified port(s). For a detailed description of possible port-string values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If the *port-string* is not specified, neighbor warning type status is displayed for all ports.

Mode

All command modes.

Examples

This example shows how to display the status of each neighbor warning type for ports **ge.1.1-5**:

```
S Chassis(rw)->show neighbors warning-detection ge.1.1-5
* Means protocol is supported and enabled for warning detection
o Means protocol is supported for warning detection
Port     |  LLDP |     CISCO    |          LLDPV2         |
         |med-poe|duplx pwr mtu|mac-phy pwr mtu lag pfc|
--------- ------- ----- --- --- ------- --- --- --- ---
ge.1.1       o      o    o   o     *     *   *   o   o
ge.1.2       o      o    o   o     *     *   *   o   o
ge.1.3       o      o    o   o     *     *   *   o   o
ge.1.4       o      o    o   o     *     *   *   o   o
ge.1.5       o      o    o   o     *     *   *   o   o
```

Extreme Networks Discovery Protocol

This section describes how to enable and configure the Extreme Networks Discovery Protocol (CDP), used to discover network topology. When enabled, CDP allows Extreme Networks devices to send periodic PDUs about themselves to neighboring devices.

For information about...	Refer to page...
show cdp	20-8
set cdp state	20-10
set cdp auth	20-10
set cdp interval	20-11
set cdp hold-time	20-11
clear cdp	20-12

show cdp

Use this command to display the status of the CDP discovery protocol and message interval on one or more ports.

Syntax

show cdp [*port-string*]

Parameters

port-string	(Optional) Displays CDP status for a specific port. For a detailed description of possible port-string values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, all CDP information will be displayed.

Mode

All command modes.

Example

This example shows how to display CDP information for ports **ge.1.1** through **ge.1.9**:

```
S Chassis(rw)->show cdp ge.1.1-9
CDP Global Status         : enabled
CDP Versions Supported    : 0x0 0x38
CDP Hold Time             : 180
CDP Authentication Code   : 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
0x0 0x0
CDP Transmit Frequency    : 60

Port        Status
-----------------
ge.1.1      auto-enable
ge.1.2      auto-enable
ge.1.3      auto-enable
ge.1.4      auto-enable
ge.1.5      auto-enable
ge.1.6      auto-enable
ge.1.7      auto-enable
ge.1.8      auto-enable
ge.1.9      auto-enable
```

Table 20-1 provides an explanation of the command output.

Table 20-1 show cdp Output Details

Output...	What it displays...
CDP Global Status	Whether CDP is globally auto-enabled, enabled or disabled. The default state of auto-enabled can be reset with the **set cdp state** command. For details, refer to “set cdp state” on page 20-10.
CDP Versions Supported	CDP version number(s) supported by the device.
CDP Hold Time	Minimum time interval (in seconds) at which CDP configuration messages can be set. The default of 180 seconds can be reset with the **set cdp hold-time** command. For details, refer to “set cdp hold-time” on page 20-11.
CDP Authentication Code	Authentication code for CDP discovery protocol. The default of 00-00-00-00-00-00-00-00 can be reset using the **set cdp auth** command. For details, refer to “set cdp auth” on page 20-10.
CDP Transmit Frequency	Frequency (in seconds) at which CDP messages can be transmitted. The default of 60 seconds can be reset with the **set cdp interval** command. For details, refer to “set cdp interval” on page 20-11.
Port	Port designation. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
Status	Whether CDP is enabled, disabled or auto-enabled on the port.

set cdp state

Use this command to enable or disable the CDP discovery protocol on one or more ports.

Syntax

set cdp state {**auto** | **disable** | **enable**} [*port-string*]

Parameters

auto | **disable** | **enable**	Auto-enables, disables, or enables the CDP protocol on the specified ports. In auto-enable mode, which is the default mode for all ports, a port automatically becomes CDP-enabled upon receiving its first CDP message.
port-string	(Optional) Enables or disables CDP on specific ports.

Defaults

If *port-string* is not specified, the CDP state will be globally set.

Mode

All command modes.

Examples

This example shows how to globally enable CDP:

```
S Chassis(rw)->set cdp state enable
```

This example shows how to enable CDP for port **ge.1.2**:

```
S Chassis(rw)->set cdp state enable ge.1.2
```

This example shows how to disable CDP for port **ge.1.2**:

```
S Chassis(rw)->set cdp state disable ge.1.2
```

set cdp auth

Use this command to set a global CDP authentication code.

Syntax

set cdp auth *auth-code*

Parameters

auth-code	Specifies an authentication code for the CDP protocol. This can be up to 16 hexadecimal values separated by commas. The default value is **00-00-00-00-00-00-00-00**.

Defaults

None.

Mode

All command modes.

Usage

This value determines a device's CDP domain. If two or more devices have the same CDP authentication code, they will be entered into each other's CDP neighbor tables. If they have different authentication codes, they are in different domains and will not be entered into each other's CDP neighbor tables.

A device with the default authentication code (16 null characters) will recognize all devices, no matter what their authentication code, and enter them into its CDP neighbor table.

Example

This example shows how to set the CDP authentication code to **1,2,3,4,5,6,7,8**:

```
S Chassis(rw)->set cdp auth 1,2,3,4,5,6,7,8
```

set cdp interval

Use this command to set the message interval frequency (in seconds) of the CDP discovery protocol.

Syntax

set cdp interval *frequency*

Parameters

frequency	Specifies the transmit frequency of CDP messages in seconds.Valid values are **5–900** seconds. The default value is **60** seconds.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the CDP interval frequency to **15** seconds:

```
S Chassis(rw)->set cdp interval 15
```

set cdp hold-time

Use this command to set the hold time value for CDP discovery protocol configuration messages.

Syntax

set cdp hold-time *hold-time-val*

Parameters

hold-time-val	Specifies the hold time value for CDP messages in seconds.Valid values are **15–600**. The default value is **180** seconds.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set CDP hold time to **60** seconds:

```
S Chassis(rw)->set cdp hold-time 60
```

clear cdp

Use this command to reset CDP discovery protocol settings to defaults.

Syntax

clear cdp {[**state**] [**port-state** *port-string*] [**interval**] [**hold-time**] [**auth-code**]}

Parameters

state	(Optional) Resets the global CDP state to auto-enabled.
port-state *port-string*	(Optional) Resets the port state on specific port(s) to auto-enabled.
interval	(Optional) Resets the message frequency interval to **60** seconds.
hold-time	(Optional) Resets the hold time value to **180** seconds.
auth-code	(Optional) Resets the authentication code to 16 bytes of 00 (**00-00-00-00-00-00-00-00**).

Defaults

At least one optional parameter must be entered.

Mode

All command modes.

Example

This example shows how to reset the CDP state to auto-enabled:

```
S Chassis(rw)->clear cdp state
```

Cisco Discovery Protocol

This section describes how to enable and configure the Cisco Discovery Protocol, used to discover network topology. When enabled, the Cisco Discovery Protocol allows Cisco devices to send periodic PDUs about themselves to neighboring devices. The Cisco Discovery Protocol is also used to manage the Cisco module of the Convergence End Points (CEP) IP phone detection function described in Chapter 92, **Convergence End Points (CEP) Phone Detection Commands**.

For information about...	Refer to page...
show ciscodp	20-13
show ciscodp port info	20-14
set ciscodp status	20-15
set ciscodp timer	20-16
set ciscodp holdtime	20-16
set ciscodp port	20-17
clear ciscodp	20-18

show ciscodp

Use this command to display global Cisco Discovery Protocol information.

Syntax

```
show ciscodp
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display Cisco Discovery Protocol information. In this case, defaults have not been changed:

```
S Chassis(rw)->show ciscodp
CiscoDP : Auto
Timer : 60
Holdtime (TTL) : 180
Device ID : 00E06314BD57
Last Change : WED FEB 08 01:07:45 2006
```

Table 20-2 provides an explanation of the command output.

Table 20-2 show ciscodp Output Details

Output...	What it displays...
CiscoDP	Whether Cisco Discovery Protocol is disabled or enabled globally. Auto indicates that Cisco DP will be globally enabled only if Cisco DP PDUs are received. Default setting of auto can be changed with the **set ciscodp status** command as described in "set ciscodp status" on page 20-15.
Timer	Number of seconds between Cisco Discovery Protocol PDU transmissions. Default value of **60** can be changed with the **set ciscodp timer** command as described in "set ciscodp timer" on page 20-16.
Holdtime (TTL)	Number of seconds neighboring devices will hold PDU transmissions from the sending device. Default value of **180** can be changed with the **set ciscodp holdtime** command as described in "set ciscodp holdtime" on page 20-16.
Device ID	The MAC address of the switch.
Last Change	The time that the last Cisco DP neighbor was discovered.

show ciscodp port info

Use this command to display summary information about the Cisco Discovery Protocol on one or more ports.

Syntax

show ciscodp port info [*port-string*]

Parameters

port-string	(Optional) Displays information about specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, CiscoDP information will be displayed for all ports.

Mode

All command modes.

Example

This example shows how to display Cisco Discovery Protocol information for ports **ge.1.1** through **ge.1.5**:

```
S Chassis(rw)->(su)->show ciscodp port info ge.1.1-5
 port       state    vvid      trust      cos
-----------------------------------------------
ge.1.1     enabled   none     untrusted    0
ge.1.2     enabled   none     untrusted    0
ge.1.3     enabled   none     untrusted    0
ge.1.4     enabled   none     untrusted    0
```

```
ge.1.5     enabled   none     untrusted    1
```

Table 20-3 provides an explanation of the command output.

Table 20-3 show port ciscodp info Output Details

Output...	What it displays...
Port	Port designation.
State	Whether CiscoDP is enabled or disabled on this port. Default state of enabled can be changed using the **set ciscodp port** command (“set ciscodp port” on page 20-17).
VVID	Whether a Voice VLAN ID has been set on this port. Default of none can changed using the **set ciscodp port** command (“set ciscodp port” on page 20-17).
Trust	The trust mode of the port. Default of trusted can be changed using the **set ciscodp port** command (“set ciscodp port” on page 20-17).
CoS	The Class of Service priority value for untrusted traffic. The default of 0 can be changed using the **set ciscodp port** command (“set ciscodp port” on page 20-17).

set ciscodp status

Use this command to enable or disable Cisco Discovery Protocol globally on the device.

Syntax

set ciscodp status {**auto** | **enable** | **disable**}

Parameters

auto	Globally enables only if CiscoDP PDUs are received.
enable	Globally enables Cisco Discovery Protocol.
disable	Globally disables Cisco Discovery Protocol.

Defaults

None.

Mode

All command modes.

Example

This example shows how to enable Cisco Discovery Protocol on the device:

```
S Chassis(rw)->set ciscodp status enable
```

set ciscodp timer

Use this command to set the number of seconds between Cisco Discovery Protocol PDU transmissions.

Syntax

set ciscodp timer *time*

Parameters

time	Specifies the number of seconds between CiscoDP PDU transmissions. Valid values are **5** - **254**.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the Cisco Discovery Protocol timer to **120** seconds:

```
S Chassis(rw)->set ciscodp timer 120
```

set ciscodp holdtime

Use this command to set the time to live (TTL) for Cisco Discovery Protocol PDUs. This is the amount of time (in seconds) neighboring devices will hold PDU transmissions from the sending device.

Syntax

set ciscodp holdtime *time*

Parameters

time	Specifies the time to live for CiscoDP PDUs. Valid values are **10** - **255**.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the Cisco Discovery Protocol hold time to **180** seconds:

```
S Chassis(rw)->set ciscodp holdtime 180
```

set ciscodp port

Use this command to set the status, voice VLAN, extended trust mode, and CoS priority for untrusted traffic for the Cisco Discovery Protocol on one or more ports.

Syntax

```
set ciscodp port {[status {disable | enable}] [vvid {vlan-id | none | dot1p |
untagged}] [trust-ext {trusted | untrusted}] [cos-ext value]} port-string
```

Parameters

status	Sets the CiscoDP port operational status.
disable	Does not transmit or process CiscoDP PDUs.
enable	Transmits and processes CiscoDP PDUs.
vvid	Sets the port voice VLAN for CiscoDP PDU transmission.
vlan-id	Specifies the VLAN ID, range 1-4094.
none	No voice VLAN will be used in CiscoDP PDUs.
dot1p	Instructs attached phone to send 802.1p tagged frames.
untagged	Instructs attached phone to send untagged frames.
trust-ext	Sets the extended trust mode on the port.
trusted	Instructs attached phone to allow the device connected to it to transmit traffic containing any CoS or Layer 2 802.1p marking. This is the default value.
untrusted	Instructs attached phone to overwrite the 802.1p tag of traffic transmitted by the device connected to it to 0, by default, or to the value configured with the **cos-ext** parameter.
cos-ext *value*	Instructs attached phone to overwrite the 802.1p tag of traffic transmitted by the device connected to it with the specified *value*, when the trust mode of the port is set to untrusted. *Value* can range from 0 to 7, with 0 indicating the lowest priority.
port-string	Specifies the port(s) on which status will be set. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Usage

Note: The Cisco Discovery Protocol must be globally enabled using the **set ciscodp status** command as described in “set ciscodp status” on page 20-15 before operational status can be set on individual ports.

The following points describe how the Cisco DP extended trust settings work on the Extreme Networks device.

- A Cisco DP port trust status of trusted or untrusted is only meaningful when a Cisco IP phone is connected to a switch port and a PC or other device is connected to the back of the Cisco IP phone.
- A Cisco DP port state of trusted or untrusted only affects tagged traffic transmitted by the device connected to the Cisco IP phone. Untagged traffic transmitted by the device connected to the Cisco IP phone is unaffected by this setting.
- If the switch port is configured to a Cisco DP trust state of **trusted** (with the **trust-ext trusted** parameter of this command), this setting is communicated to the Cisco IP phone instructing it to allow the device connected to it to transmit traffic containing any CoS or Layer 2 802.1p marking.
- If the switch port is configured to a Cisco DP trust state of **untrusted**, this setting is communicated to the Cisco IP phone instructing it to overwrite the 802.1p tag of traffic transmitted by the device connected to it to 0, by default, or to the value specified by the **cos-ext** parameter of this command.

There is a one-to-one correlation between the value set with the **cos-ext** parameter and the 802.1p value assigned to ingressed traffic by the Cisco IP phone. A value of 0 equates to an 802.1p priority of 0. Therefore, a value of 7 is given the highest priority.

Examples

This example shows how to set the Cisco DP port voice VLAN ID to 3 on port ge.1.6 and enable the transmission and processing of the Cisco DP PDUs on the port:

```
S Chassis(rw)->set ciscodp port status enable vvid 3 ge.1.6
```

This example shows how to set the Cisco DP extended trust mode to untrusted on port **ge.1.5** and set the CoS priority to **1**:

```
S Chassis(rw)->set ciscodp port trust-ext untrusted cos-ext 1 ge.1.5
```

clear ciscodp

Use this command to clear the Cisco Discovery Protocol back to the default values.

Syntax

clear ciscodp {[**status** | **timer | holdtime | port** {**status** | **vvid | trust-ext | cos-ext**}]} *port-string*

Parameters

status	Clears global CiscoDP enable status to default of auto.
timer	Clears the time between CiscoDP PDU transmissions to default of 60 seconds.
holdtime	Clears the time-to-live for CiscoDP PDU data to default of 180 seconds.
port	Clears the CiscoDP port configuration.
status	Clears the individual port operational status to the default of enabled.
vvid	Clears the individual port voice VLAN for CiscoDP PDU transmission to 0.
trust-ext	Clears the trust mode configuration of the port to trusted.

cos-ext	Clears the CoS priority for untrusted traffic of the port to 0.
port-string	Specifies the port(s) on which status will be set. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to clear all the Cisco DP parameters back to the default settings:

```
S Chassis(rw)->clear ciscodp
```

This example shows how to clear the Cisco DP port status on port **ge.1.5**:

```
S Chassis(rw)->clear ciscodp port status ge.1.5
```

Link Layer Discovery Protocol and LLDP-MED

This section describes the display and setting of the Link Layer Discovery Protocol and LLDP-MED.

For information about...	Refer to page...
show lldp	20-20
show lldp port status	20-21
show lldp port trap	20-21
show lldp port tx-tlv	20-22
show lldp port location-info	20-23
show lldp port local-info	20-24
show lldp port remote-info	20-29
show lldp port network-policy	20-32
set lldp tx-interval	20-33
set lldp tx-fast-count	20-33
set lldp tx-fast-interval	20-34
set lldp hold-multiplier	20-35
set lldp trap-interval	20-35
set lldp med-fast-repeat	20-36
set lldp port status	20-37
set lldp port trap	20-37
set lldp port med-trap	20-38
set lldp port location-info	20-38

For information about...	Refer to page...
set lldp port tx-tlv	20-39
set lldp port network-policy	20-41
clear lldp	20-43
clear lldp port status	20-43
clear lldp port trap	20-44
clear lldp port med-trap	20-44
clear lldp port location-info	20-45
clear lldp port network-policy	20-45
clear lldp port tx-tlv	20-46

show lldp

Use this command to display LLDP configuration information.

Syntax

show lldp

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display LLDP configuration information.

```
S Chassis(rw)->show lldp
Message Tx Interval         : 30
Message Tx Hold Multiplier  : 4
Notification Tx Interval    : 5
MED Fast Start Count        : 3
Tx-Enabled Ports            : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12;
                              ge.5.1-12; tg.6.1-2; ge.7.1-48
Rx-Enabled Ports            : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12;
                              ge.5.1-12;tg.6.1-2; ge.7.1-48
Trap-Enabled Ports          : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12;
                              ge.5.1-12; tg.6.1-2; ge.7.1-48
MED Trap-Enabled Ports      : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12;
                              ge.5.1-12;tg.6.1-2; ge.7.1-48
```

show lldp port status

Use this command to display the LLDP status of one or more ports.

Syntax

show lldp port status [*port-string*]

Parameters

port-string	(Optional) Displays LLDP status for one or a range of ports.

Defaults

If *port-string* is not specified, LLDP status information will be displayed for all ports.

Mode

All command modes.

Usage

The command lists the ports that are enabled to send and receive LLDP Data Units (LLDP DUs). Ports are enabled or disabled with the set lldp port status command.

Example

This example shows how to display LLDP port status information for all ports.

```
S Chassis(rw)->show lldp port status

Tx-Enabled Ports      : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12; ge.5.1-12;
                        tg.6.1-2; ge.7.1-48
Rx-Enabled Ports      : ge.1.1-60; ge.2.1-24; ge.3.1-30; ge.4.1-12; ge.5.1-12;
                        tg.6.1-2; ge.7.1-48
```

show lldp port trap

Use this command to display the ports that are enabled to send an LLDP notification when a remote system change has been detected or an LLDP-MED notification when a change in the topology has been sensed.

Syntax

show lldp port trap [*port-string*]

Parameters

port-string	(Optional) Displays the port or range of ports that have been enabled to send LLDP or LLDP-MED notifications.

Defaults

If *port-string* is not specified, LLDP port trap information will be displayed for all ports.

Mode

All command modes.

Usage

Ports are enabled to send LLDP notifications with the set lldp port trap command and to send LLDP-MED notifications with the set lldp port med-trap command.

Example

This example shows how to display LLDP port trap information for all ports.

```
S Chassis(rw)->show lldp port trap

Trap-Enabled Ports          : ge.1.1-5
MED Trap-Enabled Ports      :
S Chassis(rw)->
```

show lldp port tx-tlv

Use this command to display information about which optional TLVs have been configured to be transmitted on ports.

Syntax

show lldp port tx-tlv [**data-center-bridging**] [*port-string*]

Parameters

data-center-bridging	(Optional) Displays data center bridging specific status including Enhanced Transmission Selection configuration, recommendation, and priority flow control.
port-string	(Optional) Displays information about TLV configuration for one or a range of ports.

Defaults

If *port-string* is not specified, TLV configuration information will be displayed for all ports.

If **data-center-bridging** is not specified, Data Center Bridging (DCB) specific status is not displayed for the ports.

Mode

All command modes.

Usage

Ports are configured to send optional TLVs with the set lldp port tx-tlv command.

When the **data-center-bridging** option is specified, ETS Con refers to LLDP-DCB Enhanced-Trans-Config TLV and ETS Rec refers to LLDP-DCB Enhanced-Trans-Rec TLV.

Example

This example shows how to display transmit TLV information for port **ge.1.25**.

```
S Chassis(rw)->sh lldp port tx-tlv ge.1.25

* Means TLV is supported and enabled on this port
o Means TLV is supported on this port
  Means TLV is not supported on this port
Column Pro Id uses letter notation for enable: s-stp, l-lacp, g-gvrp
For Data Center Bridging (DCB) TLV breakdown use data-center-bridging option
Ports    Port Sys  Sys  Sys Mgmt Vlan Pro  MAC PoE Link Max   MED MED MED MED DCB EEE
         Desc Name Desc Cap Addr Id   Id   PHY     Aggr Frame Cap Pol Loc PoE
-------  ---- ---- ---- --- ---- ---- ---- --- --- ---- ----  --- --- --- --- --- ---
ge.1.25  o    o    o    o   o    o    o    o   o   o    o     o   o   o   o   o   o
```

This example shows how to display Data Center Bridging (DCB) information for three ports.

```
S Chassis(rw)->show lldp port tx-tlv data-center-bridging ge.1.1-3
* Means TLV is supported and enabled on this port
o Means TLV is supported on this port
  Means TLV is not supported on this port

Ports    ETS  ETS  PFC  App CN
         Con  Rec       Pri
-------  ---- ---- ---- --- ---
ge.1.1   o    o    o    o    o
ge.1.2   o    o    o    o    o
ge.1.3   o    o    o    o    o
```

show lldp port location-info

Use this command to display configured location information for one or more ports.

Syntax

show lldp port location-info [*port-string*]

Parameters

port-string	(Optional) Displays port location information for one or a range of ports.

Defaults

If *port-string* is not specified, port location configuration information will be displayed for all ports.

Mode

All command modes.

Usage

Ports are configured with a location value using the set lldp port location-info command.

Example

This example shows how to display port location information for three ports.

```
S Chassis(rw)->show lldp port location-info ge.1.1-3

Ports      Type            Location
--------   -------------   -------------------------
ge.1.1     ELIN            1234567890
ge.1.2     ELIN            1234567890
ge.1.3     ELIN            1234567890
```

show lldp port local-info

Use this command to display the local system information stored for one or more ports.

Syntax

show lldp port local-info [*port-string*]

Parameters

port-string	(Optional) Displays local system information for one or a range of ports.

Defaults

If *port-string* is not specified, local system information will be displayed for all ports.

Mode

All command modes.

Usage

You can use this information to detect misconfigurations or incompatibilities between the local port and the attached endpoint device (remote port).

Example

This example shows how to display the local system information stored for port **ge.1.25**. Table 20-4 describes the output fields of this command.

```
S Chassis(rw)->sh lldp port local-info ge.1.25
Local Port  : ge.1.25    Local Port Id  : ge.1.25
---------------------
Port Desc   : Extreme Networks, Inc. 1000BASE-T RJ45 Gigabit Ethernet
              Frontpanel Port
Mgmt Addr   : 20-b3-99-ad-ce-fd
Sys Desc    : Extreme Networks, Inc. S-Series Rev 08.20.01.0025T
              11/14/2013--19:59 ofc
Sys Cap Supported/Enabled     : bridge,router/bridge
Auto-Neg Supported/Enabled    : yes/yes
Auto-Neg Advertised           : 10BASE-TFD
```

```
                                : 100BASE-TXFD
                                : 1000BASE-TFD
                                : Bpause
Operational Speed/Duplex/Type :
Max Frame Size (bytes)        : 1522
Vlan Id                       : 1
LAG Supported/Enabled/Id      : no/no/0
Protocol Id : spanning tree v-3 (IEEE802.1s)
Unknown Network Policy
(app/tag)                     : voice/untagged
                                voice signaling/untagged
                                guest voice/untagged
                                guest voice signaling/untagged
                                softphone voice/untagged
                                video conferencing/untagged
                                streaming video/untagged
                                video signaling/untagged
PoE Device                    : PSE device (Type 1)
PoE Power Source              : backup
PoE MDI Supported/Enabled     : yes/yes
PoE Pair Controllable/Used    : no/signal
PoE Power Class               : 0
PoE Power Limit (mW)          : 15400
PoE Power Priority            : low
PoE PD Requested Power (dW)   : 0
PoE PSE Allocated Power (dW)  : 0
PoE Reduced Oper Power (dW)   : 0
PoE Response Time (seconds)   : 1
PoE Ready                     : yes
Enhanced Transmission Selection
 Configuration
  Max Traffic Classes         : 8
  Willing                     : no
  Credit Base Shaper Supported: no
  Priority Assignment         : Pri[0]:   0 Pri[1]:   0 Pri[2]:   0 Pri[3]:   0
                                : Pri[4]:   0 Pri[5]:   0 Pri[6]:   0 Pri[7]:   0
  Traffic Class Bandwidth     : TC [0]:  0% TC [1]:  0% TC [2]:  0% TC [3]:  0%
                                : TC [4]:  0% TC [5]:  0% TC [6]:  0% TC [7]:100%
  TSA Assignment              : TC [0]:   0 TC [1]:   0 TC [2]:   0 TC [3]:   0
                                : TC [4]:   0 TC [5]:   0 TC [6]:   0 TC [7]:   0
 Recommendation
  Priority Assignment         : Pri[0]:   0 Pri[1]:   0 Pri[2]:   0 Pri[3]:   0
                                : Pri[4]:   0 Pri[5]:   0 Pri[6]:   0 Pri[7]:   0
  Traffic Class Bandwidth     : TC [0]:  0% TC [1]:  0% TC [2]:  0% TC [3]:  0%
                                : TC [4]:  0% TC [5]:  0% TC [6]:  0% TC [7]:  0%
```

```
  TSA Assignment              : TC [0]:   0 TC [1]:   0 TC [2]:   0 TC [3]:   0
                              : TC [4]:   0 TC [5]:   0 TC [6]:   0 TC [7]:   0
Priority Flow Control
  Willing                     : no
  MACsec Bypass Capability    : yes
  Capability                  : 6
  Enable                      : Pri[0]:   0 Pri[1]:   0 Pri[2]:   0 Pri[3]:   0
                              : Pri[4]:   0 Pri[5]:   0 Pri[6]:   0 Pri[7]:   0
Congestion Notification
  PV Indicators               : Pri[0]:   0 Pri[1]:   0 Pri[2]:   0 Pri[3]:   0
                              : Pri[4]:   0 Pri[5]:   0 Pri[6]:   0 Pri[7]:   0
  Ready Indicators            : Pri[0]:   0 Pri[1]:   0 Pri[2]:   0 Pri[3]:   0
                              : Pri[4]:   0 Pri[5]:   0 Pri[6]:   0 Pri[7]:   0
Energy Efficient Ethernet
 TxTwSysLoc                   : 30
 TxTwSysEchoLoc               : 17
 RxTwSysLoc                   : 30
 RxTwSysEchoLoc               : 17
 FbTwSysLoc                   : 17
 TxDllReady                   : False
 RxDllReady                   : False
 DllEnabled                   : False
```

Table 20-4 describes the information displayed by the **show lldp port local-info** command.

Table 20-4 show lldp port local-info Output Details

Output...	What it displays...
Local Port	Identifies the port for which local system information is displayed.
Local Port Id	Mandatory basic LLDP TLV that identifies the port transmitting the LLDPDU. Value is ifName object defined in RFC 2863.
Port Desc	Optional basic LLDP TLV. Value is ifDescr object defined in RFC 2863.
Mgmt Addr	Optional basic LLDP TLV. IPv4 address of host interface.
Sys Desc	Optional basic LLDP TLV. Value is sysDescr object defined in RFC 3418.
Sys Cap Supported/Enabled	Optional basic LLDP TLV. System capabilities, value can be bridge and/or router.
Auto-Neg Supported/Enabled	IEEE 802.3 Extensions MAC-PHY Configuration/Status TLV. Auto-negotiation supported and enabled settings should be the same on the two systems attached to the same link.
Auto-Neg Advertised	IEEE 802.3 Extensions MAC-PHY Configuration/Status TLV. Lists the configured advertised values on the port.
Operational Speed/Duplex/Type	IEEE 802.3 Extensions MAC-PHY Configuration/Status TLV. Lists the operational MAU type, duplex, and speed of the port. If the received TLV indicates that auto-negotiation is supported but not enabled, these values will be used by the port.

Table 20-4 show lldp port local-info Output Details (continued)

Output...	What it displays...
Max Frame Size (bytes)	IEEE 802.3 Extensions Maximum Frame Size TLV. Value indicates maximum frame size capability of the device's MAC and PHY. In normal mode, max frame size is 1522 bytes. In jumbo mode, max frame size is 10239 bytes.
Vlan Id	IEEE 802.1 Extensions Port VLAN ID TLV. Value is port VLAN ID (pvid).
LAG Supported/Enabled/Id	IEEE 802.3 Extensions Link Aggregation TLV. Values indicate whether the link associated with this port can be aggregated, whether it is currently aggregated, and if aggregated, the aggregated port identifier.
PoE Device	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Value is the Power Type of the device. On a Extreme Networks switch port, the value is Power Sourcing Entity (PSE), type 1.
PoE Power Source	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Value can be primary or backup, indicating whether the PSE is using its primary or backup power source.
PoE MDI Supported/Enabled	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates whether sending the Power via MDI TLV is supported/enabled. Value can be yes or no.
PoE Pair Controllable/Used	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates whether pair selection can be controlled on the given port (refer to RFC 3621). Value for Controllable can be true or false. Value of Used can be signal (signal pairs only are in use) or spare (spare pairs only are in use).
PoE Power Class	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates the power class supplied by the port. Value can range from 1 to 5.
PoE Power Limit (mW)	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates the total power the port is capable of sourcing over a maximum length cable, based on its current configuration, in milliwatts.
PoE Power Priority	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates the power priority configured on the port. Value can be low, high, critical, or unknown.
PoE PD Requested Power (dW)	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates amount of power local PSE device has mirrored back to remote PD, in deciwatts. If the local device is a PD, indicates amount of power requested to remote PSE, in deciwatts.
PoE PSE Allocated Power (dW)	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates the maximum amount of power local PSE device has allocated for remote PD, in deciwatts. If the local device is a PD, indicates amount of power mirrored back to remote PSE, in deciwatts.
PoE Reduced Oper Power (dW)	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates amount of reduced power in deciwatts that the local PSE can allocate to the remote PD that will continue to keep it somewhat operational. If local device is a PD, indicates a reduced power amount in deciwatts that the PD can still be operational with, even if lacking some functionality.

Table 20-4 show lldp port local-info Output Details (continued)

Output...	What it displays...
PoE Response Time (seconds)	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates the maximum response time in seconds of the local PSE to update PoE PD Requested Power Value when the remote D requests a new power value.
PoE Ready	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates whether the local system has completed initialization and is ready to receive and process LLDPDUs.
Enhanced Transmission Selection Configuration	IEEE 802.1Qaz Enhanced Transmission Selection parameters provide a common management framework for assignment of bandwidth to 802.1p CoS-based traffic classes.
Max Traffic Classes	Maximum number of supported Enhanced Transmission Selection Traffic Classes supported.
Willing	An Enhanced Transmission Selection or Priority Flow Control setting that indicates whether the station is willing to accept configurations from a remote station.
Credit Base Shaper Supported	Specifies whether the device supports the Credit-based Shaper Transmission Selection algorithm. Currently not supported on Extreme Networks devices.
Priority Assignment	Specifies the traffic class group to which the specified priority is assigned.
Traffic Class Bandwidth	Specifies the percent of bandwidth assigned to the traffic class.
TSA Assignment	Specifies the Transmission Selection Algorithm per priority: **0** = strict priority, **1** = Credit-based Shaper, **2** = Enhanced Transmission Selection, **255** = vendor specific.
MACsec Bypass Capability	Specifies whether the MACsec Bypass capability is supported or not.
Capability	Specifies the number of PFCs supported by the device.
Enable	Specifies whether the listed priority is enabled for Priority Flow Control. **0** = disabled, **1** = enabled.
Recommendation	A TLV encoded into each IEEE Standard 802.1AB LLDP message that indicates a recommendation on how Enhanced Transmission Selection should be configured.
Priority Assignment	Specifies the traffic class group to which the specified priority is assigned.
Traffic Class Bandwidth	Specifies the recommended percent of bandwidth per traffic class.
TSA Assignment	Specifies the recommended Transmission Selection Algorithm per priority: **0** = strict priority, **1** = Credit-based Shaper, **2** = Enhanced Transmission Selection, **255** = vendor specific.
TxTwSysLoc	Specifies the system wake time the local system can support in the transmit direction.
TxTwSysEchoLoc	Specifies the system wake time advertised by the remote system that can be supported in the transmit direction.
RxTwSysLoc	Specifies the system wake time the local system is requesting in the receive direction.
RxTwSysEchoLoc	Specifies the system wake time advertised by the remote system, requested in the receive direction and echoed by the local system.

Table 20-4 show lldp port local-info Output Details (continued)

Output...	What it displays...
FbTwSysLoc	Specifies the fallback system wake time the local system is advertising to the remote system.
TxDllReady	Specifies the boolean value used to identify whether the local Data Link Layer EEE layer management function has completed initialization and is ready to receive and transmit LLDPDUs.
RxDllReady	Specifies the boolean value used to identify whether the local Data Link Layer EEE layer management function has completed initialization and is ready to receive and transmit LLDPDUs.
DllEnabled	Specifies the boolean value used to identify whether the local system has completed auto-negotiation with a link partner that has indicated at least one EEE capability.

show lldp port remote-info

Use this command to display the remote system information stored for a remote device connected to a local port.

Syntax

show lldp port remote-info [*port-string*]

Parameters

port-string	(Optional) Displays remote system information for one or a range of ports.

Defaults

If *port-string* is not specified, remote system information will be displayed for all ports.

Mode

All command modes.

Usage

You can use this information to detect misconfigurations or incompatibilities between the local port and the attached endpoint device (remote port).

Example

This example shows how to display the remote system information stored for port **ge.2.1**:

```
S Chassis(rw)->show lldp port remote-info ge.2.1

Local Port  : ge.2.1     Remote Port Id : ge.1.2
---------------------
Chassis ID  : 00-11-88-fe-52-8c

Enhanced Transmission Selection
Configuration
```

```
  Max Traffic Classes         : 8
  Willing                     : no
  Credit Base Shaper Supported: no
  Priority Assignment         : Pri[0]:   2 Pri[1]:   2 Pri[2]:   2 Pri[3]:   4
                              : Pri[4]:   4 Pri[5]:   5 Pri[6]:   6 Pri[7]:   7
  Traffic Class Bandwidth     : TC [0]:  0% TC [1]:  0% TC [2]: 30% TC [3]:  0%
                              : TC [4]: 70% TC [5]:  0% TC [6]:  0% TC [7]:  0%
  TSA Assignment              : TC [0]:   2 TC [1]:   2 TC [2]:   2 TC [3]:   2
                              : TC [4]:   2 TC [5]: 255 TC [6]: 255 TC [7]: 255
Priority Flow Control
  Willing                     : no
  MACsec Bypass Capability    : no
  Capability                  : 2
  Enable                      : Pri[0]:   0 Pri[1]:   0 Pri[2]:   0 Pri[3]:   0
                              : Pri[4]:   0 Pri[5]:   0 Pri[6]:   1 Pri[7]:   0
 Recommendation
  Priority Assignment         : Pri[0]:   2 Pri[1]:   2 Pri[2]:   2 Pri[3]:   4
                              : Pri[4]:   4 Pri[5]:   5 Pri[6]:   6 Pri[7]:   7
  Traffic Class Bandwidth     : TC [0]:  0% TC [1]:  0% TC [2]: 30% TC [3]:  0%
                              : TC [4]: 70% TC [5]:  0% TC [6]:  0% TC [7]:  0%
  TSA Assignment              : TC [0]:   2 TC [1]:   2 TC [2]:   2 TC [3]:   2
                              : TC [4]:   2 TC [5]: 255 TC [6]: 255 TC [7]: 255
PoE Device                    : PSE device (Type 1)
PoE Power Source              : primary
PoE MDI Supported/Enabled     : yes/yes
PoE Pair Controllable/Used    : no/signal
PoE Power Class               : 0
PoE Power Priority            : low
PoE PD Requested Power        : 154
PoE PSE Allocated Power       : 154
```

Note: Extended PoE info (PoE type, source, priority, and requested power) is sent only when the local device is actively supplying or drawing power.

Table 20-5 describes the information displayed by the **show lldp port local-info** command.

Table 20-5 show lldp port remote-info Output Details

Output...	What it displays...
Local Port	Identifies the port for which local system information is displayed.
Remote Port Id	Mandatory basic LLDP TLV that identifies the port transmitting the LLDPDU. Value is ifName object defined in RFC 2863.
Chassis ID	Identifies the chassis ID for the remote port.
Enhanced Transmission Selection Configuration	IEEE 802.1Qaz Enhanced Transmission Selection parameters provide a common management framework for assignment of bandwidth to 802.1p CoS-based traffic classes.

Table 20-5 show lldp port remote-info Output Details (continued)

Output...	What it displays...
Max Traffic Classes	Maximum number of supported Enhanced Transmission Selection Traffic Classes supported.
Willing	An Enhanced Transmission Selection or Priority Flow Control setting that indicates whether the station is willing to accept configurations from a remote station.
Credit Base Shaper Supported	Specifies whether the device supports the Credit-based Shaper Transmission Selection algorithm. Currently not supported on Extreme Networks devices.
Priority Assignment	Specifies the traffic class group to which the specified priority is assigned.
Traffic Class Bandwidth	Specifies the percent of bandwidth assigned to the traffic class.
TSA Assignment	Specifies the Transmission Selection Algorithm per priority: **0** = strict priority, **1** = Credit-based Shaper, **2** = Enhanced Transmission Selection, **255** = vendor specific.
MACsec Bypass Capability	Specifies whether the MACsec Bypass capability is supported or not.
Capability	Specifies the number of PFCs supported by the device.
Enable	Specifies whether the listed priority is enabled for Priority Flow Control. **0** = disabled, **1** = enabled.
Recommendation	A TLV encoded into each IEEE Standard 802.1AB LLDP message that indicates a recommendation on how Enhanced Transmission Selection should be configured.
Priority Assignment	Specifies the traffic class group to which the specified priority is assigned.
Traffic Class Bandwidth	Specifies the recommended percent of bandwidth per traffic class.
TSA Assignment	Specifies the recommended Transmission Selection Algorithm per priority: **0** = strict priority, **1** = Credit-based Shaper, **2** = Enhanced Transmission Selection, **255** = vendor specific.
PoE Device	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Value is the Power Type of the device. On a Extreme Networks switch port, the value is Power Sourcing Entity (PSE), type 1.
PoE Power Source	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Value can be primary or backup, indicating whether the PSE is using its primary or backup power source.
PoE MDI Supported/Enabled	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates whether sending the Power via MDI TLV is supported/enabled. Value can be yes or no.
PoE Pair Controllable/Used	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates whether pair selection can be controlled on the given port (refer to RFC 3621). Value for Controllable can be true or false. Value of Used can be signal (signal pairs only are in use) or spare (spare pairs only are in use).

Table 20-5 show lldp port remote-info Output Details (continued)

Output...	What it displays...
PoE Power Class	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates the power class supplied by the port. Value can range from 1 to 5.
PoE Power Priority	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates the power priority configured on the port. Value can be low, high, critical, or unknown.
PoE PD Requested Power (dW)	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates amount of power local PSE device has mirrored back to remote PD, in deciwatts. If the local device is a PD, indicates amount of power requested to remote PSE, in deciwatts.
PoE PSE Allocated Power (dW)	IEEE 802.3 Extensions Power via MDI TLV. Displayed only when a port has PoE capabilities. Indicates the maximum amount of power local PSE device has allocated for remote PD, in deciwatts. If the local device is a PD, indicates amount of power mirrored back to remote PSE, in deciwatts.

show lldp port network-policy

Use this command to display LLDP port network policy configuration information. Network policy information is configured using the set lldp port network-policy command.

Syntax

show lldp port network policy {**all** | **voice** | **voice-signaling** | **guest-voice** | **guest-voice-signaling** | **software-voice** | **video-conferencing** | **streaming-video** | **video-signaling**} [*port-string*]

Parameters

all	Displays information about all network policy applications.
voice	Displays information about only the voice application type.
voice-signaling	Displays information about only the voice signaling application type.
guest-voice	Displays information about only the guest voice application type.
guest-voice-signaling	Displays information about only the guest voice signaling application type.
software-voice	Displays information about only the softphone voice application type.
video-conferencing	Displays information about only the video conferencing application type.
streaming-video	Displays information about only the streaming video application type.
video-signaling	Displays information about only the video signaling application type.
port-string	(Optional) Displays information about LLDP network policy for one or a range of ports.

Defaults

If *port-string* is not specified, only non-default values will be displayed for all ports that have non-default values configured.

If a *port-string* is specified, then all values, default and non-default, are displayed for the specified ports.

Mode

All command modes.

Example

This example shows how to display all LLDP network policy information for **ge.1.1**.

```
S Chassis(rw)->show lldp port network-policy all ge.1.1

Ports    Application            State     Tag       Vlan-Id   Cos   Dscp
-------  ---------------------  --------  --------  -------   ---   ---
ge.1.1   voice                  enabled   untagged  10        7      44
         voice signaling        enabled   untagged  10        7      44
         guest voice            enabled   untagged  10        7      44
```

set lldp tx-interval

Use this command to set the time, in seconds, between successive LLDP frame transmissions initiated by changes in the LLDP local system information.

Syntax

set lldp tx-interval *frequency*

Parameters

frequency	Specifies the number of seconds between transmissions of LLDP frames. Value can range from **5** to **32,768** seconds. The default is **30** seconds.

Defaults

None.

Mode

All command modes.

Example

This example sets the transmit interval to **20** seconds.

```
S Chassis(rw)->set lldp tx-interval 20
```

set lldp tx-fast-count

Use this command to set the number of LLDP PDU packets sent when entering fast transmission state.

Syntax

set lldp tx-fast-count *count*

Parameters

count	Specifies the number of LLDP PDU transmissions when entering fast transmission state. Value can range from **1** to **8** transmissions. The default is **4** packets.

Defaults

None.

Mode

All command modes.

Usage

LLDP PDU packets are sent once every 30 seconds by default. When a new neighbor is discovered, LLDP enters fast transmission state, and it is desirable for packets to be sent more frequently. In fast transmission state, an LLDP PDU packet will be sent each fast transmission state interval for the number of intervals specified by *count*. The fast transmission state interval is set using the "set lldp tx-fast-interval" on page 20-34 command.

Example

This example sets the number of LLDP PDU transmissions when entering fast transmission state to **4**.

```
S Chassis(rw)->set lldp tx-fast-count 4
```

set lldp tx-fast-interval

Use this command to set the frequency of LLDP PDU transmissions while in fast transmission state.

Syntax

set lldp tx-fast-interval *frequency*

Parameters

frequency	Specifies the number of seconds between LLDP PDU transmissions when in fast transmission state. Value can range from **1** to **3600** seconds. The default is **1** second.

Defaults

None.

Mode

All command modes.

Usage

LLDP PDU packets are sent once every 30 seconds by default. When a new neighbor is discovered, it is desirable for packets to be sent more frequently. LLDP enters fast transmission state. This command specifies the length of the fast transmission state interval. In fast transmission state, an LLDP PDU packet will be sent each fast transmission state interval for the number of intervals

specified by the fast transmission state count. The fast transmission state count is set using the "set lldp tx-fast-count" on page 20-33 command.

Example

This example sets the number of seconds between LLDP PDU packets when in fast transmission state to **4**.

```
S Chassis(rw)->set lldp tx-fast-interval 4
```

set lldp hold-multiplier

Use this command to set the time-to-live value used in LLDP frames sent by this device.

Syntax

set lldp hold-multiplier *multiplier-val*

Parameters

multiplier-val	Specifies the multiplier to apply to the transmit interval to determine the time-to-live value. Value can range from **2** to **10**. Default value is **4**.

Defaults

None.

Mode

All command modes.

Usage

The time-to-live for LLDP PDU data is calculated by multiplying the transmit interval by the hold multiplier value.

Example

This example sets the transmit interval to **20** seconds and the hold multiplier to **5**, which will configure a time-to-live of 100 to be used in the TTL field in the LLDP PDU header.

```
S Chassis(rw)->set lldp tx-interval 20
S Chassis(rw)->set lldp hold-multiplier 5
```

set lldp trap-interval

Use this command to set the minimum interval between LLDP notifications sent by this device. LLDP notifications are sent when a remote system change has been detected.

Syntax

set lldp trap-interval *frequency*

Parameters

frequency	Specifies the minimum time between LLDP trap transmissions, in seconds. The value can range from 5 to 3600 seconds. The default value is 5 seconds.

Defaults

None.

Mode

All command modes.

Example

This example sets the minimum interval between LLDP traps to **10** seconds.

```
S Chassis(rw)->set lldp trap-interval 10
```

set lldp med-fast-repeat

Network connectivity devices transmit only LLDP TLVs in LLDP PDUs until they detect that an LLDP-MED endpoint device has connected to a port.

Syntax

set lldp med-fast-repeat *count*

Parameters

count	Specifies the number of fast start LLDPDUs to be sent when an LLDP-MED endpoint device, such as a phone, is detected. Value can range from 1 to 10. Default is 3.

Defaults

None.

Mode

All command modes.

Usage

When an LLDP-MED endpoint device, such as a phone, has connected to a port, the network connectivity device starts sending LLDP-MED TLVs at a fast start rate on that port. Use this command to set the number of successive LLDPDUs (with LLDP-MED TLVs) to be sent for one complete fast start interval.

Example

This example sets the number of fast start LLDPDUs to be sent to **4**.

```
S Chassis(rw)->set lldp med-fast-repeat 4
```

set lldp port status

Use this command to enable or disable transmitting and processing received LLDPDUs on a port or range of ports.

Syntax

set lldp port status {**tx-enable** | **rx-enable** | **both** | **disable**} *port-string*

Parameters

tx-enable	Enables transmitting LLDPDUs on the specified ports.
rx-enable	Enables receiving and processing LLDPDUs from remote systems on the specified ports.
both	Enables both transmitting and processing received LLDPDUs on the specified ports.
disable	Disables both transmitting and processing received LLDPDUs on the specified ports.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

All command modes.

Example

This example enables both transmitting LLDPDUs and receiving and processing LLDPDUs from remote systems on ports **ge.1.1** through **ge.1.6**.

```
S Chassis(rw)->set lldp port status both ge.1.1-6
```

set lldp port trap

Use this command to enable or disable sending LLDP notifications (traps) when a remote system change is detected.

Syntax

set lldp port trap {**enable** | **disable**} *port-string*

Parameters

enable	Enables transmitting LLDP traps on the specified ports.
disable	Disables transmitting LLDP traps on the specified ports.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

All command modes.

Example

This example enables transmitting LLDP traps on ports **ge.1.1** through **ge.1.6**.

```
S Chassis(rw)->set lldp port trap enable ge.1.1-6
```

set lldp port med-trap

Use this command to enable or disable sending an LLDP-MED notification when a change in the topology has been sensed on the port (that is, a remote endpoint device has been attached or removed from the port).

Syntax

set lldp port med-trap {**enable** | **disable**} *port-string*

Parameters

enable	Enable transmitting LLDP-MED traps on the specified ports.
disable	Disable transmitting LLDP-MED traps on the specified ports.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

All command modes.

Example

This example enables transmitting LLDP-MED traps on ports **ge.1.1** through **ge.1.6**.

```
S Chassis(rw)->set lldp port med-trap enable ge.1.1-6
```

set lldp port location-info

Use this command to configure LLDP-MED location information on a port or range of ports. Currently, only Emergency Call Services (ECS) Emergency Location Identification Number (ELIN) is supported.

Syntax

set lldp port location-info elin *value port-string*

Parameters

elin	Specifies that the ECS ELIN data format is to be used.
value	Specifies the location identifier. Value can be from 10 to 25 numerical characters.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

All command modes.

Usage

The Emergency Location Identification Number (ELIN) is a valid North America Numbering Plan format telephone number, supplied to the Public Safety Answering Point (PSAP) for Emergency Call System (ECS) purposes.

After you configure a location information value, you must also configure the port to send the Location Information TLV with the set lldp port tx-tlv command.

Example

This example configures the ELIN identifier **5551234567** on ports **ge.1.1** through **ge.1.6** and then configures the ports to send the Location Information TLV.

```
S Chassis(rw)->set lldp port location-info 5551234567 ge.1.1-6
S Chassis(rw)->set lldp port tx-tlv med-loc ge.1.1-6
```

set lldp port tx-tlv

Use this command to select the optional LLDP, LLDP-MED, and LLDP-DCBX TLVs to be transmitted in LLDPDUs by the specified port or ports. Use the show lldp port local-info command to display the values of these TLVs for the port.

Syntax

set lldp port tx-tlv {[**all**] | [**port-desc**] [**sys-name**] [**sys-desc**] [**sys-cap**] [**mgmt-addr**] [**vlan-id**] [**stp**] [**lacp**] [**gvrp**] [**mac-phy**] [**poe**] [**link-aggr**] [**max-frame**] [**med-cap**] [**med-pol**] [**med-loc**] [**med-poe**] [**enhanced-trans-config**] [**enhanced-trans-rec**] [**priority-flowctrl**] [**application-pri**] [**congestion-notif**] [**energy-eff-eth**]} *port-string*

Parameters

all	Add all optional TLVs to transmitted LLDPDUs.
port-desc	Port Description optional basic LLDP TLV. Value sent is ifDescr object defined in RFC 2863.
sys-name	System Name optional basic LLDP TLV. Value sent is the administratively assigned name for the system.
sys-desc	System Description optional basic LLDP TLV. Value sent is sysDescr object defined in RFC 3418.
sys-cap	System Capabilities optional basic LLDP TLV. For a network connectivity device, value sent can be bridge and/or router.
mgmt-addr	Management Address optional basic LLDP TLV. Value sent is IPv4 or IPv6 address of host interface.
vlan-id	Port VLAN ID IEEE 802.1 Extensions TLV. Value sent is port VLAN ID (PVID).

stp	Spanning Tree information defined by Protocol Identity IEEE 802.1 Extensions TLV. If STP is enabled on the port, value sent includes version of protocol being used.
lacp	LACP information defined by Protocol Identity IEEE 802.1 Extensions TLV. If LACP is enabled on the port, value sent includes version of protocol being used.
gvrp	GVRP information defined by Protocol Identity IEEE 802.1 Extensions TLV. If LACP is enabled on the port, value sent includes version of protocol being used.
mac-phy	MAC-PHY Configuration/Status IEEE 802.3 Extensions TLV. Value sent includes the operational MAU type, duplex, and speed of the port.
poe	Power via MDI IEEE 802.3 Extensions TLV. Values sent include whether pair selection can be controlled on port, and the power class supplied by the port. Only valid for PoE-enabled ports.
link-aggr	Link Aggregation IEEE 802.3 Extensions TLV. Values sent indicate whether the link associated with this port can be aggregated, whether it is currently aggregated, and if aggregated, the aggregated port identifier.
max-frame	Maximum Frame Size IEEE 802.3 Extensions TLV. Value sent indicates maximum frame size of the port's MAC and PHY.
med-cap	LLDP-MED Capabilities TLV.Value sent indicates the capabilities (whether the device supports location information, network policy, extended power via MDI) and Device Type (network connectivity device) of the sending device.
med-pol	LLDP-MED Network Policy TLV. Values sent include application name, VLAN type (tagged or untagged), VLAN ID, and both Layer 2 and Layer 3 priorities associated with application, for all applications enabled on the port. See the set lldp port network-policy command for more information.
med-loc	LLDP-MED Location Identification TLV. Value sent is the ECS ELIN value configured on the port. See the set lldp port location-info command for more information.
med-poe	LLDP-MED Extended Power via MDI TLV. Values sent include the Power Limit (total power the port is capable of sourcing over a maximum length cable) and the power priority configured on the port. Only valid for PoE-enabled ports.
enhanced-trans-config	Enhanced Transmission Selection Configuration TLV. This TLV specifies how Enhanced Transmission Selection is configured for a given port. Enhanced Transmission Selection is discussed in the Data Center Bridging chapter of the *Extreme Networks S-Series Configuration Guide*.
enhanced-trans-rec	Enhanced Transmission Selection Recommendation TLV. This TLV provides a recommendation to the peer as to how Enhanced Transmission Selection should be configured. The TLV contains fields for the traffic class group to which the priority is assigned, an entry containing the percent of bandwidth for each traffic class, and an entry per priority (0 - 7) specifying the priority transmission selection algorithm. Selection algorithms are strict priority, credit-based shaper, Enhanced Transmission Selection, or vendor specific.

priority-flowctrl	Specifies that priority flow control will be advertised on this port. Priority flow control is discussed in the Data Center Bridging chapter of the *Extreme Networks S-Series Configuration Guide*.
application-pri	Specifies that application priority will be advertised on this port. Application priority is discussed in the Data Center Bridging chapter of the *Extreme Networks S-Series Configuration Guide*.
congestion-notif	Specifies that congestion notification will be advertised on this port. Congestion notification is discussed in the Data Center Bridging chapter of the *Extreme Networks S-Series Configuration Guide*.
energy-eff-eth	Specifies Energy Efficient Ethernet (EEE) will be advertised on this port. EEE is discussed in the Port Configuration chapter of the *Extreme Networks S-Series Configuration Guide*.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

All command modes.

Example

This example configures the management address, MED capability, MED network policy, and MED location identification TLVs to be sent in LLDPDUs by port **ge.1.1**.

```
S Chassis(rw)->set lldp port tx-tlv mgmt-addr med-cap med-pol med-loc ge.1.1
```

set lldp port network-policy

Use this command to configure network policy for a set of applications on a port or range of ports.

Syntax

```
set lldp port network-policy {all | voice | voice-signaling | guest-voice |
guest-voice-signaling | softphone-voice | video-conferencing | streaming-video |
video-signaling} [state {enable | disable}] [tag {tagged | untagged}]
[vid {vlan-id | dot1p}] [cos cos-value] [dscp dscp-value] port-string
```

Parameters

all	Configures all applications.
voice	Configures the voice application.
voice-signaling	Configures the voice signaling application. This application will not be advertised if the **voice** application is configured with the same parameters.
guest-voice	Configures the guest voice application.
guest-voice-signaling	Configures the guest voice signaling application. This application will not be advertised if the **guest-voice** application is configured with the same parameters.
softphone-voice	Configures the softphone voice application.

video-conferencing	Configures the video conferencing application.
streaming-video	Configures the streaming video application.
video-signaling	Configures the video signaling application. This application will not be advertised if the **video-conferencing** application is configured with the same parameters.
state enable | **disable**	(Optional) Enables or disables advertising the application information being configured.
tag tagged | **untagged**	(Optional) Indicates whether the application being configured is using a tagged or untagged VLAN. If untagged, both the VLAN ID and the CoS priority fields are ignored and only the DSCP value has relevance.
vid *vlan-id* | **dot1p**	(Optional) VLAN identifier for the port. The value of *vlan-id* can range from 1 to 4094. Use **dot1p** if the device is using priority tagged frames, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used.
cos *cos-value*	(Optional) Specifies the Layer 2 priority to be used for the application being configured. The value can range from 0 to 7. A value of 0 represents use of the default priority as defined in IEEE 802.1D.
dscp *dscp-value*	(Optional) Specifies the DSCP value to be used to provide Diffserv node behavior for the application being configured. The value can range from 0 to 63. A value of 0 represents use of the default DSCP value as defined in RFC 2475.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

All command modes.

Usage

As described in the ANSI/TIA Standards document 1057, the Network Policy TLV is "intended for use with applications that have specific real-time network policy requirements, such as interactive voice and/or video services" and should be implemented only on direct links between network connectivity devices and endpoint devices. Refer to the ANSI/TIA Standards document 1057 for descriptions of the application types.

After you configure Network Policy TLVs, you must also configure the port to send the Network Policy TLV with the set lldp port tx-tlv command.

The policies configured with this command are sent in LLDPDUs as LLDP-MED Network Policy TLVs. Multiple Network Policy TLVs can be sent in a single LLDPDU.

Example

This example configures the voice application TLV on port **ge.2.1** and then configures the port to send the Network Policy TLV.

```
S Chassis(rw)->set lldp port network-policy voice state enable tag tagged vlan
dot1p ge.2.1
S Chassis(rw)->set lldp port tx-tlv med-pol ge.2.1
```

clear lldp

Use this command to return LLDP parameters to their default values.

Syntax

clear lldp {**all** | **tx-interval** | **hold-multiplier** | **trap-interval** | **med-fast-repeat**}

Parameters

all	Returns **all** LLDP configuration parameters to their default values, including port LLDP configuration parameters.
tx-interval	Returns the number of seconds between transmissions of LLDP frames to the default of 30 seconds.
hold-multiplier	Returns the multiplier to apply to the transmit interval to determine the time-to-live value to the default value of 4.
trap-interval	Returns the minimum time between LLSP trap transmissions to the default value of 5 seconds.
med-fast-repeat	Returns the number of fast start LLDPDUs to be sent when an LLDP-MED endpoint device is detected to the default of 3.

Defaults

None.

Mode

All command modes.

Examples

This example returns the transmit interval to the default value of **30** seconds.

```
S Chassis(rw)->clear lldp tx-interval
```

clear lldp port status

Use this command to return the port status to the default value of both (both transmitting and processing received LLDPDUs are enabled).

Syntax

clear lldp port status *port-string*

Parameters

port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

All command modes.

Example

This example returns port ge.1.1 to the default state of enabled for both transmitting and processing received LLDPDUs.

```
S Chassis(rw)->clear lldp port status ge.1.1
```

clear lldp port trap

Use this command to return the port LLDP trap setting to the default value of disabled.

Syntax

clear lldp port trap *port-string*

Parameters

port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

All command modes.

Example

This example returns port **ge.1.1** to the default LLDP trap state of disabled.

```
S Chassis(rw)->clear lldp port trap ge.1.1
```

clear lldp port med-trap

Use this command to return the port LLDP-MED trap setting to the default value of disabled.

Syntax

clear lldp port med-trap *port-string*

Parameters

port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

All command modes.

Example

This example returns port ge.1.1 to the default LLDP-MED trap state of disabled.

```
S Chassis(rw)->clear lldp port med-trap ge.1.1
```

clear lldp port location-info

Use this command to return the port ECS ELIN location setting to the default value of null.

Syntax

clear lldp port location-info elin *port-string*

Parameters

elin	Specifies that the ECS ELIN location information value should be cleared.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

All command modes.

Example

This example returns the location information ELIN value on port **ge.1.1** to the default value of null.

```
S Chassis(rw)->clear lldp port location-info elin ge.1.1
```

clear lldp port network-policy

Use this command to return network policy for a set of applications on a port or range of ports to default values.

Syntax

clear lldp port network-policy {**all** | **voice** | **voice-signaling** | **guest-voice** | **guest-voice-signaling** | **softphone-voice** | **video-conferencing** | **streaming-video** | **video-signaling**} {[**state**] [**tag**] [**vid**] [**cos**] [**dscp**]} *port-string*

Parameters

all	Command will be applied to all applications.
voice	Command will be applied to the voice application.
voice-signaling	Command will be applied to the voice signaling application.
guest-voice	Command will be applied to the guest voice application.
guest-voice-signaling	Command will be applied to the guest voice signaling application.
softphone-voice	Command will be applied to the softphone voice application.
video-conferencing	Command will be applied to the video conferencing application.
streaming-video	Command will be applied to the streaming video application.
video-signaling	Command will be applied to the video signaling application.
state	(Optional) Clear the state of advertising the application information being configured to disabled.

tag	(Optional) Clear the tag value of the application being configured to untagged.
vid	(Optional) Clear the VLAN identifier for the port to the default value of 1.
cos	(Optional) Clear the Layer 2 priority to be used for the application being configured to the default value of 0. (A value of 0 represents use of the default priority as defined in IEEE 802.1D.)
dscp	(Optional) Clear the DSCP value to be used to provide Diffserv node behavior for the application being configured to the default value of 0. (A value of 0 represents use of the default DSCP value as defined in RFC 2475.)
port-string	Specifies the port or range of ports to be affected.

Defaults

At least one application (or **all**) and one policy parameter must be specified.

Mode

All command modes.

Example

This example returns all network policy values for all applications on port **ge.1.1** to their default values.

```
S Chassis(rw)->clear lldp port network-policy all state tag vid cos dscp ge.1.1
```

clear lldp port tx-tlv

Use this command to clear the optional LLDP and LLDP-MED TLVs to be transmitted in LLDPDUs by the specified port or ports to the default value of disabled.

Syntax

clear lldp port tx-tlv {[**all**] | [**port-desc**] [**sys-name**] [**sys-desc**] [**sys-cap**] [**mgmt-addr**] [**vlan-id**] [**stp**] [**lacp**] [**gvrp**] [**mac-phy**] [**poe**] [**link-aggr**] [**max-frame**] [**med-cap**] [**med-pol**] [**med-loc**] [**med-poe**] [**enhanced-trans-config**] [**enhanced-trans-rec**] [**priority-flowctrl**] [**application-pri**] [**congestion-notif**]} *port-string*

Parameters

all	Disables all optional TLVs from being transmitted in LLDPDUs.
port-desc	Disables the Port Description optional basic LLDP TLV from being transmitted in LLDPDUs.
sys-name	Disables the System Name optional basic LLDP TLV from being transmitted in LLDPDUs.
sys-desc	Disables the System Description optional basic LLDP TLV from being transmitted in LLDPDUs.
sys-cap	Disables the System Capabilities optional basic LLDP TLV from being transmitted in LLDPDUs.

mgmt-addr	Disables the Management Address optional basic LLDP TLV from being transmitted in LLDPDUs.
vlan-id	Disables the Port VLAN ID IEEE 802.1 Extensions TLV from being transmitted in LLDPDUs.
stp	Disables the Spanning Tree information defined by Protocol Identity IEEE 802.1 Extensions TLV from being transmitted in LLDPDUs.
lacp	Disables the LACP information defined by Protocol Identity IEEE 802.1 Extensions TLV from being transmitted in LLDPDUs.
gvrp	Disables the GVRP information defined by Protocol Identity IEEE 802.1 Extensions TLV from being transmitted in LLDPDUs.
mac-phy	Disables the MAC-PHY Configuration/Status IEEE 802.3 Extensions TLV from being transmitted in LLDPDUs.
poe	Disables the Power via MDI IEEE 802.3 Extensions TLV from being transmitted in LLDPDUs. Only valid for PoE-enabled ports.
link-aggr	Disables the Link Aggregation IEEE 802.3 Extensions TLV from being transmitted in LLDPDUs.
max-frame	Disables the Maximum Frame Size IEEE 802.3 Extensions TLV from being transmitted in LLDPDUs.
med-cap	Disables the LLDP-MED Capabilities TLV from being transmitted in LLDPDUs.
med-pol	Disables the LLDP-MED Network Policy TLV from being transmitted in LLDPDUs.
med-loc	Disables the LLDP-MED Location Identification TLV from being transmitted in LLDPDUs.
med-poe	Disables the LLDP-MED Extended Power via MDI TLV from being transmitted in LLDPDUs. Only valid for PoE-enabled ports.
enhanced-trans-config	Disables Enhanced Transmission Selection Configuration TLV on the specified port.
enhanced-trans-rec	Disables Enhanced Transmission Selection Recommendation TLV on the specified port.
priority-flowctrl	Disables the advertisement of priority flow control on the specified port.
application-pri	Disables the advertisement of application priority on the specified port.
congestion-notif	Disables the advertisement of congestion notification on the specified port.
port-string	Specifies the port or range of ports to be affected.

Defaults

None.

Mode

All command modes.

Example

This example disables the management address, MED capability, MED network policy, and MED location identification TLVs from being sent in LLDPDUs by port **ge.1.1**.

```
S Chassis(rw)->clear lldp port tx-tlv mgmt-addr med-cap med-pol med-loc ge.1.1
```

21

Data Center Bridging Commands

This chapter provides detailed information for the Data Center Bridging (DCB) set of commands. For information about configuring DCB, refer to the "Data Center Bridging Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
Application Priority	21-1
Congestion Notification	21-4

Application Priority

This section details Application Priority commands. Application Priority advertises to the link peer a preferred priority for frames carrying application-specific traffic.

For information about...	Refer to page...
show dcb appPri	21-1
set dcb appPri	21-2
clear dcb appPri	21-3

show dcb appPri

Use this command to display Application Priority table entries by port.

Syntax

show dcb appPri [*port-string*]

Parameters

port-string	(Optional) Specifies the port string for the Application Priority settings to display. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, Application Priority settings for all ports are displayed.

Mode

All command modes.

Examples

This example shows how to display Application Priority settings for port **tg.1.1**:

```
S Chassis(rw)->show dcb appPri tg.1.1

Port          Protocol  Protocol ID Priority
------------  --------- ----------- --------
tg.1.1        ethertype        1900        4
tg.1.1        tcp              3260        5
tg.1.1        tcp/udp          5600        1
S Chassis(rw)->
```

set dcb appPri

Use this command to set the priority to be advertised to the link peer of the specified port for the specified application.

Syntax

set dcb appPri *port-string* **protocol** {**ethertype** | **tcp** | **udp** | **l4port**} **protocol-id** *protocol-id* **priority** *priority*

Parameters

port-string	Specifies the port to apply the Application Priority setting to.
protocol ethertype | **tcp** | **udp** | **l4port**	Specifies the protocol to associate with the advertised priority: • **ethertype** – Specifies that the protocol is the one encapsulated in the payload of an Ethernet frame • **tcp** – Specifies the protocol is a well known TCP port • **udp** – Specifies the protocol is a well known UDP port • **l4port** – Specifies the protocol is a well known Layer 4 (TCP and UDP) port
protocol-id *protocol-id*	Specifies the ID of the protocol to be advertised. Valid values are from **0** - **65535** depending upon the protocol specified.
priority *priority*	Specifies the priority to be advertised with the specified protocol.

Defaults

None.

Mode

All command modes.

Usage

Application priority advertises to the peer a preferred priority for frames carrying application-specific traffic. Application priority does not perform any priority tagging on the

source device. The source device's link peer that receives the Application Priority TLV tags its traffic to the advertised priority. Application priority works along with Enhanced Transmission Selection (ETS) and Priority-based Flow Control (PFC) in that tagged protocol-specific traffic for the specified priority enforces ETS and PFC settings on that traffic.

Note: The application priority feature requires that the peer supports the LLDP willing bit and the willing bit is enabled. Extreme Networks switches do not currently support the LLDP willing bit.

Use the **set lldp port tx-tlv application-pri** command to enable the sending of an Application Priority TLV on the port using the LLDP-DCB Application Priority TLV.

Examples

This example shows how to advertise priority 4 for the UDP service type dpkeyserv on port 1780 on port ge.1.2 and to enable the sending of LLDP-DCB Application Priority TLVs from that port:

```
S Chassis(rw)->set dcb appPri ge.1.2 protocol udp protocol-id 1780 priority 4
S Chassis(rw)->set lldp port tx-tlv application-pri ge.1.2
```

clear dcb appPri

Use this command to remove an Application Priority entry for the specified protocol and ID.

Syntax

set dcb appPri *port-string* **protocol** {**ethertype** | **tcp** | **udp** | **l4port**} **protocol-id** *protocol-id*

Parameters

port-string	Specifies the port to clear the Application Priority setting for.
protocol ethertype | **tcp** | **udp** | **l4port**	Specifies the protocol of the Application Priority to clear: • **ethertype** – Specifies that the protocol to clear is the one encapsulated in the payload of an Ethernet frame • **tcp** – Specifies the protocol to clear is a well known TCP port • **udp** – Specifies the protocol to clear is a well known UDP port • **l4port** – Specifies the protocol to clear is a well known Layer 4 (TCP and UDP) port
protocol-id *protocol-id*	Specifies the ID of the protocol to be cleared. Valid values are from **0** - **65535** depending upon the protocol specified.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to clear the Application Priority entry for the UDP service type dpkeyserv on port 1780:

```
S Chassis(rw)->clear dcb appPri tg.1.1 protocol udp protocol-id 1780
```

Congestion Notification

This section describes commands for the configuring Congestion Notification (CN).

For information about...	Refer to page...
show dcb cn global	21-4
set dcb cn global	21-5
show dcb cn priority	21-6
set dcb cn priority	21-8
set dcb cn priority status	21-9
set dcb cn priority choice	21-10
set dcb cn priority alt-priority	21-11
set dcb cn priority defense	21-12
set dcb cn priority lldp	21-14
clear dcb cn priority	21-15
clear dcb cn port-priority	21-16
show dcb cn port-priority	21-16
set dcb cn port-priority choice	21-19
set dcb cn port-priority alt-pri	21-20
set dcb cn port-priority defense	21-21
set dcb cn port-priority lldp	21-22
show dcb cn congestion-point	21-23
set dcb cn congestion-point	21-25
clear dcb cn congestion-point	21-27
show dcb cn q-profile	21-29
set dcb cn q-profile	21-30
clear dcb cn q-profile	21-31
show dcb cn errored-ports	21-32

show dcb cn global

Use this command to display the global status of congestion notification on the switch.

Syntax

```
show dcb cn global
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Examples

This example displays the global status of congestion notification on the switch:

```
S Chassis(rw)->show dcb cn global

CN Global Entry
-------------------------------------------------------
Status                     : Enabled
CNM Tx Priority            : 7
Discarded Frames           : 0
Active Priority Values     : 2
Maximum Active Priorities : 2
```

Table 21-1 provides an explanation of the command output.

Table 21-1 show dcb cn global Output Details

Output...	What it displays...
Status	Specifies whether congestion notification is globally enabled or disabled for this device.
CNM Tx Priority	The priority value to be used when transmitting a CNM PDU from this bridge or end station back to the reaction point. The default value is 7.
Discarded Frames	The number of frames discarded from full congestion point queues.
Active Priority Values	Specifies the number of configured and active Congestion Notification Priority Values (CNPV) on the switch.
Maximum Active Priorities	Specifies the maximum number of CNPVs supported on the switch.

set dcb cn global

Use this command to enable or disable congestion notification or set the transmit priority for Congestion Notification Message (CNM) PDUs on the switch.

Syntax

set dcb cn global {**enable** | **disable** | **tx-priority** *tx-priority*}

Parameters

enable | **disable**	Enable or disable congestion notification on the switch. The default value is **enabled**.
tx-priority *tx-priority*	Sets the priority for congestion notification message (CNM) PDUs sent from the congestion point back to the congestion notification reaction point. The default value is **7**.

Defaults

- Congestion Notification is globally enabled by default.

- The transmit priority for CNM PDUs defaults to 7.

Mode

All command modes.

Examples

This example globally disables congestion notification on the switch:

```
S Chassis(rw)->set dcb cn global disable
```

This example sets the priority for the CNM PDUs sent from the congestion point back to the reaction point to **6** on the switch:

```
S Chassis(rw)->set dcb cn global tx-priority 6
```

show dcb cn priority

Use this command to display the configuration and status of congestion notification priority values on the switch.

Syntax

```
show dcb cn priority [priority] [-interesting]
```

Parameters

priority	(Optional) Specifies the congestion notification priority value to display.
-interesting	(Optional) Specifies that only port-priority objects with a non-default defense mode will be displayed for the specified priority.

Defaults

If no option is specified, information for all congestion notification priority values is displayed.

Mode

All command modes.

Examples

This example displays configuration and status of all congestion notification priority values on the switch:

```
S Chassis(rw)->show dcb cn priority

* Alt - Admin Alternate Priority
* Aut - Auto Alternate Priority

Pri  Choice  Alt  Aut  Admin Defense  Creation     LLDP      Status
---  ------  ---  ---  -------------  -----------  --------  --------
 3   Auto     0    2   Interior       AutoEnable   Enabled   Inactive
 4   Admin    2    3   Edge           AutoEnable   Enabled   Active
 5   Auto     0    3   Interior       AutoDisable  Disabled  Active
```

This example displays configuration and status information for congestion notification priority value 4:

```
S Chassis(rw)->show dcb cn priority 4

CNPV 4 Information
---------------------------------------
Defense Mode Choice      : Admin
Admin Alternate Priority : 2
Auto Alternate Priority  : 3
Admin Defense Mode       : Edge
Creation                 : AutoEnable
LLDP Choice              : Enabled
LLDP Instance Selector   : 1
Row Status               : active
```

Table 21-2 provides an explanation of the command output.

Table 21-2 show dcb cn priority Output Details

Output...	What it displays...
Pri	Specifies a configured CNPV.
Choice	Specifies the default choice mode being used for the priority row. Valid values are Auto or Admin. If the default mode choice is Admin, the admin configured alternate priority and admin defense mode are used by the port-priority entries by default. If the default mode choice is Auto, the auto alternate priority is used and the defense mode is selected by the port.
Alt	The admin alternate priority value for this CNPV.
Aut	The auto alternate priority value for this CNPV.

Table 21-2 show dcb cn priority Output Details

Output...	What it displays...
Admin Defense	The defense mode used to protect the CNPV queue from receiving non-congestion controlled flows and determines if a CN-TAG should be removed or not. Congestion Notification defense can use LLDP to dynamically control the states. These states are defined per priority and per port: • **Disabled** – The congestion notification capability is administratively disabled for this priority value and port. This priority is not a CNPV. The priority regeneration table controls the remapping of input frames on this port for this priority. CN-TAGs are neither added by an end station nor removed by a bridge. • **Edge** – On this port and for this CNPV, the input frame priority parameters are remapped to an alternate (non-CNPV) value, regardless of the priority regeneration table settings. CN-TAGs are not added by an end station, and are removed from frames before being output by a bridge. This mode is optional for an end station. • **Interior** – On this port and for this CNPV, the input frame priority parameters are not remapped, regardless of the priority regeneration table settings. CN-TAGs are not added by an end station, and are removed from frames before being output by a bridge. This is a transition state due to the fact that the port is not yet aware of the congestion notification status of its neighbor. • **InteriorReady** - On this port and for this CNPV, the input frame priority parameters are not remapped, regardless of the priority regeneration table settings. CN-TAGs can be added by an end station, and are not removed from frames being output by a bridge. This port has successfully negotiated congestion notification with its neighbor.
Creation	Specifies the default value for priority defense mode choice for a newly created port-priority table entry. If set to AutoEnable, the congestion notification domain defense and alternate priority are both controlled by the values in the port-priority table. If set to AutoDisable, the congestion notification domain defense and alternate priority are controlled by administrative values in the same table entry as this object.
LLDP	Specifies whether LLDP instance selection is enabled or disabled.
Status	Specifies whether this priority is currently active.

set dcb cn priority

Use this command to configure an 802.1p priority as a congestion notification priority value and to optionally enable or disable auto choice mode for all ports on the switch.

Note: All **set dcb cn priority** based command options can be entered on a single command line. Command options include: creation, status, choice, alt-priority, defense, and lldp. Each option is detailed in this chapter with its own entry for purposes of clarity.

Syntax

set dcb cn priority *priority* [**creation** {**enable** | **disable**}]

Parameters

priority	Specifies a CNPV to apply the specified creation state on this switch.
creation enable	(Optional) Specifies the port-priority choice for this CNPV will be set to **default**. Default uses the default choice which is **auto**. The default domain defense mode for a port-priority is **edge** when the choice is **auto**.
creation disable	(Optional) Specifies the port-priority choice for this CNPV will be set to **admin**. The default domain defense mode for a port-priority is **interior** when the choice is **admin**.

Defaults

If **creation enable** or **disable** is not specified, the created CNPV defaults to **creation enable**. The priority defaults to **6**.

Mode

All command modes.

Usage

There are eight 802.1p values from 0 - 7. The maximum number of CNPVs configurable on a port depends upon the chassis. The SSA, S3, and S4 chassis support a maximum of seven CNPVs. The S6 and S10 chassis support a maximum of four CNPVs. There must always be at least one alternate (non-CNPV) priority value per port. By default, a CNPV is created with auto creation enabled.

This command does not activate the CNPV. Use "set dcb cn priority status" on page 21-9 to activate a CNPV on the switch.

Note: CNPVs do not exist on S-Series hardware bonding ports.

Examples

This example creates CNPV **3** on all ports for this switch, setting the priority choice to **auto**, the alternate priority to **0**, and the domain defense default to **edge**:

```
S Chassis(rw)->set dcb cn priority 3
```

This example creates CNPV **4** on all ports for this switch, setting the priority choice to **admin** the alternate priority to **0** and the domain defense default to **interior**:

```
S Chassis(rw)->set dcb cn priority 4 creation disable
```

set dcb cn priority status

Use this command to enable or disable the activation of the specified CNPV for all ports on the switch.

Syntax

set dcb cn priority *priority* **status** {**enable** | **disable**}

Parameters

priority	Specifies a CNPV to apply the specified activation state to on this switch.
enable | **disable**	Specifies whether a configured CNPV is activated or not activated: • **enable** – The CNPV is activated • **disable** – The CNPV is not activated

Defaults

The default CNPV status is activated.

Mode

All command modes.

Usage

Congestion notification only takes place for activated CNPVs. The priority status is enabled by default when creating a CNPV using any options supported by the **set dcb cn priority** command. Use this command to either disable or re-enable CNPV activation status.

Examples

This example deactivates CNPV **3** on all ports for this switch:

```
S Chassis(rw)->set dcb cn priority 3 status disable
```

set dcb cn priority choice

Use this command to configure a default method for selecting domain defense on all device ports for the specified congestion notification priority value.

Syntax

set dcb cn priority *priority* **choice** {**admin** | **auto**}

Parameters

priority	Specifies the CNPV to which the specified congestion notification mode will be applied.
choice admin | **auto**	Configures the priority choice used by a port-priority when port-priority choice is set to **default**: • **admin** – Domain defense is controlled by administratively configured values and defense mode defaults to **interior** on all ports. • **auto** – Domain defense is automatically controlled by the port based upon neighbor information advertises by LLDP in the congestion notification TLV type 127. The global default setting for priority choice is **auto**.

Defaults

Priority choice defaults to **auto**. This is the global default setting.

Mode

All command modes.

Usage

If priority choice is set to auto, the domain defense mode defaults to **edge**. The defense mode will transition to **interior-ready** if congestion notification negotiation using TLV type 127 determines that the CNPV is activated on the neighbor. If priority choice is set to admin, the domain defense mode defaults to disabled. In this case no congestion notification will occur unless the domain defense is administratively changed.

Examples

This example sets the priority choice to **admin** for CNPV **3** for all ports on the device:

```
S Chassis(rw)->set dcb cn priority 3 choice admin
```

set dcb cn priority alt-priority

Use this command to configure a default congestion notification alternate priority on all ports for the specified CNPV.

Syntax

set dcb cn priority *cnpv* **alt-pri** *alt-priority*

Parameters

cnpv	Specifies a CNPV that the specified alternate priority is applied to.
alt-priority *alt-priority*	Specifies a non-CNPV alternate priority for the specified CNPV. Default value is **0**.

Defaults

The alternate priority defaults to **0**.

Mode

All command modes.

Usage

The congestion notification alternate priority is a non-CNPV. CNPVs are configured using "set dcb cn priority" on page 21-8. At least one 802.1p priority on a port must be a non-CNPV. Any non-CNPV can be used as a congestion notification alternate priority. A non-CNPV value should never be assigned to a transmit queue that contains a CNPV.

When a packet ingresses a congestion notification domain edge port with the same priority as a CNPV configured on the edge port, the priority of the ingressing packet must be remapped to an alternate priority. Should a non-congestion notification packet trigger congestion in a CNPV queue, the source for this packet will not know what to do with the CNM PDU it receives back from the congestion point. The remapping of the priority to a non-CNPV value at the congestion notification domain edge guards against this possibility.

The CNPV alternate priority value configured using this command is only used by a port-priority if the port-priority choice set using "set dcb cn port-priority choice" on page 21-19 is **default** and the CNPV choice set using "set dcb cn priority choice" on page 21-10 is **admin**.

If the port-priority choice is default and the CNPV choice is auto, or the port-priority choice is auto, the auto alternate priority is used. The auto alternate priority is the next lowest available non-CNPV priority relative to the CNPV. If there are no lower non-CNPVs, the next higher non-CNPV priority is used.

Examples

This example sets for CNPV **4**, the port-priority choice on all ports to **default**, the CNPV choice to **admin**, and priority **3** as the alternate priority:

```
S Chassis(rw)->set dcb cn port-priority *.*.* 4 choice default
S Chassis(rw)->set dcb cn priority 4 choice admin
S Chassis(rw)->set dcb cn priority 4 alt-pri 3
```

set dcb cn priority defense

Use this command to configure a default port congestion notification domain defense mode for all ports on the device for each priority.

Syntax

set dcb cn priority *priority* **defense** {**disabled** | **edge** | **interior** | **interior-ready**}

Parameters

priority	Specifies a CNPV to which the specified defense mode will be applied on this switch.
disabled	Specifies that the congestion notification capability is administratively disabled for this priority value.
edge	Specifies that the global default domain defense setting is edge for all ports.
interior	Specifies that the global default domain defense setting is interior for all ports.
interior-ready	Specifies that the global default domain defense setting is interior-ready for all ports.

Defaults

The default mode for domain defense depends upon the creation mode when the CNPV is created using “set dcb cn priority” on page 21-8. For **creation enable**, the default domain defense is **edge**. For **creation disable**, the default domain defense is **disabled**.

Mode

All command modes.

Usage

Note: CN is supported on the S-Series S140 and S180 modules. On non-supported S-Series modules, the Congestion Notification Domain Defense can be configured for either edge or disabled only. When edge configured, flows ingressing non-supported S-Series modules are remapped on ingress. Flows ingressing a supported S-Series module and egressing a non-supported S-Series module on the same chassis generate CNMs because congestion notification logic is performed on the ingress module.

Congestion notification domain defense provides a means of defending a congestion notification domain against incoming frames from outside of the domain. Domain defense assumes:

- That every bridge along a path between two congestion aware end-stations, using a particular CNPV, is properly configured for congestion notification and therefore belongs to the congestion notification domain
- That every bridge ensures that frames not in a CNPV use different queues than the CNPV queues for those end stations

Congestion notification defense protects the boundaries of a domain by preventing frames not in a congestion controlled flow from entering congestion point controlled queues. Domain defense takes advantage of the ability to change the priority value in the port-priority generation table based upon whether or not the port's neighbor is also configured with the same CNPV. If a frame with the same priority as the CNPV is not in the congestion controlled flow, the frame priority is changed to the configured alternate priority for that CNPV.

A default domain defense mode is configured at each congestion point port. There are four possible domain defense modes depending upon whether the CNPV is configured for the congestion point or where the congestion point port is located in the congestion notification domain:

- **Disabled** – A port for which congestion notification is disabled. This priority is not a CNPV. The priority regeneration table controls the remapping of ingress frames on this port for this priority. CN-TAGs are neither added by an end station nor removed by a bridge. This defense mode is the default defense mode when priority choice is set to admin. The disabled defense mode can only be set when the priority choice is set to admin. Priority choice can be set:
  - By default when creating the CNPV using the creation disable option
  - Using "set dcb cn priority choice" on page 21-10 at the switch level
  - Using "set dcb cn port-priority choice" on page 21-19 at the port level
- **Edge** – A congestion point port that resides at the edge of the congestion notification domain. On this port and for this CNPV, the ingress frame priority parameters are remapped to an alternate (non-CNPV) value, regardless of the priority regeneration table settings. CN-TAGs are not added by an end station, and are removed from frames by a bridge before egress. This mode is optional for an end station. The edge defense mode is the default defense mode when the priority choice is set to auto.
- **Interior** – A congestion point port that resides within the congestion notification domain between the flow's source reaction point and the destination end-station. This port does not yet know whether its neighbor is able to receive a CN-TAG in frames sent to it. On this port and for this CNPV, the ingress frame priority parameters are not remapped, regardless of the priority regeneration table settings. CN-TAGs are not added by an end station, and are removed from frames by a bridge before egress.
- **InteriorReady** – An interior congestion port that knows its neighbor is able to receive a CN-TAG in frames sent to it. On this port and for this CNPV, the ingress frame priority parameters are not remapped, regardless of the priority regeneration table settings. CN-TAGs can be added by an end station, and are not removed from frames by a bridge.

Defaults for domain defense can be configured by priority or by port. This command configures a global defense mode per congestion notification priority value for all ports on the device. A default domain defense can be set on a port basis for all congestion notification priority values on that port using "set dcb cn port-priority defense" on page 21-21.

Domain defense can be administratively configured, dynamically configured using LLDP, or based upon default values on a per port basis. The method used is referred to as "choice". The priority choice method on a global basis is configured using "set dcb cn priority choice" on

page 21-10. The port-priority choice method on a port basis is configured using "set dcb cn port-priority choice" on page 21-19.

The domain defense default configured using this command is only used if the port-priority choice set using "set dcb cn port-priority choice" on page 21-19 is **default** and the global choice "set dcb cn priority choice" on page 21-10 is **admin**.

Examples

This example first sets the port-priority choice to default and the CNPV choice to admin, both required for the admin configured defense setting to be used, then the example sets the default domain defense mode to **interior** for CNPV **3** for all congestion point ports on this device:

```
S Chassis(rw)->set dcb cn port-priority *.*.* 3 choice default
S Chassis(rw)->set dcb cn priority 3 choice admin
S Chassis(rw)->set dcb cn priority 3 defense interior
```

set dcb cn priority lldp

Use this command to enable or disable LLDP congestion notification on all ports.

Syntax

set dcb cn priority *priority* **lldp** {**enable** | **disable**}

Parameters

priority	Specifies a CNPV to which this congestion notification LLDP configuration is applied.
enable | **disable**	Enables or disables LLDP for dynamic configuration of domain defense.

Defaults

Congestion notification LLDP is enabled by default for all CNPVs. The sending of LLDP CN TLVs is disabled by default for all CNPVs.

Mode

All command modes.

Usage

This global congestion notification LLDP setting is only used if the port-priority LLDP setting using the "set dcb cn port-priority lldp" on page 21-22 is set to **default**.

LLDP, defined in the IEEE 802.1AB standard, can be used by congestion notification to control the operation of domain defense by:

- Advertising the CNPVs supported on a bridge or end-station port
- Determining whether a neighbor supports the same CNPVs as this port

Multiple instances of LLDP can be supported by a port. The instance used for domain defense defaults to the nearest bridge address. Priority choice, set using "set dcb cn priority choice" on page 21-10, must be set to auto for congestion notification LLDP to control domain defense on the device. If priority choice is set to auto and congestion notification LLDP is disabled, domain defense is set to edge on all ports.

The sending of congestion notification TLVs is enabled or disabled on a port using "set lldp port tx-tlv" on page 20-39 specifying the **congestion-notif** option.

Examples

This example first sets the LLDP port-priority to default for all ports, and then disables the global LLDP CNVP setting for CNPV 3:

```
S Chassis(rw)->set dcb cn port-priority *.*.* 3 lldp default
S Chassis(rw)->set dcb cn priority 3 lldp disable
```

clear dcb cn priority

Use this command to clear congestion notification configuration for the specified priority and context.

Syntax

clear dcb cn priority *priority* {[**entry**] [**status**] [**choice**] [**alt-pri**] [**defense**] [**creation**] [**lldp**]}

Parameters

priority	Specifies the CNPV to be cleared for the specified context.
entry	Deletes a congestion notification priority table entry for the specified CNPV.
status	Resets the status to the default value to **enabled** for the specified CNPV.
choice	Resets the domain defense choice to the default of **auto**.
alt-pri	Resets the alternate priority for the specified CNPV to the default of next lowest non-CNPV priority value or next highest non-CNPV value if all lower values are CNPV, if global defense choice is set to **auto**. If global defense choice is set to **admin**, the alternate priority defaults to **0**.
defense	Resets the domain defense method for the specified CNPV to the default value of: • **Edge** – If priority choice is set to auto • **Disabled** – If priority choice is set to admin
creation	Resets the CNPV auto creation for all ports to the default value of **enabled**.
lldp	Resets the congestion notification LLDP state to the default value of **enabled**.

Defaults

None.

Mode

All command modes.

Examples

This example deletes congestion notification entry CNPV 3:

```
S Chassis(rw)->clear dcb cn priority 3 entry
```

clear dcb cn port-priority

Use this command to clear congestion notification configuration for the specified priority and context.

Syntax

set dcb cn port-priority *port-name priority* {[**choice**] [**alt-pri**] [**defense**] [**lldp**]}

Parameters

port-name	Specifies the port for the CNPV to be cleared.
priority	Specifies the CNPV to be cleared for the specified context.
choice	Resets the domain defense choice to the default of **auto** on the specified port.
alt-pri	Resets the alternate priority on the specified port for the specified CNPV to the default of next lowest non-CNPV priority value or next highest non-CNPV value if all lower values are CNPV, if global defense choice is set to **auto**. If global defense choice is set to **admin**, the alternate priority defaults to **0**.
defense	Resets the domain defense method on the specified port for the specified CNPV to the default value of: • **Edge** – If priority choice is set to auto • **Disabled** – If priority choice is set to admin
lldp	Resets the congestion notification LLDP state on the specified port to the default value of **enabled**.

Defaults

None.

Mode

All command modes.

Examples

This example deletes congestion notification entry CNPV **3** on port **tg.1.1**:

```
S Chassis(rw)->clear dcb cn port-priority tg.1.1 3 entry
```

show dcb cn port-priority

Use this command to display congestion notification port level defense mode configuration.

Syntax

show dcb cn port-priority [*port-string* [*priority*]] [**priority** *priority*] [**-interesting**]

Parameters

port-string [*priority*]	(Optional) Displays domain defense mode configuration for the specified port for all priorities or the optionally specified priority. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.
priority *priority*	(Optional) Displays domain defense mode configuration for the specified CNPV.
-interesting	(Optional) Displays entries with a non-default defense mode.

Defaults

If no option is entered, congestion notification information is displayed for each port CNPV on all ports.

Mode

All command modes.

Examples

This example displays domain defense configuration information by port for all ports configured with a CNPV:

```
S Chassis(rw)->show dcb cn port-priority priority 6

Port      Pri  Selector  Choice  Alt  Defense Mode   LLDP      Status
--------  ---  --------  ------  ---  -------------  --------  --------
tg.1.1     6   Priority  Auto     5   Edge           Enabled   Active
tg.1.2     6   Priority  Auto     5   Edge           Enabled   Active
tg.1.3     6   Priority  Auto     5   Edge           Enabled   Active
...
```

This example displays congestion notification information for port ge.1.1:

```
S Chassis(rw)->show dcb cn port-priority tg.1.1 6

Port                     : tg.1.1
CN Priority Value        : 6

Port Selection
--------------
Defense Mode Choice      : Component (Selector=Priority)
Admin Defense Mode       : Disabled
Auto Defense Mode        : Edge
LLDP Choice              : Component (Selector=Priority)
LLDP Instance Selector   : 1
Admin Alternate Priority : 0

Priority Selection
------------------
```

```
Defense Mode Choice      : Auto
Admin Alternate Priority : 0
Auto Alternate Priority  : 5
Admin Defense Mode       : Interior
LLDP Choice              : Enabled
LLDP Instance Selector   : 1
```

Table 21-3 provides an explanation of the command output.

Table 21-3 show dcb cn port-priority Output Details

Output...	What it displays...
Port	A port configured for congestion notification.
Pri	Congestion Notification Priority Value (CNPV)
Alt	Alternate priority value (non-CNPV).
Selector	Specifies whether the port-priority default mode is selected based upon **priority** as configured by "set dcb cn priority choice" on page 21-10 or by **port** as configured by "set dcb cn port-priority choice" on page 21-19.
Mode	The congestion notification default mode: **Admin** – The default mode is Admin. The admin configured alternate priority and admin defense mode are used by the port-priority entries by default. **Auto** – The default mode is Auto. The auto alternate priority is used and the defense mode is selected by the port using LLDP.
Defense Mode	The defense mode used to protect the CNPV from receiving non-congestion controlled flows and determines if a CN-TAG should be removed or not. These states are defined per priority per port. See Table 21-2 on page 21-7 for defense mode state descriptions.
CN Priority Value	The congestion notification priority value configured for the port.
LLDP	Specifies whether LLDP instance selection is **enabled** or **disabled**.
Port Selection	This display section details port selection defense mode configuration.
Defense Mode Choice	Specifies the defense mode choice. Valid values are: • **Admin** – The congestion notification domain defense mode is controlled by the administrative variables in the same table entry as this object • **Auto** – This Port or all its congestion notification domain defense modes are controlled automatically • **Component** – The congestion notification domain defense mode is controlled by the congestion notification port-priority table settings
Admin Defense Mode	The defense mode that will be used if defense choice for this CNPV is admin.
Auto Defense Mode	The defense mode that will be used if defense choice for this CNPV is auto.

Table 21-3 show dcb cn port-priority Output Details

Output...	What it displays...
LLDP Choice	The LLDP defense choice setting for for the CNPV. Valid values are: • **Admin** – The congestion notification domain defense mode is controlled by the administrative variables in the same table entry as this object • **Auto** – This Port or all its congestion notification domain defense modes are controlled automatically • **Component** – The congestion notification domain defense mode is controlled by the congestion notification port-priority table settings
LLDP Instance Selector	The LLDP instance assigned to this CNPV.
Admin Alternate Priority	The administratively configured alternate priority for this CNPV
Priority Selection	This display section details priority selection defense mode configuration.
Auto Alternate Priority	Specifies the alternate priority using defense mode auto selection.

set dcb cn port-priority choice

Use this command to set, for specified priority and port, the mode that determines how the domain defense mode is selected for the specified port.

Syntax

set dcb cn port-priority *port-string priority* **choice** {**admin** | **auto** | **default**}

Parameters

port-string	Specifies the port to which the congestion notification priority choice setting is applied. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.
priority	Specifies the CNPV for this port-priority choice configuration.
admin	Specifies that the default domain defense is controlled by "set dcb cn priority defense" on page 21-12 and the alternate priority is controlled by "set dcb cn priority alt-priority" on page 21-11.
auto	Specifies that the default domain defense and alternate priority is controlled by LLDP.
default	Specifies that the default domain defense and alternate priority is the configured default value when entering the congestion notification priority value using "set dcb cn priority" on page 21-8.

Defaults

Port-priority choice defaults to **default**.

Mode

All command modes.

Usage

When entering any variation of the **set dcb cn port-priority** command, all options can be specified on a single command line. Options are: **choice**, **alt-pri**, **defense**, and **lldp**. These commands are detailed separately in this document for purposes of clarity.

Port-priority choice defaults to default. However, the default value of port-priority choice is determined by the creation option specified when creating the CNPV. If **creation enable** is used, the default choice for each port-priority is **default**. If **creation disable** is used, the default choice for each port-priority is **admin**. Upon entering the **clear dcb cn port-priority choice** command, the port-priority choice is set to **default**.

If the **admin** keyword is specified, the domain defense defaults to **disabled**, unless changed by one of the commands listed in the **admin** parameter table row above.

If the **auto** keyword is specified, the domain defense mode defaults to **edge** but will transition to **interior-ready** if the port's neighbor CNPV is activated and agrees with this port CNPV.

If the **default** keyword is specified, the domain defense depends upon whether the CNPV was created using the option:

- **Creation enable** – Defense mode defaults to **edge** (default CNPV creation mode)
- **Creation disable** – Defeinse mode defaults to **disabled**

Examples

This example sets the defense choice to **auto** for all ports:

```
S Chassis(rw)->set dcb cn port-priority *.*.* choice auto
```

set dcb cn port-priority alt-pri

Use this command to set the congestion notification alternate priority for the specified port and congestion notification priority.

Syntax

set dcb cn port-priority *port-string priority* **alt-pri** *alt-priority*

Parameters

port-string	For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.
priority	Specifies a CNPV to which Congestion Notification will be applied on the specified port.
alt-priority	The alternate priority a non-congestion controlled flow frame is remapped to when the ingressing frame has the same priority as a CNPV configured for this port.

Defaults

The port-priority alternate priority defaults to **0**.

Mode

All command modes.

Usage

When entering any variation of the **set dcb cn port-priority** command, all options can be specified on a single command line. Options are: **choice**, **alt-pri**, **defense**, and **lldp**. These commands are detailed separately in this document for purposes of clarity.

The port-priority alternate priority is only used by the port-priority if the port-priority choice is set to **admin**.

When a frame that belongs to a non-congestion controlled flow ingresses a CNPV configured port with the same priority as the CNPV, the flow priority is remapped to the alternate priority. If frames from a non-congestion controlled flow are allowed to enter a CNPV configured transmit queue and trigger a CNM PDU back to the flows source, the source will not be able to process the CNM PDU and the transmit rate of the flow causing the congestion will not be throttled. This would defeat the purpose of congestion notification.

Up to seven CNPV priorities are configurable on a port. This assures that at least one non-CNPV priority is available on each port as an alternate priority.

Examples

This example sets the alternate priority for CNPV **6** for all ports to **3**:

```
S Chassis(rw)->set dcb cn port-priority *.*.* 6 choice admin alt-pri 3
```

set dcb cn port-priority defense

Use this command to set the congestion notification domain defense mode for the specified port and priority.

Syntax

set dcb cn port-priority *port-string priority* **defense** {**disabled** | **interior** | **interior-ready** | **edge**}

Parameters

port-string	Specifies the port the domain defense mode is applied to. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.
priority	Specifies a CNPV to which the specified domain defense mode will be applied.
disabled	Specifies that domain defense is disabled on the specified port for the specified priority.
interior	Specifies that the port will be a congestion point port that resides within the congestion notification domain between the flow's reaction point and the destination end-station, but is not yet aware of its neighbors congestion notification capabilities.
interior-ready	Specifies that the port will be an interior congestion port that knows its neighbor is able to receive a CN-TAG in frames sent to it.
edge	Specifies that the port will be a congestion point port that resides at the edge of the congestion notification domain.

Defaults

Congestion notification domain defense defaults to **disabled** for all ports and priorities.

Mode

All command modes.

Usage

The port-priority defense is only used by the port-priority if the port-priority choice is configured for **admin**.

When entering any variation of the **set dcb cn port-priority** command, all options can be specified on a single command line. Options are: **choice**, **alt-pri**, **defense**, and **lldp**. These commands are detailed separately in this document for purposes of clarity.

See the usage section of "set dcb cn priority defense" on page 21-12 for domain defense details. This command applies the defense mode configuration to a specific CNPV on a specific port. The **set dcb cn priority defense** command applies the defense mode configuration to a specific CNPV on all ports. Otherwise the discussion applies to both commands.

Examples

This example sets the domain defense mode for priority **6** on all ports to **edge**:

```
S Chassis(rw)->set dcb cn port-priority *.*.* 6 choice admin defense edge
```

set dcb cn port-priority lldp

Use this command to enable, disable, or use the global default setting for congestion notification LLDP for the specified port and priority.

Syntax

set dcb cn port-priority *port-string priority* **lldp** {**enable** | **disable** | **default**}

Parameters

port-string	Specifies the port on which this LLDP configuration is applied. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.
priority	Specifies one or more CNPVs to which congestion notification LLDP configuration will be applied on this switch.
enable	Enables congestion notification LLDP for the specified port.
disable	Disables congestion notification LLDP for the specified port
default	Specifies that the default setting configured using "set dcb cn priority lldp" on page 21-14 is used for congestion notification LLDP for the specified port.

Defaults

Congestion notification LLDP is enabled by default on all ports.

Mode

All command modes.

Usage

When entering any variation of the **set dcb cn port-priority** command, all options can be specified on a single command line. Options are: **choice**, **alt-pri**, **defense**, and **lldp**. These commands are detailed separately in this document for purposes of clarity.

If priority choice is set to auto, congestion notification LLDP must be enabled for congestion notification negotiations to take place on the link.

If congestion notification LLDP disabled and priority choice is set to auto, the domain defense is set to edge for that CNPV. It will remain configured for edge defense, regardless of its place in the congestion notification domain because congestion notification negotiation can not occur.

If congestion notification LLDP is set to default on the port, the global setting configured using "set dcb cn priority lldp" on page 21-14 is used on the specified port.

The actual sending of congestion notification TLVs is disabled by default. The sending of congestion notification TLVs is enabled or disabled on a port using "set lldp port tx-tlv" on page 20-39 specifying the **congestion-notif** option.

Examples

This example disables congestion notification LLDP for priority **5** on port **tg.1.1**:

```
S Chassis(rw)->set dcb cn port-priority tg.1.1 5 lldp disable
```

show dcb cn congestion-point

Use this command to display the configuration and status of congestion notification congestion points.

Syntax

show dcb cn congestion-point [*port-string* [*cp-id*]] [**stats** [**-interesting**]]

Parameters

port-string	(Optional) Specifies a congestion point port to display. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.
cp-id	(Optional) Specifies a congestion point ID to display.
stats	(Optional) Displays congestion point statistics.
-interesting	(Optional) Displays only statistics of ports that transmitted congestion notification messages.

Defaults

If no options are specified, a summary line for all the congestion points on the bridge are displayed.

Mode

All command modes.

Examples

This example displays congestion point information for all ports:

```
S Chassis(rw)->show dcb cn congestion-point tg.1.1-3

                        Queue                Minimum     Minimum
            CP          Size                 Sample      Header
Port Name   Index  Pri  Set Point   Weight   Base        Octets
----------  -----  ---  ----------  ------   ----------  -------
tg.1.1        5     4   26000       1        150000      0
tg.1.2        5     4   26000       1        150000      0
tg.1.3        5     4   26000       1        150000      0
...
```

This example displays congestion point information for congestion point index **7** on port **tg.1.1**:

```
S Chassis(rw)->show dcb cn congestion-point tg.1.1 7

Congestion Point
-------------------------------------------------
Port                : tg.1.1
CP Index            : 7
Lowest CNPV         : 6
MAC Address         : 00-11-88-FE-79-6A
CP Identifier       : 00-11-88-FE-79-00-01-00
Q Size Set Point    : 26000
Feedback Weight     : 1
Min Sample Base     : 150000
Min Header Bytes    : 0
Discarded Frames    : 0
Transmitted Frames  : 0
Transmitted CCMs    : 0
Queue Profile Type  : 1
Queue Profile Index : 0
```

This example displays congestion point stats for all congestion points:

```
S Chassis(rw)->show dcb cn congestion-point stats

           CP   Tx                    Discarded             Tx
Port       Idx  Frames Count          Frames Count          CNMs Count
---------  ---  --------------------  --------------------  --------------------
tg.1.1      7   0                     0                     0
tg.1.2      7   0                     0                     0
tg.1.3      7   0                     0                     0
...
```

Table 21-4 provides an explanation of the command output.

Table 21-4 show dcb cn congestion-point Output Details

Output...	What it displays...
Port or Port Name	A port configured for congestion notification.
CP Index	The congestion point table index value for a congestion point on the bridge or end station device.
Pri or Lowest CNPV	The lowest numerical congestion notification priority value this congestion point table entry serves.
MAC Address	The MAC address of the system transmitting the congestion notification message (CNM) PDU and used as the CNM PDU source address.
CP Identifier	The Congestion Point Identifier (CPID) that uniquely identifies this congestion point in a virtual bridge network, carried in CNM PDUs sent by this congestion point.
Q Set-point or Queue Size Set Point	The set point for the queue managed by this congestion point is a target value for the number of octets in the congestion point queue. CNM PDUs are transmitted to the sources of frames queued in this congestion point's queue in order to keep the total number of octets stored in the queue at this set point.
Weight (W) or Feedback Weight	W is the weight to be given to the change in queue length in the calculation of quantitized feedback as defined in the IEEE 802.1Q-2011 standard. Weight is an integer value from which W is derived (equal to two to the power of the weight value specified here). Thus, if weight equals a -1, W = 1/2. This value is platform dependent and can be between the minimum weight and maximum weight as displayed by “show dcb cn q-profile” on page 21-29. The default value is **2**.
Min or Minimum Sample Base	The minimum number of octets to enqueue in the congestion point queue between transmissions of CNM PDUs. Default value is **150000**.
Minimum Header Octets or Min Header Bytes	The minimum number of octets to be returned in the encapsulated MSDU field of each CNM PDU generated.
Tx-Frames	The number of data frames passed on to the queue controlled by a congestion point that were not discarded.
Discarded Frames	The number of frames discarded because of a full output queue.
Transmitted Frames	The number of transmitted frames by this congestion point.
Transmitted CNMs	The number of CNM PDUs enqueued on this congestion point’s transmit queue.
Queue Profile Type	The transmit queue type.
Queue Profile Index	The transmit queue index.

set dcb cn congestion-point

Use this command to modify congestion point queue settings.

Syntax

set dcb cn congestion-point *port-string cp-index* [**set-point** *set-point*] [**weight** *weight*] [**qp-index** *qp-index*]

Parameters

port-string	Specifies the congestion point port. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.
cp-index	Specifies a congestion point index. Congestion point index values are generated by the firmware. Default value: The lowest CNPV value plus 1. Valid values are **1** - **4096**.
set-point *set-point*	(Optional) Specifies a target value for the number of octets in the congestion point queue. Valid values are **100** - **4294967296**. Default value is **26000**.
weight *weight*	(Optional) Specifies the exponent used in the calculation of the quantitized feedback W value. Valid values are device specific and can be displayed using "show dcb cn q-profile" on page 21-29. The default value is **1**.
qp-index *qp-index*	(Optional) Specifies a queue profile index for this congestion point.

Defaults

- The set point value default value is 26000 octets.
- The weight value default is 1.

Mode

All command modes.

Usage

This command provides for the modification of a subset of congestion queue parameters. A congestion queue is identified by the port and CNPV which it serves. A congestion queue on a given port may serve multiple CNPVs if multiple priorities are mapped to the same queue. A queue profile which currently provides for the configuration of the minimum sample option can also be associated with the congestion point configuration using the **qp-index** option.

The congestion point index value is assigned by the firmware when the congestion point entry is created. The congestion point index value is one greater than the lowest CNPV served by the congestion point. This is because the CNPV values are 0 based and congestion point index is 1's based.

The set point for the queue managed by the congestion point is a target value for the number of octets in the congestion point queue. CNM PDUs are transmitted to the sources of frames queued in this congestion point's queue in order to keep the total number of octets stored in the queue at the set point value.

W is the weight to be given to the change in queue length when calculating a measure of transmit queue congestion known as quantitized feedback (Fb) as defined in the IEEE 802.1Q-2011 standard. The weight option is an integer value from which W is derived. W is equal to two to the power of the weight value specified here. Thus, if weight equals a -1, W = 1/2. This value can be between the values specified by Min Weight and Max Weight for this device as displayed by "show dcb cn q-profile" on page 21-29. See the IEEE 802.1Q-2011 standard for a detailed discussion for W, weight, and Fb.

The queue profile index option allows for the association of a congestion notification queue profile with the ports assigned to this congestion notification configuration. The queue profile is configured using "set dcb cn q-profile" on page 21-30.

Examples

This example associates the qp-index settings with ports ge.1.1 through ge.1.5 for congestion point index 1:

```
S Chassis(rw)->set dcb cn congestion-point ge.1.1-5 1 qp-index 1.1
```

clear dcb cn congestion-point

Use this command to reset a congestion point queue configuration for ports associated with the specified congestion point index to default values.

Syntax

clear dcb cn congestion-point *port-string cp-index* [**set-point**] [**weight**] [**qp-index**]

Parameters

port-string	For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.
cp-index	Specifies a congestion point index.
set-point	(Optional) A target value for the number of octets in the congestion point queue. CNM PDU are transmitted to the frame source queued in this congestion point's queue in order to keep the total number of octets stored in the queue at this set point. The default value is **26000**.
weight	(Optional) Specifies the exponent used in the calculation of the quantitized feedback W value. Valid values are device specific and can be displayed using "show dcb cn q-profile" on page 21-29. The default value is 2.
qp-index	(Optional) Specifies a queue profile index for this congestion point.

Defaults

If no option is specified, the specified congestion point is cleared, otherwise only the optional value specified is reset to its default value.

Mode

All command modes.

Examples

This example resets the tg.1.1 congestion point queue parameter values to default values:

```
S Chassis(rw)->clear dcb cn congestion-point tg.1.1
```

show dcb cn cp-mapping

Use this command to display the Congestion Point Identifier (CPID) to index mapping by port.

Syntax

show dcb cn congestion-point [*port-string*]

Parameters

port-string	(Optional) Specifies a congestion point port to display for CPID to index mapping. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.
cp-id	(Optional) Specifies a congestion point ID to display.
stats	(Optional) Displays congestion point statistics.
-interesting	(Optional) Displays only statistics of ports that transmitted congestion notification messages.

Defaults

If a port or range of ports is not specified, mapping information for all ports displays.

Mode

All command modes.

Usage

A unique CPID displays for each transmit queue on bonding ports. On 40GbE mux ports, four CPIDs map to a single congestion point.

Examples

This example displays congestion point mapping information for ports tg.1.1 through tg.1.3:

```
S Chassis(rw)->show dcb cn cp-mapping tg.1.1-3

CP Identifier            Port        IF Index    CP Index
-----------------------  ----------  ----------  ----------
00-1F-45-A0-6A-47-00-10  tg.1.1      13001       5
00-1F-45-A0-6A-47-00-14  tg.1.2      13002       5
00-1F-45-A0-6A-47-00-18  tg.1.3      13003       5
```

Table 21-4 provides an explanation of the command output.

Table 21-5 show dcb cn cp-mapping Output Details

Output...	What it displays...
CP Identifier	The Congestion Point Identifier (CPID) that uniquely identifies this congestion point in a virtual bridge network, carried in CNM PDUs sent by this congestion point.
Port	A port configured for congestion notification.
IF Index	Interface Index value.
CP Index	The congestion point table index value for a congestion point on the bridge or end station device.

show dcb cn q-profile

Use this command to display the congestion notification queue profile configuration stats.

Syntax

show dcb cn q-profile [*profile-id*]

Parameters

profile-id	An integer ID value in dotted notation for this queue profile. Valid values are in dotted notion by index and type. For example, index **0** and queue type **1** would be formatted as **0.1**.

Defaults

If *profile-id* is not specified, all queue profiles are displayed.

Mode

All command modes.

Examples

This example displays the congestion notification queue profile information:

```
S Chassis(rw)->show dcb cn q-profile

Support Legend:
QS  - Queue Size Set Point    FW  - Feedback Weight
SB  - Minimum Sample Base     MH  - Minimum Header Octets
CP  - Supported by CP         NS  - Not Supported

--------------------------------------------------------------------------------
QP Type       :  1
Description   :  TOR-Series Min-Sample Profile
Max QP Entries:  2
Min Weight    : -2
Max Weight    :  5
Max Min-Sample:  261120
Support       :  SB
CP Ports      :  tg.1.1-24;fg.1.1-4;
--------------------------------------------------------------------------------

Queue    Queue               Minimum     Minimum
Profile  Size                Sample      Header
Index    Set Point   Weight  Base        Octets
-------  ----------  ------  ----------  ----------
0        CP          CP      150000      NS
```

Table 21-6 provides an explanation of the command output.

Table 21-6 show dcb cn profile Output Details

Output...	What it displays...
Support Legend	Defines acronyms listed in the Support field for this display.
QP Type	Specifies a queue type integer value based upon the platform.
Description	A queue type description.
Max QP Entries	Specifies the maximum number of queue profile entries supported by the device.
Min Weight	Specifies the minimum weight value supported by this device.
Max Weight	Specifies the maximum weight value supported by this device.
Max Min-Sample	Specifies the maximum minimum sample supported by this device.
Support	Specifies congestion point queue features supported by this device.
CP Ports	Specifies congestion point ports configured on the device.
QP Index	An index value for this queue profile.
Set Point	A target value for the number of octets in the congestion point queue. CNM PDUs are transmitted to the frame source queued in this congestion point's queue in order to keep the total number of octets stored in the queue at this set point.
Weight (W)	W is the weight to be given to the change in queue length in the calculation of quantitized feedback (a measure of transmit queue congestion) as defined in the IEEE 802.1Q-2011 standard. Weight is an integer value from which W is derived equal to two to the power of the weight value specified here. Thus, if weight equals a -1, W = 1/2. This value can be between the values specified by Min Weight and Max Weight for this device. The default value is **1**.
Minimum Sample Base	The minimum number of octets to enqueue in the congestion point queue between transmissions of CNM PDUs. The default value is **150000**.
Minimum Header Octets	The minimum number of octets to be returned in the encapsulated MSDU field of each CNM PDU generated.

set dcb cn q-profile

Use this command to configure a congestion notification queue profile.

Syntax

set dcb cn q-profile *qp-identifier* [**min-sample** *min-sample*]

Parameters

qp-identifier	Specifies the Congestion Notification queue profile identifier. The queue profile identifier is made up of the queue profile index and the queue type in dotted notation. For example, index 0 and type 1 would be specified as **0.1**. Valid index values are from **0** - **1**. The S-Series queue type is always **1**.

min-sample *min-sample*	(Optional) Specifies the minimum number of octets to enqueue in the congestion point queue between transmissions of CNM PDUs. Default value is **150000** octets.

Defaults

The minimum sample default is **150000** octets.

Mode

All command modes.

Usage

Each congestion notification queue belongs to one of two possible queue profiles on the S-Series. A queue profile is a management object containing congestion notification queue configuration. A queue profile is named based upon an index value and the queue type in dotted notation. The S-Series queue type is always **1**. The default queue profile is **0.1** and can not be modified. You can configure index value **1**.

The S-Series queue profile configuration supports the modification of the minimum sample parameter.

A queue profile is applied to a congestion queue by specifying its identifier when configuring a congestion point queue using "set dcb cn congestion-point" on page 21-25.

Examples

This example configures the queue profile for index **0** queue type **1**:

```
S Chassis(rw)->set dcb cn q-profile 0.1
```

clear dcb cn q-profile

Use this command to remove a queue profile or to reset an option to the default value.

Syntax

clear dcb cn q-profile *profile-name* {**entry** | **min-sample** *min-sample*}

Parameters

profile-name	Specifies the congestion notification queue profile name. The profile name is made up of the queue profile index and the queue type in dotted notation. For example, index 0 and type 1 would be specified as **0.1**.
entry	Deletes the queue profile entry specified by the entered profile name.
min-sample *min-sample*	Resets the minimum sample value to the default of **150000**.

Defaults

The minimum sample default value is **150000** octets.

Mode

All command modes.

Examples

This example removes the index 0 queue type 1 queue profile:

```
S Chassis(rw)->clear dcb cn q-profile 0.1 entry
```

show dcb cn errored-ports

Use this command to display ports with the alternate priority set to a priority that is acting as a CNPV.

Syntax

show dcb cn errored-ports

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

Configuring an alternate priority to a CNPV is not supported. When a packet that does not belong to a congestion controlled flow has the same priority as a CNPV configured on a congestion notification domain edge ingress port, it must be remapped to an alternate priority to defend against a false triggering of a congestion notification by a non-congestion controlled flow. Any non-congestion aware priority (non-CNPV) can be used as a congestion notification alternate priority.

Examples

This example displays ports with the alternate priority set to a CNPV:

```
S Chassis(rw)->show dcb cn errored-ports
Port        Pri  Selector  Alt
----------  ---  --------  ---
tg.1.1       7   Priority   4
```

22

Tracked Object Manager Commands

This chapter provides detailed information for the Tracked Object Manager set of commands.

Tracked object manager functionality includes the creation and configuration of tracked objects and probes. Tracked objects monitor the state of local entities, such as interfaces. State probes monitor the state of remote entities, such as host servers. Timing probes collect packet timing data. Tracked objects and probes are used by client applications.

Note: For Bidirectional Forwarding Detection (BFD) State and Timing probe command information see Chapter 23, **Bidirectional Forwarding Detection Commands**.

For information about configuring tracked objects and probes, refer to the "Tracked Object Manager Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
State Probe Commands	22-1
Timing Probe Commands	22-18
Tracked Object Commands	22-24

State Probe Commands

State probes monitor the state of remote entities, such as host servers. Probes are used by client applications such as policy based routing, server load balancing, TWCB, and VRRP critical IP interfaces.

For information about...	Refer to page...
probe	22-2
acv close	22-3
acv reply	22-4
acv request	22-5
acv search-depth	22-5
description	22-6
dns-query type	22-7
faildetect	22-8
inservice	22-9

For information about...	Refer to page...
l5-type	22-10
open	22-11
passdetect	22-11
receive	22-12
show probe	22-13
show probe session	22-16
show probe default	22-17

probe

Use this command to create a probe and enter probe configuration mode.

Syntax

probe *probe-name* {**icmp** | **tcp** | **udp**}

no probe *probe-name* {**icmp** | **tcp** | **udp**}

Parameters

probe-name	Specifies a probe name. Valid values are up to 31 characters. The space character is not supported.
icmp	Specifies an ICMP probe.
tcp	Specifies a TCP probe.
udp	Specifies a UDP probe.

Defaults

None.

Mode

Global configuration.

Usage

Probe names are case sensitive.

Use the **no probe** command to delete the specified probe.

Examples

This example enters configuration mode for a TCP probe with ACV configured named **TCP-HTTP** and displays a detailed level of information for the probe:

```
S Chassis(su)->configure
S Chassis(su-config)->probe TCP-HTTP tcp
S Chassis(su-config-probe)->show probe TCP-HTTP detail

Probe:                          TCP-HTTP  Type:                          tcp-acv
```

```
Administrative state:   not-in-service  Session count:                        1
Fail-detect count:                   3  Pass-detect count:                    3
Fail-detect interval:                5  Pass-detect interval:                 5
3-way TCP handshake wait time:       5  Server response wait time:           10
Application Content Verification:
 Request-string: GET / HTTP/1.1\\r\\nHost: 2.0.0.5\\r\\n\\r\\n
 Reply-string:   HTTP/1.1 200 OK\\r\\n
 Close-string:
 Search-Depth:   255

Displayed 1 probes
S Chassis(su-config-probe)->
```

acv close

Use this command when the probe is configured for Application Content Verification (ACV) and the remote server requires you to close the session.

Syntax

acv close *close-string*

no acv close *close-string*

Parameters

close-string	Specifies the close string used to close the session. Valid value is a string of up to 127 printable characters. If a space character is used, the string must be enclosed in double quotes (“”).

Defaults

None.

Mode

State probe configuration mode.

Usage

Use the **no acv close** command to delete the close string configuration for this probe.

Examples

This example sets the ACV close string for the TCP-HTTP probe to **quit**:

```
S Chassis(su-config)->probe TCP-HTTP udp
S Chassis(su-config-probe)->acv close quit
S Chassis(su-config-probe)->show probe TCP-HTTP detail

Probe:                       TCP-HTTP  Type:                             tcp-acv
Administrative state:   not-in-service  Session count:                        1
Fail-detect count:                   3  Pass-detect count:                    3
```

```
Fail-detect interval:               10  Pass-detect interval:               10
3-way TCP handshake wait time:       5  Server response wait time:          10
Application Content Verification:
 Request-string:
 Reply-string:
 Close-string:   quit
 Search-Depth:   255

Displayed 1 probes
S Chassis(su-config-probe)->
```

acv reply

Use this command to set the expected validation ACV reply string that the Tracked Object Manager uses to validate the string the server responds with.

Syntax

acv reply *reply-string*

no acv reply *reply-string*

Parameters

reply-string	Specifies the expected reply returned from the server. Valid value is a string of up to 127 printable characters. If a space character is used, the string must be enclosed in double quotes (**“”**).

Defaults

None.

Mode

State probe configuration mode.

Usage

The server reply to the ACV request is validated against the ACV reply string specified in this command.

Use the **no acv reply** command to remove the reply string configuration for this probe.

Examples

This example sets the TCP-HTTP probe reply string to **“HTTP/1.1 200 OK”**:

```
S Chassis(su-config)->probe TCP-HTTP tcp
S Chassis(su-config-probe)->acv reply “HTTP/1.1 200 OK”
S Chassis(su-config-probe)->
```

acv request

Use this command to set the request string to send to the remote application.

Syntax

acv request *request-string*

no acv request *request-string*

Parameters

request-string	Specifies the request string sent to the server application port. Valid value is a string of up to 127 printable characters. If a space character is used, the string must be enclosed in double quotes (**“”**).

Defaults

None.

Mode

State probe configuration mode.

Usage

The ACV *request-string* is required when the probe is configured for ACV. This is the string that the Tracked Object Manager sends to the application port of the server. The server’s reply will be validated against the ACV *reply-string* specified in the command “acv reply” on page 22-4.

A Carriage Return / Line Feed character “\\r\\n” should be included in the ACV *request-string* if it is required by the server protocol. Carriage Returns and Line Feeds are control characters and require a double backslash “\\” to be treated as control characters. That is '\\r' is a Carriage Return and '\\n' is a Line Feed, and ‘\\t’ is a TAB.

Use the **no acv request** command to delete the ACV request configuration for this probe.

Examples

This example sets the request string for probe TCP-HTTP to **“GET / HTTP/1.1\\r\\nHost: 2.0.0.5\\r\\n\\r\\n”**:

```
S Chassis(su-config)->probe TCP-HTTP tcp
S Chassis(su-config-probe)->acv request “GET / HTTP/1.1\\r\\nHost:
2.0.0.5\\r\\n\\r\\n”
S Chassis(su-config-probe)->
```

acv search-depth

Use this command to set the number of characters into the server response to search for the ACV reply string.

Syntax

acv search-depth *search-depth*

Parameters

search-depth	Specifies how deep into the server response to search for the ACV reply string. Valid values are **1** - **255** characters. Default value is **255** characters.

Defaults

None.

Mode

State probe configuration mode.

Usage

A match within the response must occur prior to exceeding the search-depth.

Use the **no acv search-depth** command to reset the search depth to the default value of **255** characters.

Examples

This example sets the search depth for the TCP-HTTP probe to **150** characters:

```
S Chassis(su-config)->probe TCP-HTTP tcp
S Chassis(su-config-probe)->acv search-depth 150
S Chassis(su-config-probe)->
```

description

Use this command to configure a useful description for the probe.

Syntax

description *description-text*

no description *description-text*

Parameters

description-text	Specifies a description of this probe. Valid values are up to 127 printable characters. If a space character is used, the description must be enclosed in double quotes (“”).

Defaults

None.

Mode

State probe configuration mode.

Usage

Use the **no description** command to remove the current description for this probe.

Examples

This example configures the docUdp1 probe description as **"Doc Server UDP probe"**:

```
S Chassis(su-config)->probe docUdp1 udp
S Chassis(su-config-probe)->description "Doc Server UDP probe"
S Chassis(su-config-probe)->
```

dns-query type

Use this command to specify a DNS query type to send with this state probe.

Syntax

dns-query type {[**domain** [**ip** *ip-address* | *name*] | **host** *name* | **ipv6** *ipv6-address*]}

no dns-query type {[**domain** [**ip** *ip-address* | *name*] | **host** *name* | **ipv6** *ipv6-address*]}

Parameters

domain *name*	Specifies the domain name as the query type to be sent with this state probe.
ip *ip-address*	Specifies an in-addr.arpa or ip6.arpa address.
host *name*	Specifies a host name as the query type to be sent with this state probe.
ipv6 *ipv6-address*	Specifies an IPv6 address as the query type to be sent with this state probe.

Defaults

None.

Mode

State probe configuration mode.

Usage

The **ip** *ip-address* option provides the user a shortcut for configuring an in-addr.arpa or ip6.arpa address.

The **no** form of the command deletes the query type configuration for this state probe.

Example

This example configures the **docUdp1** probe to send domain **extremenetworks** as the DNS query type for this probe.

```
S Chassis(su)->configure
S Chassis(su-config)->probe docUdp1 udp
S Chassis(su-config-probe-timing)->dns-query type domain extremenetworks
```

dns-verify match

Use this command to verify the response to a DNS query.

Syntax

dns-verify match {**address** *ip-address* | **domain** *name*}

no dns-verify match {**address** *ip-address* | **domain** *name*}

Parameters

address *ip-address*	Specifies the IP address to verify in the DNS query response.
domain *name*	Specifies the domain name to verify in the DNS query response. Valid values are up to 255 characters.

Defaults

None.

Mode

State probe configuration mode.

Usage

The **ip** *ip-address* option provides the user a shortcut for configuring an in-addr.arpa or ip6.arpa address.

The **no** form of the command deletes the query type configuration for this state probe.

Example

This example configures the **docUdp1** probe to send domain **extremenetworks** as the DNS query type for this probe.

```
S Chassis(su)->configure
S Chassis(su-config)->probe docUdp1 udp
S Chassis(su-config-probe-timing)->dns-query type domain extremenetworks
```

faildetect

Use this command to configure the probe faildetect object parameters.

Syntax

faildetect {[**count** *count*] [**interval** *seconds*]}

no faildetect {[**count** *count*] [**interval** *seconds*]}

Parameters

count *count*	(Optional) Specifies the consecutive number of failed attempts before the service is declared down. Valid values are **1** - **65535** attempts. The default value is **3** attempts.
interval *seconds*	(Optional) Specifies the delay between probes to a service that is up. Valid values are **2** - **300** seconds. The default value is **10** seconds.

Defaults

Any parameter not specified remains at its current value. You must specify at least one parameter.

Mode

State probe configuration mode.

Usage

Fail detection is used to determine if a service is up. When the number of consecutive failed retries equals the fail detection count value, the service is declared down.

Modifying the interval will not update for currently scheduled sessions. The new interval value takes affect for any subsequently scheduled probes.

Use the **no faildetect** command to reset the faildetect count and interval to the default values of **3** attempts for count and **10** seconds for interval.

Examples

This example sets the number of failed attempts before a service is declared down to **5** and the interval between probes, when a service is up, to **15** seconds:

```
S Chassis(su-config)->probe docUdp1 udp
S Chassis(su-config-probe)->faildetect count 5 interval 15
S Chassis(su-config-probe)->
```

inservice

Use this command to enable the probe for this context.

Syntax

inservice

no inservice

Parameters

None.

Defaults

None.

Mode

State probe configuration mode.

Usage

Use the **no inservice** command to set the probe for this context to not-in-service. Probe configuration remains unchanged. Use the **no probe** command to delete a probe. A probe is not-in-service by default.

Taking a probe out-of-service, removes its sessions from the Tracked Object Manager's scheduler. Putting a probe inservice adds its sessions to the Tracked Object Manager scheduler.

Examples

This example places you in the docUdp1 probe context and enables the context:

```
S Chassis(su-config)->probe docUdp1 udp
S Chassis(su-config-probe)->inservice
```

l5-type

Use this command to specify the Layer 5 protocol to use with this state probe.

Syntax

l5-type {**acv** | **dns**}

no l5-type {**acv** | **dns**}

Parameters

acv	Specifies ACV objects should be used with this state probe.
dns	Specifies that DNS objects should be used with this state probe.

Defaults

None.

Mode

Timing probe configuration mode.

Usage

The **no** form of the command deletes the L5 protocol type configuration for this timing probe.

Example

This example configures the **docUdp1** probe to use the DNS L5 type protocol objects with this probe.

```
S Chassis(su)->configure
S Chassis(su-config)->probe docUdp1 udp
S Chassis(su-config-probe-timing)->l5type dns
```

open

Use this command to specify the interval to wait for the TCP 3-way handshake to complete.

Syntax

open *wait-interval*

Parameters

wait-interval	Specifies an interval in seconds that the Tracked Object Manager will wait for the TCP 3-way handshake to complete. Valid values are **1** - **30** seconds. The default value is **5** seconds.

Defaults

None.

Mode

State probe configuration mode.

Usage

TCP uses a 3-way handshake to establish a connection. If the handshake does not complete within this interval, the switch assumes the connection establishment has failed. This command is only supported for TCP probes.

Examples

This example configures the wait interval to **7** seconds:

```
S Chassis(su-config)->probe docTcp1 tcp
S Chassis(su-config-probe)->open 7
S Chassis(su-config-probe)->
```

passdetect

Use this command to configure the parameters used to determine when a service marked as down can be declared up.

Syntax

passdetect {[**count** *count*] [**interval** *seconds*]}

no passdetect {[**count** *count*] [**interval** *seconds*]}

Parameters

count *count*	(Optional) Specifies the consecutive number of successful probes to a service before the service is declared up. Valid values are **1** - **65535** successful probes. The default value is **3** successful probes.
interval *seconds*	(Optional) Specifies the delay between probes to a service that is currently down. Valid values are **2** - **300** seconds. The default value is **300** seconds.

Defaults

Any parameter not specified remains at its current value. You must specify at least one parameter.

Mode

State probe configuration mode.

Usage

Pass detection is used to determine when a service that is currently down can be declared up. When the number of consecutive successful probes to a service equals the pass detection count value, the service is declared up.

Modifying the interval will not update for currently scheduled sessions.

Use the **no passdetect** command to reset the passdetect count and interval to the default values of **3** successful probes for count and **300** seconds for interval.

Examples

This example sets the number of successful probes before a service that is currently down will be declared up to **5** and the interval between probes to **15** seconds:

```
S Chassis(su-config)->probe docTcp1 tcp
S Chassis(su-config-probe)->passdetect count 5 interval 15
S Chassis(su-config-probe)->
```

receive

Use this command to specify the time the Tracked Object Manager waits for a response from the monitored service before declaring a failed probe.

Syntax

receive *wait-interval*

no receive *wait-interval*

Parameters

wait-interval	Specifies the time in seconds the Tracked Object Manager waits for a response from the monitored service before declaring a failed probe. Valid values are **1** - **65535** seconds. Default value is **10** seconds.

Defaults

None

Mode

State probe configuration mode.

Usage

Use the **no receive** command to reset the time the Tracked Object Manager waits for a reply from the service before declaring that a probe has failed to the default value of **10** seconds.

Examples

This example sets the interval the Tracked Object Manager waits before declaring a failed probe for the **docTcp1** probe to **5** seconds:

```
S Chassis(su-config)->probe docTcp1 tcp
S Chassis(su-config-probe)->receive 5
```

show probe

Use this command to display probe configuration and statistics.

Syntax

show probe [*probe-name* [**detail** | **session**]]

Parameters

probe-name	(Optional) Specifies the name of the probe for which a summary information line will display.
detail	(Optional) Specifies that a detailed level of configuration information should display for the specified probe.
session	(Optional) Specifies that session information should display for the specified probe.

Defaults

If *probe-name* is not specified, a summary line for all probes displays.

If **detail** or **session** is not specified, a summary line for the specified probe displays.

Mode

All command modes.

Examples

This example displays a summary line of information for all configured probes:

```
S Chassis(su)->show probe

Type Codes: S-state probe, T-timing probe

Probe name                     T Protocol  Status     Sessions
------------------------------ - --------- ---------- --------
$rte_default                   S bfd       Inservice  1
UdpDoc                         S udp       Disabled   0
icmpDoc                        S icmp      Inservice  1
icmpTimingDoc                  T icmp      Disabled   0
```

```
tcpDoc                          S tcp       Inservice  1
bfdDoc                          S bfd       Inservice  1

Displayed 6 probes
S Chassis(su)->
```

This example displays a detailed level of information for probe **tcpDoc**:

```
S Chassis(su)->show probe tcpDoc detail
Description: HTTP TCP probe with ACV
Probe:                          tcpDoc  Protocol:                        tcp-acv
Administrative state:        inservice  Session count:                         1
Fail-detect count:                   3  Pass-detect count:                    3
Fail-detect interval:                2  Pass-detect interval:                10
3-way TCP handshake wait time:       5  Server response wait time:           10
Application Content Verification:
 Request-string: GET / HTTP/1.1\\r\\nHost: 2.0.0.5\\r\\n\\r\\n
 Reply-string:   HTTP
 Close-string:
 Search-Depth:   255

Displayed 1 probes
S Chassis(su)->
```

This example displays a detailed level of information for the BFD probe **bfdDoc**:

```
show probe bfdDoc detail


Description: BFD Documentation Probe
State Probe:                      bfdDoc Protocol:                          bfd
Administrative state:        inservice  Session count:                         1
Desired tx rate (ms):               50  Echo tx rate (ms):                  250
Minimum rx rate (ms):               50  Echo rx rate (ms):                  250
Detection multiplier:                7  Echo miss-count:                     4
Slow-timer (ms):                  1050  Echo mode:                       enabled
Demand-mode (seconds):             136
```

This example displays a summary line of information for probe **docProbeTcp1**:

```
S Chassis(su)->show probe tcpDoc
                                        Faildetect     Passdetect
Probe name                      Type    Count/Interval Count/Interval Sessions
------------------------------- ------- -------------- -------------- --------
tcpDoc                          tcp     3/10           3/300          1

Displayed 1 probes
S Chassis(su)->
```

Table 22-1 provides an explanation of the **show probe detail** command output.

Table 22-1 show probe detail Output Details

Output...	What it displays...
Description	Specifies an administratively configured description for this probe, as configured using "description" on page 22-6. This field only displays if the description has been set.

Table 22-1 show probe detail Output Details (continued)

Output...	What it displays...
Probe name	Specifies the name of the probe, as configured using "probe" on page 22-2 or "probe icmp timing" on page 22-18.
T	Specifies the probe type: • **S** – State probe • **T** – Timing probe
Protocol	Specifies the probe protocol: BFD, ICMP, TCP, or UDP.
Status	Specifies whether the probe is inservice or disabled.
Sessions or Session count	Specifies the number of active sessions for this probe.
Administrative state	Specifies whether the probe is inservice or not-in-service, as configured using "inservice" on page 22-9.
Fail-detect count	Specifies the consecutive number of failed attempts before the service is declared down, as configured using "faildetect" on page 22-8.
Fail-detect interval	Specifies the delay between probes to a service that is up, as configured using "faildetect" on page 22-8.
3-way TCP handshake wait time	Specifies an interval in seconds that the Tracked Object Manager will wait for the 3-way handshake to complete, as configured using "open" on page 22-11.
Type	Specifies the probe protocol specified when creating the probe. "-acv" is appended to the type if any ACV parameter is configured.
Session count	Specifies the number of active sessions using this probe.
Pass-detect count	Specifies the consecutive number of successful probes to a service before the service is declared up, as configured using "passdetect" on page 22-11.
Pass-detect interval	Specifies the delay between probes to a service that is currently down, as configured using "passdetect" on page 22-11.
Server response wait time	Specifies the time in seconds the Tracked Object Manager waits for a response from the service, before declaring a failed probe, as configured using "receive" on page 22-12.
Request-string	Specifies the command string sent to the server application port, as configured using "acv request" on page 22-5.
Reply-string	Specifies the expected reply returned from the server, as configured using "acv reply" on page 22-4.
Close-string	Specifies the close string used to close the session, if required by the remote protocol, as configured using "acv close" on page 22-3.
Search-depth	Specifies how deep into the response packet from the server to search for the ACV reply string, as configured using "acv search-depth" on page 22-5.
Desired tx rate (ms)	Specifies the minimum interval in 50ms increments between the transmission of control packets.
Minimum rx rate (ms)	Specifies the minimum interval in 50ms increments between received control packets the system supports.
Detection multiplier	Specifies the minimum number of consecutive packets that can be missed before the BFD session transitions to down.

Table 22-1 show probe detail Output Details (continued)

Output...	What it displays...
Slow-timer (ms)	Specifies the value of the BFD slow timer feature to override the Control min-rx value when echo mode is active.
Demand-mode (seconds)	Specifies the number of seconds a session must remain up before demand-mode will be enabled.
Echo tx rate (ms)	Specifies the minimum interval in 50ms increments between the transmission of echo packets.
Echo rx rate (ms)	Specifies the minimum interval in 50ms increments between received echo packets the system supports.
Echo miss-count	Specifies the minimum number of consecutive echo packets that can be missed before the BFD session transitions to down.
Echo mode	Specifies whether the Echo feature is enabled or disabled.

show probe session

Use this command to display probe information for all sessions.

Syntax

show probe [*probe-name*] **session**

Parameters

None.

Defaults

None.

Mode

All command modes.

Examples

This example displays probe sessions:

```
S Chassis(su)->show probe bfdDoc session

Client Codes: P-policy based routing, S-SLB, V-VRRP, W-TWCB, U-tunnel
              R-static routes, I-IP SLA, G-routing protocols

Probe: bfdDoc, bfd
IP Address                        Port  Status    StChngs Last Change   Clients
--------------------------------- ----- --------- ------- ------------- -------
10.211.254.2                      0     Up        1            6h29m37s G
Displayed 1 sessions

Displayed 1 probes, 1 sessions
S Chassis(su)->
```

Table 22-2 provides an explanation of the **show probe sessions** command output.

Table 22-2 show probe sessions Output Details

Output...	What it displays...
IP Address	Specifies the IP address the probe is monitoring.
Port	Specifies the port the probe is monitoring
Status	Specifies the port status.
StChngs	Specifies the number of state changes that have occurred since session creation.
Last Change	Specifies period of time since the last state change.
Clients	Specifies the probe local application type(s): • **P** – Policy Based Routing probe • **S** – Server Load Balancing (SLB) probe • **W** – Transparent Web Cache Balancing (TWCB) probe • **V** – Virtual Router Redundancy Protocol (VRRP) probe • **U** – Tunnel probe • **R** – Static route probe • **I** – IP SLA probe • **G** – Routing Protocol

show probe default

Use this command to display the default probes.

Syntax

```
show probe default
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

```
S Chassis(su)->show probe default

Type Codes: S-state probe, T-timing probe

Probe name                     T Protocol  Status     Sessions
------------------------------ - --------- ---------- --------
$ipsla_default                 T icmp      Inservice  0
$ls_default                    S icmp      Inservice  0
$pbr_default                   S icmp      Inservice  0
$rte_default                   S bfd       Inservice  1
$slb_default                   S icmp      Inservice  0
$sr_default                    S icmp      Inservice  0
```

```
$tunnel_default                 S icmp      Inservice  0
$twcb_default                   S icmp      Inservice  0
$vrrp_default                   S icmp      Inservice  0

Displayed 9 probes
```

Timing Probe Commands

Timing probes collect packet timing data and are used by applications such as the IP SLA application.

For information about...	Refer to page...
probe icmp timing	22-18
probe udp timing	22-19
description	22-6
dns-query type	22-7
inservice	22-9
interval	22-22
l5-type	22-10
packet-options	22-23
receive	22-12

probe icmp timing

Use this command to create an ICMP timing probe and enter probe timing configuration mode.

Syntax

probe *probe-name* **icmp timing**

no probe *probe-name* **icmp timing**

Parameters

probe-name	Specifies a ICMP timing probe name. Valid values are up to 31 characters. The space character is not supported.

Defaults

None.

Mode

Global configuration.

Usage

The ICMP timing probe allows you to collect timing information for ICMP echo requests. After you execute this command, you enter probe timing configuration mode where you can further configure the probe.

The **no** form of the command deletes the probe from the Tracked Object Manager.

Example

This example creates the ICMP timing probe named ICMP_STATS and enters probe timing configuration mode.

```
S Chassis(su)->configure
S Chassis(su-config)->probe ICMP_STATS icmp timing
S Chassis(su-config-probe-timing)->
```

probe udp timing

Use this command to create an UDP timing probe and enter probe timing configuration mode.

Syntax

probe *probe-name* **udp timing**

no probe *probe-name* **udp timing**

Parameters

probe-name	Specifies a UDP timing probe name. Valid values are up to 31 characters. The space character is not supported.

Defaults

None.

Mode

Global configuration.

Usage

The UDP timing probe allows you to collect timing information for UDP echo requests. After you execute this command, you enter probe timing configuration mode where you can further configure the probe.

The **no** form of the command deletes the probe from the Tracked Object Manager.

Example

This example creates the UDP timing probe named UDP_STATS and enters probe timing configuration mode.

```
S Chassis(su)->configure
S Chassis(su-config)->probe UDP_STATS udp timing
S Chassis(su-config-probe-timing)->
```

description

Use this command to add a description to the ICMP timing probe.

Syntax

description *string*

no description *string*

Parameters

string	Enter a string of up to 127 characters in length to describe this ICMP timing probe. If the string includes spaces, enclose the string in quotes.

Defaults

None.

Mode

Timing probe configuration mode.

Usage

The **no** form of the command deletes the description.

Example

This example creates the ICMP timing probe named ICMP_STATS, enters probe timing configuration mode, then enters a description for the probe.

```
S Chassis(su)->configure
S Chassis(su-config)->probe ICMP_STATS icmp timing
S Chassis(su-config-probe-timing)->description "campus1 SLA"
```

dns-query type

Use this command to specify a DNS query type to send with this timing probe.

Syntax

dns-query type {[**domain** [**ip** *ip-address* | *name*] | **host** *name* | **ipv6** *ipv6-address*]}

no dns-query type {[**domain** [**ip** *ip-address* | *name*] | **host** *name* | **ipv6** *ipv6-address*]}

Parameters

domain *name*	Specifies the domain name as the query type to be sent with this timing probe.
ip *ip-address*	Specifies an in-addr.arpa or ip6.arpa address.
host *name*	Specifies a host name as the query type to be sent with this timing probe.
ipv6 *ipv6-address*	Specifies an IPv6 address as the query type to be sent with this timing probe.

Defaults

None.

Mode

Timing probe configuration mode.

Usage

The **ip** *ip-address* option provides the user a shortcut for configuring an in-addr.arpa or ip6.arpa address.

The **no** form of the command deletes the query type configuration for this timing probe.

Example

This example configures the **UDPtiming1** probe to send domain **extremenetworks** as the DNS query type for this probe.

```
S Chassis(su)->configure
S Chassis(su-config)->probe UDPtiming1 udp timing
S Chassis(su-config-probe-timing)->dns-query type domain extremenetworks
```

inservice

Use this command to place the probe in service and put its associated sessions on the scheduling queue.

Syntax

inservice

no inservice

Parameters

None.

Defaults

A probe is not in service by default.

Mode

Timing probe configuration mode.

Usage

Use the **no inservice** command to set the probe to not-in-service. Probe configuration remains unchanged. Use the **no probe** command to delete a probe. A probe is not in service by default.

Taking a probe out-of-service removes its sessions from the Tracked Object Manager's scheduler. Putting a probe in service adds its sessions to the Tracked Object Manager's scheduler.

Examples

This example creates the ICMP timing probe named ICMP_STATS, enters probe timing configuration mode, then puts the probe in service.

```
S Chassis(su)->configure
S Chassis(su-config)->probe ICMP_STATS icmp timing
S Chassis(su-config-probe-timing)->inservice
```

interval

Use this command to set the transmit rate of the ICMP echo requests.

Syntax

interval *millisecs*

no interval *millisecs*

Parameters

millisecs	Specifies the transmit rate in milliseconds. Value can range from 100 to 30000 milliseconds, in increments of 100 milliseconds. Default is 2000 ms. This value must be larger than the "receive wait" time.

Defaults

2000 milliseconds.

Mode

Timing probe configuration mode.

Usage

The interval must be specified in increments of 100 milliseconds. This value must be larger than the time configured with the receive command to wait for an ICMP echo reply. If you try to set a value smaller than the currently configured "receive wait" time, the command will be rejected and you will get a system message.

The **no** form of this command returns the transmit rate to the default of 2000 milliseconds.

Example

This example sets the transmit rate to 1000 milliseconds.

```
S Chassis(su)->configure
S Chassis(su-config)->probe ICMP_STATS icmp timing
S Chassis(su-config-probe-timing)->interval 1000
```

l5-type

Use this command to specify the Layer 5 protocol to use with this timing probe.

Syntax

l5-type {**acv** | **dns**}

no l5-type {**acv** | **dns**}

Parameters

acv	Specifies ACV objects should be used with this timing probe.
dns	Specifies that DNS objects should be used with this timing probe.

Defaults

None.

Mode

Timing probe configuration mode.

Usage

The **no** form of the command deletes the L5 protocol type configuration for this timing probe.

Example

This example configures the **UDPtiming1** probe to use the DNS L5 type protocol objects with this probe:

```
S Chassis(su)->configure
S Chassis(su-config)->probe UDPtiming1 udp timing
S Chassis(su-config-probe-timing)->l5type dns
```

packet-options

Use this command to set the IP type of service or VLAN priority code point value to be included in the ICMP echo requests sent.

Syntax

packet-options {**ip-tos** *tos* | **vlan-pcp** *pcp*}

no packet-options {**ip-tos** *tos* | **vlan-pcp** *pcp*}

Parameters

ip-tos *tos*	Specifies a value for the type of service field in the IP header of the ICMP echo request sent. Value can range from 0 to 255. Default is 0.
vlan-pcp *pcp*	Specifies a value for the VLAN priority code point of the echo request sent. Value can range from 0 to 7. Default is 0.

Defaults

ToS and PCP defaults are 0.

Mode

Timing probe configuration mode.

Usage

The value set with this command is sent in the ICMP echo request. The Tracked Object Manager collects information about whether the responding device's reply contained the same ToS or PCP value.

The **no** form of this command returns the ToS or PCP value to 0.

Example

This example sets the ToS value to 5.

```
S Chassis(su)->configure
S Chassis(su-config)->probe ICMP_STATS icmp timing
S Chassis(su-config-probe-timing)->packet-option ip-tos 5
```

receive

Uses this command to configure the length of time to wait for an ICMP echo reply.

Syntax

receive *milliseconds*

no receive *milliseconds*

Parameters

millisecs	Specifies the time to wait in milliseconds. Value can range from 50 to 29900 milliseconds. This value MUST be less than the transmit rate set with the interval command. Default is 1000 ms.

Defaults

1000 milliseconds.

Mode

Timing probe configuration mode.

Usage

This wait time must be less than the transmit rate time. If you want to change the transmit rate time to a value smaller than the current receive wait time, change the receive wait time first, before changing the tranmit rate, as shown in the second example below.

The **no** form of this command returns the wait time to the default of 1000 milliseconds.

Examples

This example sets the transmit rate to 1500 milliseconds and the receive wait time to 500 milliseconds.

```
S Chassis(su)->configure
S Chassis(su-config)->probe ICMP_STATS icmp timing
S Chassis(su-config-probe-timing)->interval 1500
S Chassis(su-config-probe-timing)->receive 500
```

This example shows how to change the transmit rate and receive wait time when the current receive wait time is the default of 1000 ms and the desired transmit rate is 900 ms.

```
S Chassis(su)->configure
S Chassis(su-config)->probe ICMP_STATS icmp timing
S Chassis(su-config-probe-timing)->receive 500
S Chassis(su-config-probe-timing)->interval 900
```

Tracked Object Commands

Tracked objects monitor the state of local entities, such as interfaces and are used by client applications such as the Link-State application.

For information about...	Refer to page...
track	22-25

For information about...	Refer to page...
delay	22-26
description	22-26
inservice	22-27
port	22-28
threshold count	22-28
show track	22-29

track

Use this command to create a tracked object and enter tracked object configuration mode.

Syntax

track *track-name* **port-group**

no track *track-name* **port-group**

Parameters

track-name	Specifies the name of the tracked object. Value is a character string from 1 to 31 characters long.
port-group	Specifies that the tracked object is a port group type of tracked object.

Defaults

None.

Mode

Global configuration.

Usage

The port group tracked object allows you to monitor the line protocol status of a group of ports. After you execute this command, you enter tracked object configuration mode where you can further configure the tracked object.

The **no** form of the command deletes the tracked object from the Tracked Object Manager.

Example

This example creates the port group tracked object named ls_group and enters tracked object configuration mode.

```
S Chassis(su)->configure
S Chassis(su-config)->track ls_group port-group
S Chassis(su-config-track-obj)->
```

delay

Use this command to configure the amount of time to wait prior to informing the client applications of the state change.

Syntax

delay {[**up** *secs*]|[**down** *secs*]}

no delay {[**up** *secs*]|[**down** *secs*]}

Parameters

up *secs*	Specifies the number of seconds that the tracked object should wait before informing the client application of an "up" status change. The value of *secs* can range from 1 to 180 seconds. The default value is 3.
down *secs*	Specifies the number of seconds that the tracked object should wait before informing the client application of a "down" status change. The value of *secs* can range from 1 to 180 seconds. The default value is 3.

Defaults

At least one parameter must be entered, but either one of the parameters or both can be specified.

The default value is 3 seconds for both "up" and "down" status change timers.

Mode

Tracked object configuration mode.

Usage

The **no** form of the command returns the notification timers to their default values of 3 seconds.

Example

The following example changes the notification timer values for port group tracked object named ls_group to 5 seconds.

```
S Chassis(su)->configure
S Chassis(su-config)->track ls_group port-group
S Chassis(su-config-track-obj)->delay up 5 down 5
```

description

Use this command to add a description to the tracked object.

Syntax

description *string*

no description *string*

Parameters

string	Enter a string of up to 127 characters in length to describe this tracked object. If the string includes spaces, enclose the string in quotes.

Defaults

None.

Mode

Tracked object configuration mode.

Usage

The **no** form of the command deletes the description. The tracked object description is displayed with the **show track** *tracked-obj* **detail** command.

Example

The following example adds a description to port group tracked object named ls_group.

```
S Chassis(su)->configure
S Chassis(su-config)->track ls_group port-group
S Chassis(su-config-track-obj)->description "link-state group1"
```

inservice

Use this command to enable the tracked object.

Syntax

inservice

no inservice

Parameters

None.

Defaults

None.

Mode

Tracked object configuration mode.

Usage

Use the **no inservice** command to set the tracked object to not-in-service. Tracked object configuration remains unchanged. Use the **no track** command to delete a tracked object. A tracked object is not enabled by default.

Example

The following example creates the port group tracked object named ls_group, changes the notification timer values to 5 seconds, adds a description and ports to the group, then enables the object.

```
S Chassis(su)->configure
S Chassis(su-config)->track ls_group port-group
S Chassis(su-config-track-obj)->delay up 5 down 5
S Chassis(su-config-track-obj)->description "link-state group1"
S Chassis(su-config-track-obj)->port ge.1.1-5
S Chassis(su-config-track-obj)->inservice
```

port

Adds one or more ports to the port group tracked object.

Syntax

port *port-string*

no port *port-string*

Parameters

port-string	Adds one or more ports to the port group tracked object. These ports will be monitored by the tracked object.

Defaults

None.

Mode

Tracked object configuration mode.

Usage

This command is valid for port group tracked objects only. It specifies the ports to be monitored by the port group tracked object.

Use the **no** form of the command to remove ports from the tracked object.

Example

This example creates the port group tracked object named ls_group, changes the notification timer values to 5 seconds, adds a description, and then adds ports to be monitored to the group.

```
S Chassis(su)->configure
S Chassis(su-config)->track ls_group port-group
S Chassis(su-config-track-obj)->delay up 5 down 5
S Chassis(su-config-track-obj)->description "link-state group1"
S Chassis(su-config-track-obj)->port ge.1.1-5
```

threshold count

Use this command to set the port group threshold counts which control the up and down state of the port group tracked object.

Syntax

threshold count {[**up** *count*]|[**down** *count*]}

no threshold count {[**up** *count*]|[**down** *count*]}

Parameters

up *count*	Set the tracked object state to UP when the number of UP ports is greater than or equal to this *count* value. Value can range from 1 to 255. Default is 1. The **up** count must be greater than the **down** count.
down *count*	Set the tracked object state to DOWN when the number of UP ports is less than or equal to this *count* value. Value can range from 0 to 254. Default is 0. The **down** count must be smaller than the **up** count.

Defaults

Up count default is 1. Down count default is 0.

Mode

Tracked object configuration mode.

Usage

This command is valid for port group tracked objects only. The tracked object changes to the "up" state if the number of ports "up" is greater than or equal to the **up** *count*. The tracked object changes to the "down" state if the number of ports "up" is less than or equal to the **down** *count*.

By default, the port group is "up" if there is at least one port up.

The **up** count must be larger than the **down** count.

Example

This example changes the threshold counts to port group tracked object ls_group.

```
S Chassis(su)->configure
S Chassis(su-config)->track ls_group port-group
S Chassis(su-config-track-obj)->threshold count up 3 down 2
```

show track

Use this command to display information about all tracked objects or a specific tracked object.

Syntax

show track [*track-name* [**detail**]]

Parameters

track-name	(Optional) Identifies a specific tracked object to display.
detail	(Optional) Specifies to display detailed information about the identified tracked object.

Defaults

If no tracked object is specified, information about all tracked objects is displayed.

If detail is not specified, high-level information about the tracked object is displayed.

Mode

All command modes.

Examples

This example displays information about all tracked objects.

```
S Chassis(su)->show track
Track name                      Type Object (truncated)   Status    Last Change
------------------------------- ---- -------------------- --------- ------------
ls_group                        Port ge.1.1-5             Disabled      2h13m23s

Displayed 1 tracked objects
```

This example displays detailed information about port group tracked object ls_group.

```
S Chassis(su)->show track ls_group detail

Description: link-state group1
Track ls_group
 Port-Group ge.1.1-5
  5 ports used
  threshold up 3, down 2
  speed 0 [aggregate]
 Status is Disabled
  1 changes, last change  2h13m43s
 Delay up 5 seconds, down 5 seconds
Registrants:
  Link-state

Displayed 1 tracked objects
```

23

Bidirectional Forwarding Detection Commands

This chapter describes the Bidirectional Forwarding Detection (BFD) set of commands and how to use them. For information about configuring 802.1x, refer to the "Bidirectional Forwarding Detection Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show probe	23-1
probe bfd	23-1
bfd	23-2
bfd probe	23-3
control	23-3
demand-mode	23-4
description	23-5
echo-mode	23-6
echo	23-6
inservice	23-7
slow-timer	23-8

show probe

Use the probe display commands to display probe configuration and statistics.

Probe display commands are detailed in Chapter 22, **Tracked Object Manager Commands** as follows:

- "show probe" on page 22-13
- "show probe session" on page 22-16
- "show probe default" on page 22-17

probe bfd

Use this command to create a BFD probe and enter probe configuration mode.

Syntax

probe *probe-name* **bfd**

no probe *probe-name* **bfd**

Parameters

probe-name	Specifies a BFD probe name. Valid values are up to 31 characters. The space character is not supported.

Defaults

None.

Mode

Global configuration.

Usage

Probe names are case sensitive.

Use the **no probe** command to delete the specified probe.

Examples

This example enters configuration mode for a BFD probe named **bfdProbe1**:

```
S Chassis(su)->configure
S Chassis(su-config)->probe bfdProbe1 bfd
S Chassis(su-config-probe-bfd)->
```

bfd

Use this command to direct OSPF to create BFD sessions for its neighbors on the specified interface.

Syntax

bfd interface *interface-name*

no bfd interface *interface-name*

Parameters

interface *interface-name*	Specifies that OSPF creates BFD sessions for its neighbors on the specified interface

Defaults

None.

Mode

OSPF router configuration.

Usage

Use the **no bfd** command to disable the creation of BFD sessions for its neighbors in the specified interface context and closes any existing BFD probe sessions for the interface removed.

Examples

This example enters OSPF router configuration **1** and configures OSPF to create BFD sessions for its neighbors on all VLAN interfaces:

```
S Chassis(su)->configure
S Chassis(su-config)->router ospf 1
S Chassis(su-config-ospf-1)->bfd interface vlan.0.*
S Chassis(su-config-ospf-1)->
```

bfd probe

Use this command to configure the BFD probe for neighbors connected to this interface.

Syntax

bfd probe {**default** | *probe-name*}

no bfd probe {**default** | *probe-name*}

Parameters

default	Specifies that the BFD routing protocol default probe ($rte_default) should be used in this interface context.
probe-name	Specifies the name of the BFD probe to use in this interface context.

Defaults

None.

Mode

Interface configuration mode.

Usage

Use the “no” option to remove the BFD probe from this OSPF enabled interface context.

Examples

This example shows how to use the BFD probe bfdProbe1 on the VLAN 1 interface:

```
S Chassis(rw)->
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->bfd probe bfdProbe1
```

control

Use this command to configure BFD Control packet parameters.

Syntax

control {**min-tx** *interval* | **min-rx** *interval* | **multiplier** *number*}

no control {**min-tx** | **min-rx** | **multiplier**}

Parameters

min-tx *interval*	Specifies the minimum interval in 50ms increments between the transmission of BFD Control packets. Valid values are from 50 - 10000ms. The default value is 250ms.
min-rx *interval*	Specifies the minimum interval in 50ms increments between received Control packets the BFD Control sessions can support. Valid values are from 50 - 10000ms. The default value is 250ms.
multiplier *number*	Specifies the value multiplied by the negotiated transmit rate that produces the detection time. Defaults to 4.

Defaults

- The min-tx interval defaults to 250ms
- The min-rx interval defaults to 250ms
- The multiplier defaults to 4

Mode

BFD probe configuration mode.

Usage

The peer will transition the BFD session to the down state if a control packet is not received within the detection time interval that is produced by multiplying the multiplier value and the negotiated transmit rate.

See RFC 5880 for an explanation for minimum transmit and receive settings when Control packets are used in conjunction with the Echo function.

Use the “no” option to reset the specified parameter to its default value.

Examples

This example shows how to set the minimum transmit and receive intervals to 350ms and the minimum number of missed consecutive Control packets to 5 for BFD probe bfdProbe1:

```
S Chassis(rw)->configure
S Chassis(rw-config)->probe bfdProbe1 bfd
S Chassis(su-config-probe-bfd)->control min-tx 350 min-rx 350 multiplier 5
S Chassis(su-config-probe-bfd)->
```

demand-mode

Use this command to enable BFD demand-mode for a session that has been in the up state for the designated time in seconds.

Syntax

demand-mode *up-time*

no demand-mode

Parameters

up-time	Specifies the amount of time a BFD session must remain in the up state before entering BFD mode. Valid values are between 15 - 3600 seconds. The default value is 0 (demand-mode) is disabled.

Defaults

up-time defaults to 0 seconds (demand-mode disabled).

Mode

BFD probe configuration mode.

Usage

The default *up-time* value of 0 can not be administratively entered. Use the “no” option to disable demand mode, resetting the *up-time* to 0.

Examples

This example shows how to enable demand-mode for BFD session bfdProbe1 after the sessions has been up for 60 seconds:

```
S Chassis(rw)->configure
S Chassis(rw-config)->probe bfdProbe1 bfd
S Chassis(su-config-probe-bfd)->demand-mode 60
S Chassis(su-config-probe-bfd)->
```

description

Use this command to define a string that characterizes the probe.

Syntax

description “*string*”

no description

Parameters

string	Specifies a string of up to 127 characters enclosed in double quotes that characterizes the probe.

Defaults

None.

Mode

BFD probe configuration mode.

Usage

Use the “no” option to remove the description associated with this probe.

Examples

This example shows how to associate the “First BDF Probe” string with the bdfProbe1 probe:

```
S Chassis(rw)->configure
S Chassis(rw-config)->probe bfdProbe1 bfd
S Chassis(su-config-probe-bfd)->description “First BDF Probe”
S Chassis(su-config-probe-bfd)->
```

echo-mode

Use this command to enable or disable BFD echo-mode for this BDF session.

Syntax

echo-mode

no echo-mode

Parameters

None.

Defaults

BFD echo-mode is enabled by default.

Mode

BFD probe configuration mode.

Usage

Use the “no” option to disable echo mode.

Examples

This example shows how to disable the Echo function for BFD session **bfdProbe1**:

```
S Chassis(rw)->configure
S Chassis(rw-config)->probe bfdProbe1 bfd
S Chassis(su-config-probe-bfd)->no echo-mode
S Chassis(su-config-probe-bfd)->
```

echo

Use this command to configure echo packet settings.

Syntax

echo {**min-tx** *interval* | **min-rx** *interval* | **miss-count** *number*}

no echo {**min-tx** | **min-rx** | **miss-count**}

Parameters

min-tx *interval*	Specifies the minimum interval in 50ms increments between the transmission of echo packets. Valid values are from 50 - 10000ms. The default value is 250ms.
min-rx *interval*	Specifies the minimum interval in 50ms increments between the transmission of echo packets by the neighbor. Valid values are from 50 - 10000ms. The default value is 250ms.
miss-count *number*	Specifies the minimum number of consecutive echo packets that can be missed before the BFD session transitions to down. Valid values are 1 - 100. Defaults to 3 consecutive packets.

Defaults

- The min-tx interval defaults to 250ms
- The min-rx interval defaults to 250ms
- The minimum number of missed consecutive echo packets defaults to 3

Mode

BFD probe configuration mode.

Usage

The “no” option resets echo packet settings to default values.

Examples

This example shows how to set the minimum transmit and receive intervals to **350**ms and the minimum number of missed consecutive echo packets to **5** for BFD probe **bfdProbe1**:

```
S Chassis(rw)->configure
S Chassis(rw-config)->probe bfdProbe1 bfd
S Chassis(su-config-probe-bfd)->echo min-tx 350 min-rx 350 miss-count 5
S Chassis(su-config-probe-bfd)->
```

inservice

Use this command to place the BFD probe in service.

Syntax

```
inservice
no inservice
```

Parameters

None.

Defaults

None.

Mode

BFD probe configuration mode.

Usage

Use the “no” option to take the BFD probe out of service and remove its associated sessions from the scheduling queue.

Examples

This example shows how to place the bfdProbe1 BFD probe in service:

```
S Chassis(rw)->configure
S Chassis(rw-config)->probe bfdProbe1 bfd
S Chassis(su-config-probe-bfd)->inservice
S Chassis(su-config-probe-bfd)->
```

slow-timer

Use this command to configure the BFD slow timer feature to override the Control min-rx value when echo mode is active.

Syntax

slow-timer *interval*

no slow-timer *interval*

Parameters

interval	Specifies the Control min-rx override value in increments of 500ms when echo mode is active. Valid values are 1000 - 10000ms. Default value is 2000ms.

Defaults

The slow timer defaults to 2000ms.

Mode

BFD probe configuration mode.

Usage

The BFD session on the remote peer does not interact with the Echo packets. The Echo function runs by default and is used in conjunction with a slow timer, which reduces the frequency of transmitted Control packets from the remote peer to the local peer.

Use the “no” option to reset the slow-timer value to the default of 2000ms.

Examples

This example shows how to set the slow timer interval to 2500ms for the bfdProbe1 BFD probe:

```
S Chassis(rw)->configure
S Chassis(rw-config)->probe bfdProbe1 bfd
S Chassis(su-config-probe-bfd)->slow-timer 2500
```

```
S Chassis(su-config-probe-bfd)->
```

24

Link-State Application Commands

This chapter provides detailed information for the Link-State application set of commands. For information about configuring the Link-State application, refer to the "Link-State Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
set link-state track	24-1
clear link-state track	24-2
show link-state	24-3

set link-state track

Use this command to associate downstream ports with upstream ports, defined by a tracked object, in order to facilitate link state changes to the operational status of downstream ports due to link state changes by upstream ports.

Syntax

set link-state track *object-name* [**downstream** *port-string*]

Parameters

object-name	Specifies a port-group tracked object.
downstream *port-string*	(Optional) Specifies the downstream ports to associate with the upstream ports defined by the tracked object. Only Ethernet ports are supported.

Defaults

If no downstream ports are specified, none are added to the Link-State application entry.

Mode

Command mode.

Usage

Devices connected to the switch may have failover capabilities that enhance network redundancy, but require an action by the switch to trigger that functionality. The Link-State application provides a facility that triggers link loss on downstream links if the associated upstream links go down.

The Link-State application associates with downstream links, while the upstream links are associated with tracked objects (part of the Tracked Object Manager). If the Tracked Object Manager detects a state change with the upstream links, the Link-State application is informed. If the upstream links are down, the Link-State application brings down the link to the downstream ports, causing link loss. The downstream device reacts to this and initiates its failover capability. Similarly, if the upstream links are up, the Link-State application attempts to bring up the downstream links. There may be other protocols or applications in the system that prevents the link from coming up.

When the Link-State application needs to influence the operational state of the downstream ports, it sets their operational status to down. In order for this feature to function, you must enable the force link down feature with the **set forcelinkdown enable** command. You can display the cause for port operation status down with the **show port operstatuscause** command.

Refer to "Tracked Object Commands" on page 22-24 for details on creating a port-group tracked object for use with the Link-State application.

Example

This example creates a port-group tracked object named ls_group, changes the defaults for delays to the up/down status messages for the object from the Tracked Object Manager, gives it a description, puts it in service, then configures the Link-State application to use that tracked object and associate it with downstream ports.

```
S Chassis(su)->configure
S Chassis(su-config)->track ls_group port-group
S Chassis(su-config-track-obj)->delay up 5 down 5
S Chassis(su-config-track-obj)->description "link-state group1"
S Chassis(su-config-track-obj)->port tg.2.1-4
S Chassis(su-config-track-obj)->inservice
S Chassis(su-config-track-obj)->exit
S Chassis(su-config)->exit
S Chassis(su)->set link-state track ls_group downstream ge.1.1-5
```

clear link-state track

Use this command to remove a tracked object from the Link-State application or to remove downstream ports from a Link-State tracked object entry.

Syntax

clear link-state track *object-name* [**downstream** *port-string*]

Parameters

object-name	Specifies a port-group tracked object.
downstream *port-string*	(Optional) Specifies the downstream ports to remove from the Link-State tracked object entry.

Defaults

If no downstream ports are specified, the Link-State application entry is removed.

Mode

Command mode.

Example

This example removes downstream port ge.1.5 from the Link-State entry for port-group tracked object ls_group.

```
S Chassis(su)->clear link-state track ls_group downstream ge.1.5.
```

show link-state

Use this command to display information about Link-State application entries.

Syntax

show link-state [*object-name* [**detail**]]

Parameters

object-name	(Optional) Specifies the name of the port-group tracked object associated with the Link-State entry to display.
detail	(Optional) Specifies that detailed information should be displayed.

Defaults

If an object-name is not specified, information about all Link-State entries is displayed.

If detail is not specified, only basic information about the specified entry is displayed.

Mode

All command modes.

Examples

This example displays information about Link-State entry ls_group.

```
S Chassis(su)->show link-state ls_group
Link-state name                 State    Object (truncated)       Last Change
------------------------------- -------- ------------------------ -------------
ls_group                        Down     ge.1.1-5                   1d19h03m28s
------------------------------- -------- ------------------------ -------------
Displayed 1 link-state entries
```

This example displays detailed information about Link-State entry ls_group.

```
S Chassis(su)->show link-state ls_group detail

Link-state ls_group
 Ports
  Uplinks: tg.2.1-4
  Downlinks: ge.1.1-5
 State is Down, Last action shutdown downlinks
  3 state changes, last change   1d19h04m39s ago

Displayed 1 link-state entries
```

25

IP SLA Commands

This chapter describes the IP service level agreement (SLA) feature, which provides packet timing measurements to verify the service level on the network layer. For information about configuring IP SLA, refer to the IP SLA chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
sla entry	25-1
collections	25-2
destination	25-3
distribution	25-4
history	25-4
monitor	25-6
sla schedule	25-6
entry	25-7
stop-all	25-8
show sla	25-9
show sla entry detail	25-10
show sla entry distribution	25-11
show sla entry history	25-12
show sla entry summary	25-13
show sla scheduler	25-15
show limits application sla-entry-data	25-15

sla entry

Use this command to enter IP SLA entry configuration mode. This command allows you to create or modify an IP SLA entry.

Syntax

sla entry *entry* **{echo}**

Parameters

entry	The number of the IP SLA entry you want to create or modify. Possible values are 1–8.
echo	The IP SLA entry type. An echo entry measures round-trip delay, packet loss, and packet ordering.

Defaults

None.

Mode

Configuration command.

Usage

You must specify **echo**.

Use the **exit** command to exit IP SLA entry configuration mode.

Example

This example shows how to enter the configuration mode for IP SLA entry 8:

```
S Chassis(su-config)->sla entry 8 echo
S Chassis(su-config-sla)->
```

collections

Use this command to configure the statistical collections for an IP SLA entry.

Syntax

collections *collections*

no collections

Parameters

collections	Specifies the number of tests for which the statistical data is kept. Possible values are 1–10. The default value is 1.

Defaults

None.

Mode

Configuration IP SLA entry mode.

Usage

Each collection keeps the summary of the results and the statistical distribution data. The IP SLA application clears the next collection in preparation for storing the statistics for the new test. Using the default value of one, the application clears the data prior to each test execution.

Use the **no collections** command to reset the value back to the default, one.

Example

This example shows the collections for IP SLA entry 8 set to 2.

```
S Chassis(su-config)->sla entry 8 echo
S Chassis(su-config-sla)->collections 2
```

destination

Use this command to configure the destination host and probe for an SLA entry. You can use the default probe or an ICMP probe configured through the Tracked Object Manager.

Syntax

destination *IP-address* **probe** {**default** | *probe-name*} [**port** *port*]

no destination *IP-address* **probe** {**default** | *probe-name*} [**port** *port*]

Parameters

IP-address	The IPv4 or IPv6 destination address of the ICMP requests.
probe {default | *probe-name***}**	The probe to use for the SLA entry. • default—Use the default ICMP timing probe, $ipsla_default, which is configured with the default ICMP timing probe settings. • *probe name*—Use an ICMP timing probe created in the Tracked Object Manager. For more information about ICMP timing probes, see "probe icmp timing" on page 22-18.
port *port*	(Optional) Specify the port number of the host service.

Defaults

None.

Mode

Configuration IP SLA entry mode.

Usage

Ensure that you set the destination IP address; otherwise, history collections will not return any data.

Use the **no destination** command to reset the IP address and probe values.

Example

This example shows the destination IP address for the ICMP requests set and the probe set to the default probe, $ipsla_default.

```
S Chassis(su-config)->sla entry 8 echo
S Chassis(su-config-sla)->destination 1.1.1.1 probe default
```

distribution

Use this command to distribute the measured round-trip delay statistics for an IP SLA entry.

Syntax

distribution {[**count** *count*] [**interval** *milliseconds*]}

no distribution {[**count** *count*] [**interval** *milliseconds*]}

Parameters

count *count*	(Optional) Specifies the number of distributions to create. Possible values are 0 and 2–5. The default value is 0.
interval *milliseconds*	(Optional) Specifies the time range of each distribution. Possible values are 5–1000 milliseconds. The default value is 25 milliseconds.

Defaults

Any parameter not specified remains at its current value.

Mode

Configuration IP SLA entry mode.

Usage

If the count is 3 and the interval is 10, the first distribution has the range from 0–9 milliseconds, the second distribution has the range from 10–19 milliseconds, and the third distribution has the range from 20–29 milliseconds.

Use the **no distribution** command to reset the distribution count and interval to the default values of **0** attempts for count and **25** milliseconds for interval.

Example

This example shows the distribution count set to 4 and the interval set to 20 milliseconds.

```
S Chassis(su-config)->sla entry 8 echo
S Chassis(su-config-sla)->distribution count 4 interval 20
```

history

Use this command to store timing information for statistical modeling of the network for an IP SLA entry.

Syntax

history ageout *minutes*

history buckets *buckets* {[**samples** *samples*] |[**interval** *seconds*]}

history collections *collections* [**wrap**]

no history ageout

no history buckets

no history collections

Parameters

ageout *minutes*	The amount of time, in minutes, before a history collection is aged out and the memory it used is returned to the free pool. Possible values are 0 and 15–7200 minutes. The default value, 0, indicates that a history collection does not age out. If **ageout** is set to a value other than 0, it is possible to configure a history collection that runs longer than the **ageout** value. In this case, the test will finish running before it ages out.
buckets *count*	The number of storage units for timing information in a history collection. Possible values are 1–50. The default value is 50 buckets.
samples *count*	Indicates that the buckets have a static depth of *n* samples. Possible values are 16–512 samples. The default value is 16 samples.
interval *seconds*	Indicates that the buckets have a timed depth, in seconds. To estimate the depth of a timed bucket, multiply the number of packets per second defined in the probe by the number of seconds represented by the each bucket. Possible values are 30–3600 seconds.
collections *count*	Specifies the number of history collections to maintain. Possible values are 0 and 1–10. The default value, 0, indicates that no collections are kept.
wrap	Indicates whether the storage history wraps when the number of collections exceeds the value of the collection parameter. By default, the collections do not wrap.

Defaults

For the **samples**, **interval** and **wrap** parameters, any parameter not specified remains at its current value.

Mode

Configuration IP SLA entry mode.

Usage

Use the **no** forms of the **history** command to reset the **ageout**, **buckets**, and **collections** parameters to the default values.

The packet timing entry, which is stored in the bucket, comes from the global pool. If the global pool is exhausted, the IP SLA application will not start the test.

If you have not specified a destination IP address for the IP SLA entry and your history settings use the defaults for **ageout** and **wrap**, the test uses a history collection but not data is collected. Also, the resources used by the history collection will not be freed. To free the resources, set the destination IP address and change the value of either **ageout** or **wrap** from the default.

Example

This example shows the ageout, buckets, and collections parameters set.

```
S Chassis(su-config)->sla entry 8 echo
S Chassis(su-config-sla)->history ageout 18
S Chassis(su-config-sla)->history buckets 5 interval 300
S Chassis(su-config-sla)->history collections 2 wrap
```

monitor

Use this command to configure path monitoring.

Syntax

monitor {[hop-count *count*] **[path-count** *count*]}

Parameters

hop-count *count*	The number of hops per path to track. Possible values are 0–8 hops. The default value is one hop.
path-count *count*	The number of ECMP paths to track. Possible values are 0 and 1–4 paths. The default value is zero paths.

Defaults

Any parameter not specified remains at its current value.

Mode

Configuration IP SLA entry mode.

Usage

The **monitor** command applies only to IP SLA echo entries.

Use the **no** form of the command to reset the **hop-count** and **path-count** parameters to their default values.

Example

This example shows the hop count set to 8 hops and the path count set to 2 paths.

```
S Chassis(su-config)->sla entry 8 echo
S Chassis(su-config-sla)->monitor hop-count 8 path-count 2
```

sla schedule

Use this command to enter IP SLA entry schedule mode. In the schedule mode, you can schedule the IP SLA entries.

Syntax

sla schedule

Parameters

None.

Defaults

None.

Mode

Configuration command.

Usage

If you are currently in the IP SLA entry configuration mode, you must exit the IP SLA entry configuration mode before you can enter the IP SLA entry schedule mode.

You must be in the IP SLA entry schedule mode to schedule IP SLA entries.

Example

This example shows how to enter the IP SLA schedule mode:

```
S Chassis(su-config)->sla schedule
S Chassis(su-config-sla-sched)->
```

entry

Use this command to schedule an IP SLA entry to execute now or at a specific time. You can also set how often a test cycle occurs, the number of tests in a test cycle, the duration of the tests, and the delay between tests.

Syntax

entry *ip-sla-entry* {{[**start** {[**time** <*yyyy-mm-dd:hh.mm.ss*>] | [**now**] | [**after** <*5-300*>]}]} [**duration** <*30-3600*>] [**frequency** <*30-3600*>] [**recurrence** <*120-7776000*>] [**repetitions** <*1-10*>] {[**reset**] | [**stop**]}

Parameters

ip-sla-entry	The IP SLA entry to schedule.
start time <*yyyy-mm-dd:hh.mm.ss*> | **now** | **after** <*5-300*>	Specify the start time. • time—Schedule the entry to begin at a specific time in the following format yyyy-mm-dd:hh.mm.ss • now—Schedule the entry to begin immediately. • after—Schedule the entry to begin after the specified number of seconds.
duration <*30-3600*>	The length, in seconds, of each test in the test cycle. The default value is 30 seconds.
frequency <*30-3600*>	The interval, in seconds, between each test in the test cycle. The default value is 30 seconds

recurrence <*0*, *120-7776000*>	The time, in seconds, between the end of one test cycle and the start of the next test cycle. A value of zero indicates that the test cycle will run only once for the IP SLA entry. A value other than zero means that test cycles will continue until you stop them with either the **reset** or **stop** parameters. The maximum value, 7776000, is 90 days. One day is 86400. See the "Usage" section below for information on how to set the **recurrence** parameter to avoid overlapping test cycles.
repetitions <*1-10*>	The number of tests to run in each test cycle. The default value is 1.
reset	Stop the test cycle and clear the IP SLA entry's schedule attributes.
stop	Stop the test cycle but do not clear the IP SLA entry's schedule attributes.

Defaults

Any parameter not specified remains at its current value.

Mode

IP SLA Entry Schedule Configuration.

Usage

If you change the value of **recurrence** from the default, you may inadvertently schedule the new test cycle to begin while the current test cycle is still running. Overlapping test cycles are skipped.

To avoid this from happening, ensure that the **recurrence** value is greater than the run time of a test cycle (**repetitions** * (**duration** + **frequency**)).

For example, if an IP SLA entry is scheduled for two repetitions with a duration of 60 seconds and a frequency of 30 seconds, the run time of the test cycle 180 seconds. To avoid overlapping test cycles, you must set the value of **recurrence** to greater than 180 seconds.

If the specify the start time using the **now** or **after** options, the running config will display the start time in the yyyy-mm-dd:hh.mm.ss format.

Example

This example shows how that the test cycles of the IP SLA entry 2 are scheduled to begin 60 seconds after the command is entered. Each test cycle will include five tests that are each 60 seconds long. The interval between the tests in the test cycle is set to 60 seconds. The next test cycle will begin one second after the current test cycle ends.

```
S Chassis(su-config)->sla schedule
S Chassis(su-config-sla-sched)->entry 2 start after 60 recurrence 601 duration 60
repetitions 5 frequency 60
```

stop-all

Use this command to stop all scheduled tests.

Syntax

```
stop-all
```

Parameters

None.

Defaults

None.

Mode

Configuration IP SLA schedule mode.

Usage

The **stop-all** command resets the start time for all scheduled IP SLA entries to zero. The other schedule attributes for the IP SLA entries remain unchanged.

Example

This example shows how to stop all scheduled tests.

```
S Chassis(su-config)->sla schedule
S Chassis(su-config-sla-sched)->stop-all
```

show sla

Use this command to display a summary of the configuration and scheduler state of all IP SLA entries or the specified IP SLA entry.

Syntax

show sla

show sla entry *entry*

Parameters

entry	The number of the IP SLA entry for which you want to display configuration and scheduler state information.

Defaults

None.

Mode

All command modes.

Example

```
S Chassis(su)->sh sla
-------------------------------------------------------------------------------
   | Scheduler                    | Statistics   | Storage-History | Path
Id | State    Time                | Col Distrib  | Col Buckets     | Cnt Hops
-------------------------------------------------------------------------------
1  | Queued   2012-10-11:18.39.25 |  5 0/25   ms |  5  15/16    smp|  2   6
```

```
2  | Running  2012-10-11:20.00.12 |  2 0/25   ms |  0  15/16    smp|  2   4
-------------------------------------------------------------------------------
S Chassis(su)->
```

show sla entry detail

Use this command to display the configuration and scheduling information of the selected IP SLA entry.

Syntax

show sla entry *entry* **detail**

Parameters

entry	The number of the IP SLA entry.

Defaults

None.

Mode

All command modes.

Example

```
S Chassis(su)->show sla entry 2 detail

Entry:                              2  Type:                              echo
Collections:                        2  Probe:                       sla-timing1
Destination:                3504::1

Distribution count:                 0  Distribution interval (ms):         25
History collections:                0  History wrap:                       off
History bucket count:              15  History ageout (minutes):            0
History bucket type:           static  History bucket depth (samples):     16
Monitor path count:                 2  Monitor hop count                    4

Scheduling
Start-time:      2012-10-11:20.00.12  Recurrence (seconds):              300
Repetitions:                        2  Duration (seconds):                120
Frequency (seconds):               30  State:                         Running

Status:
  Test 2 of 2 ends in 89 seconds

Displayed 1 sla entry
```

show sla entry distribution

Use this command to display statistical distribution data for a selected SLA entry.

Syntax

show sla entry *entry* **distribution** [**collection** *collection* [**destination** destination | **path** *path* [**hop** *hop*]]]

Parameters

entry	The number of the IP SLA entry.
collection *collection*	Display the data for the specified collection.
destination *destination*	Display the data for the specified destination.
path *path*	Display the data for the specified path.
hop *hop*	Display the data for the specified hop.

Defaults

None.

Mode

All command modes.

Usage

To specify a hop for a collection, you must also specify a path.

Example

```
S Chassis(su)->show sla entry 3 distribution
Entry number: 3                    Type: echo

Collection: 1
Start-time: 2012-11-15:21.16.30
* Destination Host: 192.3.254.1
  Total samples: 20
  Round-trip-time
   Id Range(ms)  Samples    Min      Max      Sum          Sum-of-squares
   1  0-4        15         2.502    4.963    60.308       249.720166
   2  5-9        5          5.119    5.641    27.009       146.48759
   3  10-14      0          0.000    0.000    0.000        0.000
   4  15-19      0          0.000    0.000    0.000        0.000
   5  20+        0          0.000    0.000    0.000        0.000
```

show sla entry history

Use this command to display statistical history data for the selected IP SLA entry.

Syntax

show sla entry *entry* **history** [**collection** *collection* [**destination** destination | [**path** *path* [**hop** *hop* **[bucket** *bucket*]]]]]

Parameters

entry	The number of the IP SLA entry.
collection *collection*	Display the data for the specified collection.
destination *destination*	Display the data for the specified destination.
path *path*	Display the data for the specified path.
hop *hop*	Display the data for the specified hop.
bucket *bucket*	Display the data for the specified bucket.

Defaults

None.

Mode

All command modes.

Usage

To specify a bucket for a collection, you must also specify a path and a hop.

Example

```
S Chassis(su)->show sla entry 1 history collection 1
Entry number: 1                          Type: Echo

Collection: 1
  Start-time: 2012-11-15:21.39.25
* Destination Host
      IP4: 192.8.255.1
~     Bucket: 1
        Start-time: 2012-11-15:21.39.28
        RTT:  min 8.175, avg 9.568, max 11.672 (ms)
              smpls 10, sum 95.689, sum-of-squares 924.753729 (ms)
        PKT: out-of-order 0, missing 0, late-arrivals 0
~     Bucket: 2-15 [No Data]
+ Path 1
-   Hop 1
      IP4: 192.1.254.1
~     Bucket: 1
        Start-time: 2012-11-15:21.39.26
        RTT:  min 1.059, avg 2.016, max 2.925 (ms)
```

```
                smpls 11, sum 22.178, sum-of-squares 47.775388 (ms)
          PKT: out-of-order 0, missing 0, late-arrivals 0
~       Bucket: 2-15 [No Data]
-     Hop 2
        IP4: 192.1.255.2
~       Bucket: 1
          Start-time: 2012-11-15:21.39.28
          RTT:  min 1.791, avg 3.065, max 4.501 (ms)
                smpls 10, sum 30.652, sum-of-squares 99.556186 (ms)
          PKT: out-of-order 0, missing 0, late-arrivals 0
~       Bucket: 2-15 [No Data]
-     Hop 3
        IP4: 192.2.254.1
~       Bucket: 1
          Start-time: 2012-11-15:21.39.26
          RTT:  min 2.633, avg 3.818, max 5.448 (ms)
                smpls 11, sum 42.004, sum-of-squares 168.862624 (ms)
          PKT: out-of-order 0, missing 0, late-arrivals 0
~       Bucket: 2-15 [No Data]
.
.
.
```

show sla entry summary

Use this command to display statistical summary data for a selected SLA entry.

Syntax

show sla entry *entry* **summary** [**collection** *collection* [destination destination | **path** *path* [**hop** *hop*]]]

Parameters

entry	The number of the IP SLA entry.
collection *collection*	Display the data for the specified collection.
destination *destination*	Display the data for the specified destination.
path *path*	Display the data for the specified path.
hop *hop*	Display the data for the specified hop.

Defaults

None.

Mode

All command modes.

Usage

To specify a hop for a collection, you must also specify a path.

Example

```
S Chassis(su)->show sla entry 2 summary collection 1
Entry: 2 (echo)

Collection: 1
Start-time: 2012-11-15:21.10.12
* Destination Host
      IP6: 3504::1
      RTT: min 1.393, avg 1.538, max 1.775 (ms)
           smpls 21, sum 32.298, sum-of-squares 49.862438
      PKT: out-of-order 0, missing 0, late-arrivals 0

+ Path  1
-   Hop  1
      IP6: 3001::1
      RTT: min 1.645, avg 1.956, max 2.815 (ms)
           smpls 21, sum 41.095, sum-of-squares 82.204263
      PKT: out-of-order 0, missing 0, late-arrivals 0
-   Hop  2
      IP6: 3501::2
      RTT: min 0.902, avg 0.975, max 1.067 (ms)
           smpls 21, sum 20.495, sum-of-squares 20.40115
      PKT: out-of-order 0, missing 0, late-arrivals 0
-   Hop  3
      IP6: 3002::1
      RTT: min 0.832, avg 2.356, max 3.351 (ms)
           smpls 21, sum 49.486, sum-of-squares 127.90960
      PKT: out-of-order 0, missing 0, late-arrivals 0
-   Hop  4
      IP6: 3502::2
      RTT: min 0.693, avg 0.956, max 1.784 (ms)
           smpls 21, sum 20.095, sum-of-squares 20.891499
      PKT: out-of-order 0, missing 0, late-arrivals 0
+ Path  2
-   Hop  1
      IP6: 21::1
      RTT: min 1.219, avg 1.814, max 2.194 (ms)
           smpls 21, sum 38.098, sum-of-squares 70.798048
      PKT: out-of-order 0, missing 0, late-arrivals 0
.
.
```

.

show sla scheduler

Use this command to display the schedule information for the IP SLA entries.

Syntax

show sla scheduler

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

```
S Chassis(su)->show sla scheduler

   Attributes            Scheduler
Id Rec.   Dur. Rep Freq  State     Status
-- ------ ---- --- ----  --------- ----------------------------------------
1  1800   300  5   60    Queued    Cycle begins in 120 seconds
2  300    120  2   30    Running   Test 2 of 2 starts in 19 seconds
```

show limits application sla-entry-data

Use this command to display the number of resources left.

Syntax

show limits application sla-entry-data

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

The number of statistical entry resources required to start the test is dependent on the distribution count, number of paths and hops, and the number of history buckets. The calculation is as follows:

(distribution count + history buckets) * (paths + hops + 1)

If the value of this calculation is less than the number of resources available, the test will start.

Example

This example shows how to display the number of resources left.

```
S Chassis(su)->show limits application sla-entry-data

Application: sla-entry-data
Description: The number of objects that store round-trip-time and jitter data

VRF NAME                              limit   in use reserved
------------------------------- -------- -------- --------
global                                30000      228        0
x                                     30000      228        0
y                                     30000      228        0


Chassis Total Resources .............      30000
Chassis Total Reserved  .............          0
Chassis Total Reserved Available ....          0
Chassis Total Unreserved Available ..      29316
```

26

Port Configuration Commands

This chapter provides detailed information for the port configuration set of commands. For information about configuring ports, refer to the "Port Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show console	26-2
set console	26-3
clear console	26-5
show forcelinkdown	26-6
set forcelinkdown	26-6
clear forcelinkdown	26-7
show port	26-7
set port	26-8
show port advertise	26-8
set port advertise	26-10
clear port advertise	26-10
show port alias	26-11
set port alias	26-12
show port counters	26-13
show port duplex	26-15
set port duplex	26-15
show port energy-eff-eth	26-16
set port energy-efficient-eth	26-17
show port flowcontrol	26-18
set port flowcontrol	26-19
show port ingress-filter	26-19
set port ingress-filter	26-20
show port jumbo	26-21
set port jumbo	26-22
clear port jumbo	26-23

For information about...	Refer to page...
set port jumbo mtu	26-23
clear port jumbo mtu	26-24
show port mdix	26-25
set port mdix	26-25
clear port mdix	26-26
show port negotiation	26-26
set port negotiation	26-27
show port oam	26-27
set port oam status	26-31
set port oam mode	26-32
set port oam loopback-rx	26-32
set port oam remote-loopback	26-33
set port oam notify-retry	26-34
clear port oam	26-35
set port oam link-monitor	26-36
clear port oam link-monitor	26-38
show oam uld-config	26-40
set port oam uld mode	26-41
set port oam uld action	26-43
set port oam uld fast-timer	26-43
clear port oam uld	26-44
show port operstatuscause	26-45
show port speed	26-47
set port speed	26-48
show port status	26-48
show port transceiver	26-50

show console

Use this command to display properties set for one or more console ports.

Syntax

show console [**baud**] [**bits**] [**flowcontrol**] [**parity**] [**stopbits**] [*port-string*]

Parameters

baud	Displays the input/output baud rate.
bits	Displays the number of bits per character.
flowcontrol	Displays the type of flow control.

parity	Displays the type of parity.
stopbits	Displays the number of stop bits.
port-string	(Optional) Displays properties for specific console port(s).

Defaults

If a property is not specified, all properties will be displayed. If *port-string* is not specified, all properties or the specified property for all console ports will be displayed.

Mode

All command modes.

Examples

This example shows how to display properties for all console ports:

```
S Chassis(rw)->show console

Port          Baud    Flow    Bits  StopBits    Parity
------------  ------  ------  ----  ----------  ------
com.1.1       9600    ctsrts  8     one         none
com.2.1       9600    ctsrts  8     one         none
com.3.1       9600    ctsrts  8     one         none
```

This example shows how to display properties for console port com.1.1:

```
S Chassis(rw)->show console com.1.1

Port          Baud    Flow    Bits  StopBits    Parity
------------  ------  ------  ----  ----------  ------
com.1.1       38400   ctsrts  8     one         none
```

This example shows how to display the bits property for console port com.1.1:

```
S Chassis(rw)->show console bits com.1.1

Port          Bits
------------  --------
com.1.1       8
```

set console

Use this command to set the properties for one or more console ports.

Syntax

set console {[**baud** *rate*] | [**bits** *num-bits*] | [**cts-link** {**enable** | **disable**}] | [**flowcontrol** {**none** | **ctsrts** | **dsrdtr**}] | [**parity** {**none** | **odd** | **even** | **mark** | **space**}] | [**stopbits** {**one** | **oneandhalf** | **two**}][**vt100 dsr** {**enable** | **disable** | **timeout** *timeout*]} [*port-string*]

Parameters

rate	Sets the console baud rate. Valid values are: **300**, **600**, **1200**, **2400**, **4800**, **9600**, **14400**, **19200**, **38400**, **57600**, **115200**, **230400**. Default value: **9600**.
num-bits	Specifies the number of bits per character. Valid values are **5**, **6**, **7**, and **8**. Default value: **8**.
flowcontrol {**none** | **ctsrts** | **dsrdtr**}	Sets flowcontrol as follows: • **none** disables all hardware flow control, or specifies that no parity checking will be performed. • **ctsrts** enables CTS/RTS (Clear to Send/Request to Send) hardware flow control. • **dsrdtr** enables DSR/DTR (Data Set Ready/Data Terminal Ready) hardware flow control. Default value: **ctsrts**.
odd | **even** | **mark** | **space**	Enables odd, even mark or space parity checking.
one | **oneandhalf** | **two**	Sets stop bits per character to 1, 1.5 or 2.
vt100 dsr	Sets the Device Status Request (DSR) status for the VT100 console: • enable – Enables DSR for the VT100 • disable – Disables DSR for the VT100 • *timeout* – Sets the number of seconds to wait for a VT100 DSR response from the terminal.
port-string	(Optional) Sets baud rate for specific port(s).

Defaults

If *port-string* is not specified, the property value specified will be set for all console ports.

Mode

All command modes. The **vt100 dsr** option is only available in Super-User management access mode when the security profile is set to C2.

Usage

If C2 security mode is enabled, You can not create, modify, or clear a console configuration while in Read-Write user mode.

Examples

This example shows how to set the baud rate to 19200 on console port com.1.1:

```
S Chassis(rw)->set console baud 19200 com.1.1
```

This example shows how to set the bits property value to 8 on all console ports:

```
S Chassis(rw)->set console bits 8
```

This example shows how to set the flowcontrol property value to none on console port com.1.1:

```
S Chassis(rw)->set console flowcontrol none com.1.1
```

This example shows how to set the parity property value to even on all ports:

```
S Chassis(rw)->set console parity even
```

This example shows how to set the stopbits property value to one on console ports com.1.1 and com.1.2:

```
S Chassis(rw)->set console stopbits one com.1.1-2
```

clear console

Use this command to clear the properties set for one or more console ports to its default value.

Syntax

clear console [**baud**] [**bits**] [**flowcontrol**] [**parity**] [**stopbits**] [*port-string*]

Parameters

baud	Clears the input/output baud rate.
bits	Clears the number of bits per character.
cts-link	Sets CTS link detection to the default value of enabled.
flowcontrol	Clears the type of flow control.
parity	Clears the type of parity.
stopbits	Clears the number of stop bits.
vt100	Clears the Device Status Request (DSR) status for the VT100 console.
port-string	(Optional) Clears properties for specific console port(s).

Defaults

If no property is specified, all property values are reset to the default value. If *port-string* is not specified, all or the specified property for all console ports will be cleared.

Mode

All command modes.

Usage

If C2 security mode is enabled, You can not clear a console configuration while in Read-Write user mode.

Example

This example shows how to clear the baud rate on console port com.1.1:

```
S Chassis(rw)->clear console baud com.1.1
```

This example shows how to clear the bits property on all console ports:

```
S Chassis(rw)->clear console bits
```

This example shows how to clear the flowcontrol property value console port com.1.1:

```
S Chassis(rw)->clear console flowcontrol com.1.1
```

This example shows how to clear the parity property value on all ports:

```
S Chassis(rw)->clear console parity
```

This example shows how to clear the stopbits property value on console ports com.1.1 and com.1.2:

```
S Chassis(rw)->clear console stopbits one com.1.1-2show console
```

show forcelinkdown

Use this command to display the status of the force link down function.

Syntax

show forcelinkdown

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the status of the force link down function:

```
S Chassis(rw)->show forcelinkdown
ForceLinkDown feature is globally enabled
```

set forcelinkdown

Use this command to enable or disable the force link down function.

Syntax

set forcelinkdown {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables the force link down function on all ports.

Defaults

None.

Mode

All command modes.

Usage

When enabled, this command forces ports in the “operstatus down” state to become disabled.

When force linkdown is enabled, disabling a port using the **set port disable** command will not disable PoE on that port.

Example

This example shows how to enable the force link down function:

```
S Chassis(rw)->set forcelinkdown enable
```

clear forcelinkdown

Use this command to resets the force link down function to the default state of disabled.

Syntax

clear forcelinkdown

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the force link down function to disabled:

```
S Chassis(rw)->clear forcelinkdown
```

show port

Use this command to display whether or not one or more ports are enabled for switching.

Syntax

show port [*port-string*]

Parameters

port-string	(Optional) Displays operational status for specific port(s). For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, operational status information for all ports will be displayed.

Mode

All command modes.

Examples

This example shows how to display operational status information for GbE port 14 in module 3:

```
S Chassis(rw)->show port ge.3.14
Port ge.3.14 enabled
```

set port

Use this command to administratively enable or disable one or more ports.

Syntax

set port {**enable** | **disable**} *port-string*

Parameters

enable | **disable**	Enables or disables the specified port(s). Default value: port state disabled.
port-string	Specifies the port(s) to enable or disable. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Usage

When force linkdown (see "set forcelinkdown" on page 26-6) is enabled, disabling a port using the **set port disable** command will not disable PoE on that port.

Example

This example shows how to disable port ge.1.1:

```
S Chassis(rw)->set port disable ge.1.1
```

show port advertise

Use this command to display the advertised ability on one or more ports.

Syntax

show port advertise [*port-string*]

Parameters

port-string	(Optional) Displays advertised ability for specific port(s).

Defaults

If *port-string* is not specified, advertised ability for all ports will be displayed.

Mode

All command modes.

Example

This example shows how to display the advertised operational abilities of port:

```
S Chassis(rw)->show port advertise ge.4.36
ge.4.36      capability   advertised    remote
-------------------------------------------
10BASE-T         yes          yes          no
10BASE-TFD       yes          yes          no
100BASE-TX       yes          yes          no
100BASE-TXFD     yes          yes          no
1000BASE-X       no           no           no
1000BASE-XFD     no           no           no
1000BASE-T       no           no           no
1000BASE-TFD     yes          yes          no
other            no           no           yes
pause            yes          no           no
Apause           yes          no           no
Spause           yes          no           no
Bpause           yes          yes          no
```

Table 26-1 provides an explanation of the command output.

Table 26-1 show port advertise Output Details

Output...	What it displays...
capability	Whether or not the port is capable of operating in the following modes: • **10BASE-T** - 10BASE-T half duplex mode • **10BASE-TFD** - 10BASE-T full duplex mode • **100BASE-TX** - 100BASE-TX half duplex mode • **100BASE-TXFD** - 100BASE-TX full duplex mode • **1000BASE-X** - 1000BASE-X, -LX, -SX, -CX half duplex mode • **1000BASE-XFD** - 1000BASE-X, -LX, -SX, -CX full duplex mode • **1000BASE-T** - 1000BASE-T half duplex mode • **1000BASE-TFD** - 1000BASE-T full duplex mode • **other** - Other modes. • **pause** - PAUSE for full-duplex links • **apause** - Asymmetric PAUSE for full-duplex links • **spause** - Symmetric PAUSE for full-duplex links • **bpause** - Asymmetric and Symmetric PAUSE for full-duplex links
advertised	Whether or not the port is configured to advertise it is capable of operating in the modes listed.
remote	Whether this port's link partner is advertising the listed mode.

set port advertise

Use this command to configure the auto-negotiation advertised capabilities on one or more ports.

Syntax

set port advertise *port-string* {[**10t**] [**10tfd**] [**100tx**] [**100txfd**] [**1000x**] [**1000xfd**] [**1000t**] [**1000tfd**] [**pause**] [**apause**] [**spause**] [**bpause**])

Parameters

port-string	Specifies the port(s) for which to set advertised ability.
10t	(Optional) Advertises 10BASE-T half duplex mode.
10tfd	(Optional) Advertises 10BASE-T full duplex mode.
100tx	(Optional) Advertises 100BASE-TX half duplex mode.
100txfd	(Optional) Advertises 100BASE-TX full duplex mode.
1000x	(Optional) Advertises 1000BASE-X, -LX, -SX, -CX half duplex mode.
1000xfd	(Optional) Advertises 1000BASE-X, -LX, -SX, -CX full duplex mode.
1000t	(Optional) Advertises 1000BASE-T half duplex mode.
1000tfd	(Optional) Advertises 1000BASE-T full duplex mode.
pause	(Optional) Advertises PAUSE for full-duplex links.
apause	(Optional) Advertises asymmetric PAUSE for full-duplex links.
spause	(Optional) Advertises symmetric PAUSE for full-duplex links.
bpause	(Optional) Advertises asymmetric and symmetric PAUSE for full-duplex links.

Defaults

At least one optional parameter must be specified.

Mode

All command modes.

Example

This example shows how to set port ge.3.4 to advertise 1000BASE-TX full duplex operation:

```
S Chassis(rw)->set port advertise ge.3.4 1000txfd
```

clear port advertise

Use this command to reset auto-negotiation advertised capabilities to the default setting on one or more ports.

Syntax

clear port advertise *port-string* [**10t** | **10tfd** | **100tx** | **100txfd** | **1000x** | **1000txfd** | **1000t** | **1000tfd** | **pause** | **apause** | **spause** | **bpause**]

Parameters

port-string	Specifies port(s) for which advertised ability will be reset.
10t	(Optional) Clears 10BASE-T half duplex mode from the port's advertised ability.
10tfd	(Optional) Clears 10BASE-T full duplex mode from the port's advertised ability.
100tx	(Optional) Clears 100BASE-TX half duplex mode from the port's advertised ability.
100txfd	(Optional) Clears 100BASE-TX full duplex mode from the port's advertised ability.
1000x	(Optional) Clears 1000BASE-X, -LX, -SX, -CX half duplex mode from the port's advertised ability.
1000xfd	(Optional) Clears 1000BASE-X, -LX, -SX, -CX full duplex mode from the port's advertised ability.
1000t	(Optional) Clears 1000BASE-T half duplex mode from the port's advertised ability.
1000tfd	(Optional) Clears 1000BASE-T full duplex mode from the port's advertised ability.
pause	(Optional) Clears PAUSE for full-duplex links from the port's advertised ability.
apause	(Optional) Clears asymmetric PAUSE for full-duplex links from the port's advertised ability.
spause	(Optional) Clears symmetric PAUSE for full-duplex links from the port's advertised ability.
bpause	(Optional) Clears asymmetric and symmetric PAUSE for full-duplex links from the port's advertised ability.

Defaults

If not specified, all modes of advertised ability will be cleared.

Mode

All command modes.

Example

This example shows how to reset all advertised ability to default settings on port ge.3.4:

```
S Chassis(rw)->clear port advertise ge.3.4
```

show port alias

Use this command to display alias name(s) assigned to one or more ports.

Syntax

show port alias [*port-string*]

Parameters

port-string	(Optional) Displays alias name(s) for specific port(s).

Defaults

If *port-string* is not specified, aliases for all ports will be displayed.

Mode

All command modes.

Examples

This example shows how to display alias information for ge.1.1. In this case, an alias has been assigned:

```
S Chassis(su)->show port alias ge.1.1
Alias on port ge.1.1 set to:  Documentation.
```

This example shows how to display alias information for ge.3.1. In this case, an alias has not been assigned:

```
S Chassis(rw)->show port alias ge.3.1
Alias not assigned on port ge.3.1.
```

set port alias

Use this command to assign an alias name to a port.

Syntax

set port alias *port-string* [*string*]

Parameters

port-string	Specifies the port to which an alias will be assigned.
string	(Optional) Assigns a text string name to the port.

Defaults

If *string* is not specified, the alias assigned to the port will be cleared.

Mode

All command modes.

Example

This example shows how to assign the alias “Documentation” to ge.1.1:

```
S Chassis(rw)->set port alias ge.1.1 Documentation
```

show port counters

Use this command to display port counter statistics detailing traffic through the device and through all MIB2 network devices.

Syntax

show port counters [*port-string*] [[**switch** | **mib2**] | [**brief** | **packets** | **detail** | **errors**] [**nonzero**]]

Parameters

port-string	(Optional) Displays counter statistics for specific port(s).
switch | **mib2**	(Optional) Displays switch or MIB2 statistics. Switch statistics detail performance of the Extreme Networks switch device. MIB2 interface statistics detail performance of all network devices.
brief	(Optional) Displays a summary of MIB2 counters.
packets	(Optional) Displays high capacity packet counters statistics.
detail	(Optional) Displays all MIB2 counters.
errors	(Optional) Displays error, discard, and unknown protocol counters.
nonzero	(Optional) Displays only ports that have counters with a non-zero value.

Defaults

- If *port-string* is not specified, counter statistics will be displayed for all ports.
- If neither **mib2** nor **switch** are specified, all counter statistics will be displayed for the specified port(s).
- If **brief** is not specified, a standard level of information is displayed.
- If **packets** is not specified, information is displayed for all counters.
- If **detail** is not specified, a standard level of information is displayed.
- If **errors** is not specified, information is displayed for all counters.
- if **nonzero** is not specified, information is displayed for all counters.

Mode

All command modes.

Example

This example shows how to display all counter statistics, including MIB2 network traffic and traffic through the device for ge.3.1:

```
S Chassis(rw)->show port counters ge.3.1

Port: ge.3.1   MIB2 Interface: 1   Bridge Port: 2
No counter discontinuity time
-------------------------------------------------------------------

MIB2 Interface Counters
```

```
----------------------
In Octets                          0
In Unicast Pkts                    0
In Multicast Pkts                  0
In Broadcast Pkts                  0
In Discards                        0
In Errors                          0
In Unknown Protocol                0
Out Octets                         0
Out Unicasts Pkts                  0
Out Multicast Pkts                 0
Out Broadcast Pkts                 0
Out Errors                         0
Out Queue Length                   256

802.1Q Switch Counters
----------------------
Frames Received                    0
Frames Transmitted                 0
Frames Filtered                    0
```

This example shows how to display all ge.1.1 port counter statistics related to traffic through the device.

```
S Chassis(rw)->show port counters ge.1.1 switch

Port: ge.1.1   Bridge Port: 65
No counter discontinuity time
-------------------------------------------------------------------------
Frames Received                  1923736
Frames Transmitted                328967
Frames Filtered                        0

S Chassis(rw)->
```

Table 26-2 provides an explanation of the command output.

Table 26-2 show port counters Output Details

Output...	What it displays...
Port	Port designation.
MIB2 Interface	MIB2 interface designation.
Bridge Port	IEEE 802.1D bridge port designation.
MIB2 Interface Counters	MIB2 network traffic counts for In Octets, Unicast Packets, Broadcast Packets, Discards, Errors, and Unknown Protocol. Counts for Out Octets, Unicasts Packets, Multicast Packets, Broadcast Packets Discards, Errors, and Queue Length.
802.1Q Switch Counters	Counts of frames received, transmitted, and filtered.

show port duplex

Use this command to display the default duplex setting (half or full) for one or more ports.

Syntax

show port duplex [*port-string*]

Parameters

port-string	(Optional) Displays default duplex setting(s) for specific port(s).

Defaults

If *port-string* is not specified, default duplex settings for all ports will be displayed.

Mode

All command modes.

Example

This example shows how to display the default duplex setting for Gigabit Ethernet port 14 in module 3:

```
S Chassis(rw)->show port duplex ge.3.14
default duplex mode is full on port ge.3.14.
```

set port duplex

Use this command to set the default duplex type for one or more ports.

Syntax

set port duplex *port-string* {**full** | **half**}

Parameters

port-string	Specifies the port(s) for which duplex type will be set.
full | **half**	Sets the port(s) to full-duplex or half-duplex operation.

Defaults

None.

Mode

All command modes.

Usage

This command will only take effect on ports that have auto-negotiation disabled.

Example

This example shows how to set Gigabit Ethernet slot 1, port 17 to full duplex:

```
S Chassis(rw)->set port duplex ge.1.17 full
```

show port energy-eff-eth

Use this command to display the Energy Efficient Ethernet (EEE) information for one or more Ethernet ports that support EEE.

Syntax

show port energy-eff-eth [*port-string*]

Parameters

port-string	(Optional) Displays EEE information for specific port(s).

Defaults

If *port-string* is not specified, EEE information for all ports will be displayed.

Mode

All command modes.

Example

This example shows how to display the port flow control state for port range tg.1.1:

```
S Chassis(rw)->show port energy-eff-eth tg.1.1

Port: tg.1.1   MIB2 Interface: 13001
------------------------------------------------------------------------
  Energy Eff Eth Admin State    : Disabled
  Energy Eff Eth LLDP TLV State : Disabled
  Energy Eff Eth Oper State     : Disabled

  Admin Rx Tw    :        5 usecs
  Admin Fb Tw    :       20 usecs

  Local
  ------------------------------
  Tx Tw          :        5 usecs
  Rx Tw          :        5 usecs
  Fallback Rx Tw :       20 usecs

  Echo Tx Tw     :        5 usecs
  Echo Rx Tw     :        5 usecs

  Ready to Tx LLDPDU+EEE TLV    : False
  Ready to Rx LLDPDU+EEE TLV    : False
  EEE negotiation Completed     : False
S Chassis(rw)->
```

set port energy-efficient-eth

Use this command to enable and configure Energy Efficient Ethernet (EEE) on Ethernet ports that support EEE.

Syntax

set port energy-eff-eth *port-string* [**enable** | **disable**] [**wakeup-time** *wakeup-time*] [**fallback-wakeup-time** *fallback-wakeup-time*]

Parameters

enable | **disable**	(Optional) Enables or disables EEE on the specified port(s). EEE is disabled by default.
wakeup-time *wakeup-time*	(Optional) Specifies a wakeup time value in micro-seconds. Default value = **30** for 100 and 1000 Mb ports and **5** for 10000 Mb ports. Valid values are **17** - **1000** for 10 and 100Mb ports and 5 - 1000 for 1000Mb ports.
fallback-wakeup -time *fallback-wakeup-time*	(Optional) Specifies a fallback wakeup time value in micro-seconds. Default value is **17** for 100 and 1000 Mb ports and **20** for 10000 Mb ports.

Defaults

- EEE is disabled by default.
- Wakeup time defaults to **30** micro-seconds for 100 and 1000 Mb ports and **5** micro-seconds for 10000 Mb ports.
- Fallback wakeup time defaults to **17** micro-seconds for 100 and 1000 Mb ports and **20** micro-seconds for 10000 Mb ports.

Mode

All command modes.

Usage

Enabling EEE on a link reduces the power consumption on the Ethernet link during low data activity. EEE must be enabled on both sides of the link to operate. Auto negotiation is restarted when you enable or disable EEE, causing the link to bounce. Link state does not change as a result of an EEE transition to and from a lower level of power. Frames that are in transit are neither dropped nor corrupted during EEE transition to and from a lower level of power.

The wakeup time is the period between the reception of an IDLE signal and the reception of the first data permitted on the interface. It is recommended that you only modify wakeup and fallback values if a longer wakeup time is required. The negotiation of wakeup times ia accomplished using the LLDP EEE TLV which must be enabled on both sides of the link using "set lldp port tx-tlv" on page 20-39. If the configured wakeup time is not acceptable, the fallback wakeup time is used.

Example

This example shows how to enable EEE on port ge.1.5:

```
S Chassis(rw)->set port energy-eff-eth ge.1.5 enable
```

show port flowcontrol

Use this command to display the flow control state for one or more ports.

Syntax

show port flowcontrol [*port-string*]

Parameters

port-string	(Optional) Displays flow control state for specific port(s).

Defaults

If *port-string* is not specified, flow control information for all ports will be displayed.

Mode

All command modes.

Example

This example shows how to display the port flow control state for port range ge.1.1-5:

```
S Chassis(rw)->show port flowcontrol ge.1.1-5

Port         TX Admin  TX Oper RX Admin  RX Oper TX Pause Count RX Pause Count
------------ -------- -------- -------- -------- -------------- --------------
ge.1.1        enabled disabled  enabled disabled              0              0
ge.1.2        enabled disabled  enabled disabled              0              0
ge.1.3        enabled  enabled  enabled  enabled              0              0
ge.1.4        enabled disabled  enabled disabled              0              0
ge.1.5        enabled disabled  enabled disabled              0              0
```

Table 26-3 provides an explanation of the command output.

Table 26-3 show port flow control Output Details

Output...	What it displays...
Port	Port designation.
TX Admin	Whether or not the port is administratively **enabled** or **disabled** for sending flow control frames.
TX Oper	Whether or not the port is operationally **enabled** or **disabled** for sending flow control frames.
RX Admin	Whether or not the port is administratively **enabled** or **disabled** for acknowledging received flow control frames.
RX Oper	Whether or not the port is operationally **enabled** or **disabled** for acknowledging received flow control frames.
TX Pause Count	Number of Pause frames transmitted.
RX Pause Count	Number of Pause frames received.

set port flowcontrol

Use this command to enable or disable flow control settings for one or more ports.

Syntax

set port flowcontrol *port-string* {**receive** | **send** | **both**} {**enable** | **disable**}

Parameters

port-string	Specifies port(s) for which to enable or disable flow control.
receive	Enables or disables the port(s) to receive flow control packets. Receive acknowledges flow control information from its link partner.
send	Enables or disables the port(s) to send flow control packets. Send allows flow control information to be sent to its link partner.
both	Enables or disables the port(s) to receive and send flow control packets. Both allows for the sending and receiving of flow control information with the link partner Default: **both**.
enable | **disable**	Enables or disables flow control settings. Default: **enable**.

Defaults

None.

Mode

All command modes.

Usage

This command only disables flowcontrol for links that have auto-negotiation disabled. Auto-negotiation enabled ports still advertise pause and act on pause according to their advertised abilities in auto-negotiation. To disable pause on an autonegotiation link issue the command "clear port advertise" on page 26-10 for that link specifying apause, bpause, spause, and pause as options to clear.

Example

This example shows how to enable ports ge.3.1 through 5 to send and receive flow control packets:

```
S Chassis(rw)->set port flowcontrol ge.3.1-5 both enable
```

show port ingress-filter

Use this command to display all ingress-filter enabled ports or the ingress-filter state of the specified port(s).

Syntax

show port ingress-filter *port-string*

Parameters

port-string	Specifies the port(s) to display the port ingress-filter state.

Defaults

None.

Mode

All command modes.

Example

This example displays the port ingress-filter state for all ports:

```
S Chassis(rw)->show port ingress-filter
Port          State
------------  --------
host.0.1      enabled
ge.1.1        enabled
ge.1.2        enabled
ge.1.4        enabled
.
.
.
lag.0.59      enabled
lag.0.62      enabled
```

set port ingress-filter

Use this command to limit the forwarding of received frames based on port VLAN egress lists.

Syntax

set port ingress-filter *port-string* {**enable** | **disable**}

Parameters

port-string	Specifies the port(s) to enable or disable for limiting the forwarding of received frames based on port.
enable | **disable**	Enable or disable ingress filtering. Default value: **disable**.

Defaults

None.

Mode

All command modes.

Example

This example shows how to enable ingress-filter on ports ge.1.1-4:

```
S Chassis(rw)->set port ingress-filter ge.1.1-4 enable
```

show port jumbo

Use this command to display the status of jumbo frame support and Maximum Transmission Units (MTU) on one or more ports.

Syntax

show port jumbo [*port-string*]

Parameters

port-string	(Optional) Displays the status of jumbo frame support for specific port(s).

Defaults

If *port-string* is not specified, jumbo frame support status for all ports will display.

Mode

All command modes.

Usage

It is possible for Jumbo Admin Status to be enabled and Jumbo Oper Status to be deferred. Jumbo frame support is supported on all module ports, but some modules can only handle 12 jumbo enabled ports at one time without a reset. Resetting the module will enable deferred ports.

Example

This example shows how to display the status of jumbo frame support for port ge.1.1:

```
S Chassis(rw)->show port jumbo tg.1.1

* Applicable only if port jumbo is enabled

    Port     Oper      Admin      MTU     MTU    MTU    MTU    MTU    MTU   Application
             Status    Status   Dynamic    Min    Max  Oper*  Admin  Delta    Name(size)
---------- -------- -------- -------- ----- ----- ----- ----- ----- ------------
    tg.1.1 Disabled Disabled Disabled  1000 10239 10239 10239     0
Bonded_TOR_14(su)->
```

Table 26-4 provides an explanation of the command output.

Table 26-4 show port jumbo Output Details

Output...	What it displays...
Port	Port for this line of information.
Oper Status	Whether the jumbo frames feature is operationally enabled or disabled for this port.
Admin Status	Whether the jumbo frames feature is administratively enabled or disabled for this port.
MTU Dynamic	Whether the dynamic jumbo MTU feature is enabled or disabled for this port.

Table 26-4 show port jumbo Output Details (continued)

Output...	What it displays...
MTU Min	Minimum MTU supported by the port.
MTU Max	Maximum MTU supported by the port.
MTU Oper	The operational maximum MTU value in bytes for this port.
MTU Admin	The administratively configured maximum MTU value in bytes for this port. This value is only applicable if jumbo MTU is enabled on the port.
MTU delta	Specifies the total additional header bytes added to the maximum MTU size if dynamic jumbo MTU is enabled.
Application Name	Specifies the name(s) of the application(s) for the specified MTU delta, if any.

set port jumbo

Use this command to enable or disable jumbo frame support on one or more ports.

Syntax

set port jumbo {**enable** | **disable**} *port-string*

Parameters

enable | **disable**	Enables or disables jumbo frame support.
port-string	Specifies the port(s) on which to disable or enable jumbo frame support.

Defaults

None.

Mode

All command modes.

Usage

By default, jumbo frame support is disabled on all ports and path MTU discovery is enabled. When jumbo frame support is enabled, path MTU discovery should also be enabled. For details on setting the path MTU state, refer to "set mtu" on page 7-20.

It is possible for the jumbo administrative status to be enabled and the jumbo operational status to be deferred. Jumbo frame support is supported on all module ports, but some modules can only handle 12 jumbo frames enabled ports at one time without a reset. Resetting the module will enable deferred ports.

If jumbo support has not been manually configured, or if no port number is listed when enabling jumbo frame support on a module that only supports 12 jumbo ports, the first 12 ports will be set for jumbo support. Under these circumstances, selection of ports 1 - 12 will not require a reset. If Ports 13 or higher are selected, jumbo resources are withdrawn from ports 1 - 12 and a module reset is required. For these modules, any combination of 12 ports will support Jumbos.

See the "show port jumbo" on page 26-21 to verify the operational status of a jumbo enabled port. A jumbo administratively disabled port will always have a jumbo operational status of disabled. If you have manually enabled the maximum number of ports allowed on the module, and you attempt to enable additional ports, the additional jumbo frame configurations will fail. You must

free up resources by disabling jumbo frames on a port for each additional port you are trying to add before continuing.

By default maximum jumbo MTU is set to 10239 bytes for untagged packets and supports 10243 bytes for tagged packets. This maximum jumbo MTU size can be modified to a value between **1000 – 10239** using "set port jumbo mtu" on page 26-23.

Example

This example shows how to enable jumbo frame support for port ge.3.14:

```
S Chassis(rw)->set port jumbo enable ge.3.14
```

clear port jumbo

Use this command to reset jumbo frame support status to disabled on one or more ports.

Syntax

clear port jumbo *port-string*

Parameters

port-string	Specifies the port(s) on which to reset jumbo frame support status to disabled.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset jumbo frame support status for port ge.3.14:

```
S Chassis(rw)->clear port jumbo ge.3.14
```

set port jumbo mtu

Use this command to set the port jumbo MTU size or enable dynamic jumbo MTU on one or more ports.

Syntax

set port jumbo mtu {**size** *size* | **dynamic** {**enable** | **disable**}} *port-string*

Parameters

size *size*	Specify the size of maximum jumbo MTU frame allowed. Valid values are **1000 – 10239**.

dynamic enable | **disable**	Enables or disables dynamic jumbo MTU.
port-string	Specifies the port(s) on which the maximum jumbo MTU size is set or dynamic MTU is enabled or disabled.

Defaults

If MTU jumbo frames is enabled using "set port jumbo" on page 26-22, jumbo MTU frame size defaults to **10239** bytes for untagged frames and supports **10243** bytes for tagged frames.

Mode

All command modes.

Usage

The port jumbo MTU size can be administratively set to a packet size between 1000 and 10239. This administratively set packet size is applicable only if jumbo frames is enabled using "set port jumbo" on page 26-22.

Dynamic jumbo MTU allows you to set the maximum jumbo size to any supported size and jumbo MTU will automatically add the extra header bytes for supported applications if required. Currently, only provider bridging is supported and 4 extra bytes are automatically added to the maximum frame size to account for the provider bridging frame size. If you enable dynamic jumbo MTU, make sure you set the jumbo MTU size to at least 1518.

Example

This example shows how to set the jumbo MTU size to 2000 for port tg.1.5:

```
S Chassis(rw)->set port jumbo enable tg.1.5
S Chassis(rw)->set port jumbo mtu size 2000 tg.1.5
```

clear port jumbo mtu

Use this command to reset the port jumbo MTU size or dynamic jumbo MTU state to default values on one or more ports.

Syntax

clear port jumbo mtu [**dynamic**] *port-string*

Parameters

dynamic	(Optional) Specifies that the dynamic jumbo MTU state should be reset to the default value of disable.
port-string	Specifies the port(s) on which the maximum jumbo MTU size is set or dynamic MTU is enabled or disabled.

Defaults

If **dynamic** is not specified, the jumbo MTU size configuration is cleared.

Mode

All command modes.

Example

This example shows how to clear the jumbo MTU size configuration for port tg.1.5:

```
S Chassis(rw)->clear port jumbo mtu tg.1.5
```

show port mdix

Use this command to display the MDI/MDIX mode on one or more ports.

Syntax

show port mdix [*port-string*] {**all** | **auto** | **mdi** | **mdix**}

Parameters

port-string	(Optional) Displays mode for specific port(s).
all	Displays port(s) MDI and MDIX admin status.
auto	Displays port(s) automatically determining MDI/MDIX.
mdi	Displays port(s) forced to MDI configuration.
mdix	Displays port(s) forced to MDIX configuration.

Defaults

If *port-string* is not specified, the mode for all ports will be displayed.

Mode

All command modes.

Example

This example shows how to display MDI/MDIX mode for Gigabit Ethernet port 14 in module 3:

```
S Chassis(rw)->show port negotiation ge.3.14
mdix configuration is auto on port ge.3.14
```

set port mdix

Use this command to set MDI/MDIX mode on one or more ports.

Syntax

set port mdix [*port-string*] {**auto** | **mdi** | **mdix**}

Parameters

port-string	(Optional) Sets MDIX mode for specified port(s).
auto	Sets port(s) to automatically determine MDI/MDIX.
mdi	Forces port(s) to MDI configuration.
mdix	Forces port(s) to MDIX configuration.

Defaults

If *port-string* is not specified, mode will be set for all ports.

Mode

All command modes.

Usage

This function detects and adapts to straight through (MDI) or cross-over (MDIX) Ethernet cabling on switch ports.

Port MDIX defaults to automatically determining MDI/MDIX.

Example

This example shows how to force Gigabit Ethernet port 14 in module 3 to MDIX configuration:

```
S Chassis(rw)->set port mdix ge.3.14 mdix
```

clear port mdix

Use this command to reset MDIX mode to the default setting of auto on one or more ports.

Syntax

clear port mdix [*port-string*]

Parameters

port-string	(Optional) Resets mode for specific port(s).

Defaults

If *port-string* is not specified, mode will be reset for all ports.

Mode

All command modes.

Example

This example shows how to reset Gigabit Ethernet port 14 in module 3 to auto MDI/MDIX configuration:

```
S Chassis(rw)->set port mdix ge.3.14
```

show port negotiation

Use this command to display the status of auto-negotiation for one or more ports.

Syntax

show port negotiation [*port-string*]

Parameters

port-string	(Optional) Displays auto-negotiation status for specific port(s).

Defaults

If *port-string* is not specified, auto-negotiation status for all ports will be displayed.

Mode

All command modes.

Example

This example shows how to display auto-negotiation status for port ge.3.14:

```
S Chassis(rw)->show port negotiation ge.3.14
auto-negotiation is enabled on port ge.3.14.
```

set port negotiation

Use this command to enable or disable auto-negotiation on one or more ports.

Syntax

set port negotiation *port-string* {**enable** | **disable**}

Parameters

port-string	Specifies the port(s) for which to enable or disable auto-negotiation. Port auto-negotiation is enabled by default.
enable | **disable**	Enables or disables auto-negotiation.

Defaults

None.

Mode

All command modes.

Example

This example shows how to disable auto-negotiation on port ge.3.14:

```
S Chassis(rw)->set port negotiation ge.3.14 disable
```

show port oam

Use this command to display Ethernet port Operations, Administration, and Maintenance (OAM) information, statistics, and eventlogs.

Syntax

show port oam [*port-string*] [**stats**] [**eventlog**]] [**-interesting**]

Parameters

port-string	(Optional) Displays a detailed status for the specified port(s).
stats	(Optional) Displays counters, statistics and records for the specified port(s).

eventlog	(Optional) Displays local and remote events logged by the device for the specified port(s).
-interesting	(Optional) Displays only ports with port OAM status enabled using "set port oam status" on page 26-31.

Defaults

If no options are specified, a summary of the current Ethernet OAM state of all ports is displayed.

Mode

All command modes.

Examples

This example shows how to display the Ethernet OAM status for all ports:

```
S Chassis(rw)->show port oam

Capability Legend
L - Link Monitor           U - Unidirection
R - Remote Loopback        V - Variable Retrieval

Port      MAC Address        Remote OUI   Mode      Capability
----      -----------------  ----------   -------   ----------
ge.2.1    00-00-00-00-00-00  00-00-00     Active    L R
.
.
.
ge.2.39   00-1f-45-9d-46-3d  00-1f-45     Active    L R
ge.2.40   00-1f-45-9d-46-3c  00-1f-45     Active    L R
ge.2.41   00-00-00-00-00-00  00-00-00     Active    L R
.
.
.
ge.4.47   00-00-00-00-00-00  00-00-00     Active    L R
ge.4.48   00-00-00-00-00-00  00-00-00     Active    L R
```

This example shows how to display Ethernet OAM information for port ge.4.20:

```
S Chassis(rw)->show port oam ge.4.20

Port: ge.4.20   MIB2 Interface: 42020
------------------------------------------------------------------------

Local Client
------------
  Oper State            : linkFault
  Mode                  : Active
  Unidirection          : Not Supported
```

```
  Link Monitor          : Supported (on)
  Remote Loopback       : Supported (off)
  Variable Retrieval    : Not Supported
  Loopback Status       : NoLoopback
  Loopback Ignore Rx    : Ignore
  MTU Size              : 1518
  Notification Retries  : 1

Remote Client
-------------
  MAC Address           : 00-00-00-00-00-00
  Vendor OUI            : 00-00-00
  Mode                  : Passive
  Unidirection          : Not Supported
  Link Monitor          : Not Supported
  Remote Loopback       : Not Supported
  Variable Retrieval    : Not Supported
  MTU Size              : 0

Link Monitoring
---------------
  Status : Supported (on)

  symbol-period Error
    Window          : 524288000 symbols
    Threshold       : 1 symbol errors
    Actions         : Notify

  Frame Error
    Window          : 10 x 100 milliseconds
    Threshold       : 1 frame errors
    Actions         : Notify

  Frame Period Error
    Window          : 1488000 frames
    Threshold       : 1 frame errors
    Actions         : Notify

  Frame Seconds Error
    Window          : 600 x 100 milliseconds
    Threshold       : 1 errored frame seconds
    Actions         : Notify

Unidirectional Link Detection
-----------------------------
```

```
  Mode              : Fast
  Action            : syslog-only
  Status            : active
  Fast Status       : activeFast
  Fast Timer Config : 2 x 100 milliseconds
  Active Fast Timer : 5 x 100 milliseconds
  Port Status       : Operational
S Chassis(rw)->
```

This example shows how to display Ethernet OAM statistics for port ge.4.20

```
S Chassis(rw)->show port oam ge.4.20 stats

Counters
--------

  Port: ge.4.20   MIB2 Interface: 42020
  ------------------------------------------------------------------------
  Information OAMPDU Tx                   : 1234567890
  Information OAMPDU Rx                   : 1234123412
  Unique Event Notification OAMPDU Tx     : 0
  Unique Event Notification OAMPDU Rx     : 0
  Duplicate Event Notification OAMPDU Tx  : 0
  Duplicate Event Notification OAMPDU Rx  : 0
  Loopback Control OAMPDU Tx              : 0
  Loopback Control OAMPDU Rx              : 0
  Variable Request OAMPDU Tx              : 0
  Variable Request OAMPDU Rx              : 0
  Variable Response OAMPDU Tx             : 0
  Variable Response OAMPDU Rx             : 0
  Unsupported OAMPDU Tx                   : 0
  Unsupported OAMPDU Rx                   : 0
  Frames Lost due to OAM                  : 0
  Fast ULD Information TLV Tx             : 329
  Fast ULD Information TLV Rx             : 332
  Fast ULD Information TLV Errors Rx      : 0
  Last Fast ULD Information TLV Rx Time   : 71236

  Local Faults   (Max records is 8)
  --------------
  Org Spec Event records : 0

  Remote Faults
  ---------------
  Org Spec Event records : 0
```

```
  Local Event Logs
  ------------------
  Errored symbol-period records : 0
  Errored Frame records         : 0
  Errored Frame Period records  : 0
  Errored Frame Second records  : 0

  Remote Event Logs
  ------------------
  Errored symbol-period records : 0
  Errored Frame records         : 0
  Errored Frame Period records  : 0
  Errored Frame Second records  : 0
S Chassis(rw)->
```

set port oam status

Use this command to enable or disable Operations, Administration, and Maintenance (OAM) port status on the specified port.

Syntax

set port oam *port-string* **status** {**enable** | **disable**}

Parameters

port-string	Specifies the port(s) to enable or disable OAM status on. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.
enable | **disable**	Enable or disable OAM operations for a port. The default value is **disabled**.

Defaults

None.

Mode

All command modes.

Usage

This command enables or disables Ethernet OAM operations on the specified port. The default status is **disabled**.

Example

This example shows how to enable OAM operations on ports ge.1.3 through ge.1.5:

```
S Chassis(rw)->set port oam ge.1.3-5 status enable
```

set port oam mode

Use this command to set the operating mode for the OAM client on the specified port.

Syntax

set port oam *port-string* **mode** {**active** | **passive**}

Parameters

port-string	Specifies the port(s) to configure for OAM port mode. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.
active | **passive**	Set the OAM mode for a port. The default value is **active**.

Defaults

None.

Mode

All command modes.

Usage

This command sets the operating mode for the OAM client on the specified port. Clients configured for active mode may initiate contact with remote peers. Once the discovery process has completed with the remote peer, active clients are allowed to send remote loopback control OAMPDUs to that peer. OAM clients configured for passive mode may not initiate any contact with a remote peer. Passive OAM clients are only allowed to respond to requests received from a remote peer. In either operational mode, the client will silently discard OAM PDUs received on ports that are not configured for OAM operations.

The default value is **active**.

Example

This example shows how to set the port ge.1.3 OAM mode to passive:

```
S Chassis(rw)->set port oam ge.1.3 mode passive
```

set port oam loopback-rx

Use this command to set the OAM loopback mode for the specified port.

Syntax

set port oam *port-string* **loopback-rx** {**ignore** | **process**}

Parameters

port-string	Specifies the port(s) to configure for OAM loopback mode. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.
ignore | **process**	Set the OAM loopback mode for a port. The default value is **ignore**.

Defaults

None.

Mode

All command modes.

Usage

Determines the behavior of the OAM client when receiving a remote loopback request from a remote OAM client. Setting this value to process will allow the OAM client to receive and operate upon an OAM PDU request. Setting this value to ignore will force the OAM client to discard any received remote loopback OAM PDUs. The default value is **ignore**.

Example

This example shows how to set the OAM client behavior on port ge.1.3 to receive and operate upon OAM PDU requests:

```
S Chassis(rw)->set port oam ge.1.3 loopback-rx process
```

set port oam remote-loopback

Use this command to enable or disable OAM remote loopback for the specified port.

Syntax

set port oam *port-string* **remote-loopback** {**enable** | **disable**}

Parameters

port-string	Specifies the port(s) to enable or disable remote loopback. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.
enable | **disable**	Enables or disables OAM remote-loopback for the specified port(s). The default value is **disable**.

Defaults

None.

Mode

All command modes.

Usage

This command:

- Instructs the remote OAM client to initiate, if enabled, or terminate, if disabled, the remote loopback process.
- Is a volatile configuration option that does not persist across reboots, and is not displayed in the **show config port** output.

Port OAM must be configured for active mode, the OAM client must have completed the discovery process with the remote OAM client, and that client must indicate that it supports

loopback in order to initiate the loopback process. A client which has been put into loopback mode will re-transmit all traffic that has been received on that port (with the exception of OAM PDUs) back towards the sender.

A client which has put its peer into loopback mode will discard all received traffic (with the exception of OAM PDUs) on that port. Be aware that OAM remote loopback is a disruptive test state intended to aid in the diagnosis of network issues, and will interfere with the normal operation of other network protocols and data flows over that link.

Caution must be used when placing an OAM enabled port in remote loopback. When requesting the remote OAM enabled port to be placed in loopback, the loopback mode of the remote port must be set to **process** using "set port oam loopback-rx" on page 20-28. OAM remote loopback's behavior is "fire and forget". If for any reason, including OAM mode set to **ignore**, or the loopback request or remote response should be lost in transit, remote loopback will remain in either an initiating or terminating loopback state. The potential for harm to the network exists where one end of the link believes remote loopback is in effect, and the other does not.

Should the loopback request PDU be lost in transit or the remote end be set to ignore the PDU, the loopback session will be left in a bad state, and the port will be prevented from both sending and receiving data until OAM is administratively disabled and then enabled on both ends of the link.

The default value for OAM remote loopback is **disable**.

Example

This example shows how to enable remote loopback on port ge.1.3:

```
S Chassis(rw)->set port oam ge.1.3 remote-loopback enable
```

set port oam notify-retry

Use this command to set the number of notify retries to send for the specified port.

Syntax

set port oam *port-string* **notify-retry** *retries*

Parameters

port-string	Specifies the port(s) to enable or disable. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.
retries	Set the number of notification retries to send. The default value is **0**. The maximum value is **10**.

Defaults

None.

Mode

All command modes.

Usage

Instructs the remote OAM client to retransmit event notification OAM PDUs to the remote peer up to the configured number of retries. If a monitor link threshold is crossed, generating an event, and the notification action is configured, a single event notification OAM PDU is always generated. By default no further notifications are sent unless a value greater than zero is

configured using this command. This retransmission process will halt if the link-monitoring process determines that additional events have transpired upon the link. A notification of the new event is then sent by the remote OAM client. The default value is **0**, and the maximum value is **10**.

Example

This example shows how to set the number of OAM notify retry attempts for port ge.1.3 to 3:

```
S Chassis(rw)->set port oam ge.1.3 notify-retry 3
```

clear port oam

Use this command to clear OAM counters or reset OAM configuration to default values for the specified port(s).

Syntax

clear port oam *port-string* {**all** | **status** | **mode** | **loopback-rx** | **remote-loopback** | **notify-retry**}

Parameters

port-string	Specifies the port(s) to reset the OAM configuration to default values for. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.
all	Resets all OAM configuration to the default values for the specified port(s).
status	Resets OAM status for the specified port(s) to the default value of **disabled**.
mode	Resets the operating mode for the OAM client to the default value of **active** for the specified port(s).
loopback-rx	Resets the OAM loopback mode to the default value of **ignore** for the specified port(s).
remote-loopback	Resets the OAM remote loopback to the default value of **disable** for the specified port(s).
notify-retry	Resets the number of OAM notify retries to send for the specified port(s) to the default value of **0**.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the OAM operating mode for the OAM client to the default value of active for port ge.1.3:

```
S Chassis(rw)->clear port oam ge.1.3 mode
S Chassis(rw)->
```

set port oam link-monitor

Use this command to configure OAM link monitor functionality for the specified port.

Syntax

set port oam *port-string* **link-monitor** {**frame** | **frame-period** | **frame-seconds** | **symbol-period**} {**threshold** *threshold* | **window** *window* | **action** {[**syslog**] [**disable-interface**] [**notify**]}

Parameters

port-string	Specifies the port(s) to enable or disable. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.
frame	Configure OAM monitoring of frame events for a port.
frame-period	Configure OAM monitoring of frame-period events for a port.
frame-seconds	Configure OAM monitoring of frame-second events for a port.
symbol-period	Configure OAM symbol-period event for a port.
threshold *threshold*	Specifies the number of errors threshold for the specified OAM link monitor function. See the Usage section of this command for default and range threshold values for each link-monitor function.
window *window*	Specifies the window value for: • The errored frame event and the errored frame-seconds summary events in seconds. • The errored frame-period event, in number of frames • The errored-symbol-period event in number of symbols See the Usage section of this command for default and range window values for each link-monitor function.
syslog	Specifies that a syslog message will be generated upon detecting a link monitor event.
disable-interface	Specifies that the port will be operationally disabled upon detecting a link monitor event.
notify	Specifies that a link notification event is triggered upon detecting a link monitor event.

Defaults

None.

Mode

All command modes.

Usage

This command configures the link-monitoring process on the specified port. Should the number of errors exceed the value specified in the threshold parameter for the configured window parameter, the link-monitoring process will take one or more specified actions.

Note: If the threshold value is zero (**0**), then an Event Notification OAM PDU is sent at the end of every window, regardless of whether the threshold is exceeded or not for that window. This can be used as an asynchronous notification to the peer OAM entity of the statistics related to this threshold crossing alarm.

The **frame** option monitors frame errors occurring during a period of time. The default threshold is **1** errored-frame. Valid threshold values are **0** - **4294967295** errored-frames. The default window is a **1** second interval. Valid window values are **1** - **60** seconds.

The **frame-period** option monitors frame errors that occur during the reception of a given number of frames. The default threshold is **1** errored-frame. Valid threshold values are **0** - **4294967295** errored-frames. The default window is equivalent to the maximum number of minimum sized frames that may be transmitted over the link during a one second interval, and the upper bound is the maximum number of minimum sized frames that may be transmitted over the link during a one minute interval. Therefore, the maximum frame-period window value can be set to 60 times the default window value.

The frame-period option defines its window value (number of frames) based upon the line rate of the port being configured. As such, the value may not be determined until the port has achieved a valid link state. The possible frame-period window default and range values, based upon link speed are displayed in Table 26-5.

Table 26-5 Frame-Period Window Values

Port Line Rate	Default Window Value	Window Value Range
100 Mbps	148,800 frames	14880 - 8928000 frames
1Gbps	1,488,000 frames	148,800 to 89,280,000 frames
10 Gbps	14,880,000 frames	1,488,000 to 892,800,000 frames

The **frame-seconds** option monitors the number of one-second intervals in which one or more frame errors occurred. The default threshold is **1** errored-second. Valid threshold values are **0** - **4294967295** errored-seconds. The default window is 60 seconds, the minimum is 10 seconds, and the maximum is 900 seconds.

The **symbol-period** option monitors symbol errors that occur during the reception of a given number of symbols. The default threshold is one errored-symbol. Valid threshold values are **0** - **4294967295** errored-symbol. The default window is equivalent to the maximum number of symbols that may be transmitted over the link during a one second interval, and the upper bound is the number of symbols that may be transmitted over the link during a one minute interval. Therefore, the maximum symbol-period window value can be set to 60 times the minimum window value.

The symbol-period option defines its window value based upon the line rate of the port being configured. As such, the value may not be determined until the port has achieved a valid link state. The possible symbol-period window default and range values, based upon link speed are displayed in Table 26-6.

Table 26-6 Symbol-Period Window Values

Port Line Rate	Default Window Value	Window Value Range
100 Mbps	131,072,000 symbols	52,428,800 - 7,864,320,000
1Gbps	524,288,000 symbols	524,288,000 - 31,457,280,000
10 Gbps	5,242,880,000 symbols	5,242,880,000 - 314,572,800,000

The administrator may configure any one of three actions to be taken upon the detection of a link event:

- The **syslog** option triggers a syslog message to be generated, which confers information related to the event.
- The **notify** option triggers the transmission of a link event notification OAM PDU to the remote client.
- The **disable-interface** option operationally disables the port in question, and the port remains in that state until the administrator restores the port to operational status.

Examples

This example shows how to set the OAM link monitor frame threshold to 1, window to 300 seconds, and action to syslog for port ge.1.3:

```
S Chassis(rw)->set port oam ge.1.3 link-monitor frame threshold 1
S Chassis(rw)->set port oam ge.1.3 link-monitor frame window 300
S Chassis(rw)->set port oam ge.1.3 link-monitor frame action syslog
S Chassis(rw)->
```

This example shows how to set the OAM link monitor frame-period threshold to 1, window to 500000, and action to disable the interface, generate a syslog message and send a link notification:

```
S Chassis(rw)->set port oam ge.1.3 link-monitor frame-period threshold 1
S Chassis(rw)->set port oam ge.1.3 link-monitor frame-period window 500000
S Chassis(rw)->set port oam ge.1.3 link-monitor frame-period action
disable-interface syslog notify
```

clear port oam link-monitor

Use this command to reset OAM link monitor configuration to default values for the specified port(s).

Syntax

set port oam *port-string* **link-monitor** {**frame** | **frame-period** | **frame-seconds** | **symbol-period**} {**threshold** | **window** | **action** [**syslog**] [**disable-interface**] [**notify**]

Parameters

port-string	Specifies the port(s) to reset for OAM link monitor. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.
frame	Reset OAM monitoring of frame events to the default value for the specified port(s).
frame-period	Reset OAM monitoring of frame-period events to the default value for the specified port(s).
frame-seconds	Reset OAM monitoring of frame-second events to the default value for the specified port(s).
symbol-period	Reset OAM symbol-period event configuration to the default value for the specified port(s).

threshold	Resets the number of errors threshold for the specified OAM link monitor function to the default value. See the Usage section of this command for default and maximum threshold values for each link-monitor function.
window	Resets the window value for the specified OAM link monitor function to the default value. See the Usage section of this command for default and maximum window values for each link-monitor function.
action	
syslog	Clears whether a syslog message will be generated upon detecting a link monitor event.
disable-interface	Clears whether the port will be operationally disabled upon detecting a link monitor event.
notify	Clears whether a link notification event is triggered upon detecting a link monitor event.

Defaults

None.

Mode

All command modes.

Usage

This command resets the link-monitoring process on the specified port to the default value and clears any specified action.

The **frame** option monitors frame errors occurring during a period of time. The default threshold is one errored frame. The default window is a **1** second interval.

The **frame-period** option monitors frame errors that occur during the reception of a given number of frames. The default threshold is one errored frame. The default window is equivalent to the maximum number of minimum sized frames that may be transmitted over the link during a one second interval. See the Usage section of "set port oam link-monitor" on page 26-36 for details.

The **frame-seconds** option monitors the number of one-second intervals in which one or more frame errors occurred. The default threshold is one errored-second. The default window is 60 seconds.

The **symbol-period** option will monitor symbol errors that occur during the reception of a given number of symbols. The default threshold is one errored-symbol. The default window is equivalent to the maximum number of symbols that may be transmitted over the link during a one second interval. See the Usage section of "set port oam link-monitor" on page 26-36 for details.

Any specified action is cleared. If a specific action is not specified, the action keyword resets all actions to the default value of notify.

Example

This example shows how to reset the OAM link monitor frame threshold to the default value of 1, the frame window to the default value of 1 second, and clears the syslog action for port ge.1.3:

```
S Chassis(rw)->set port oam ge.1.3 link-monitor frame threshold window action
syslog
S Chassis(rw)->
```

show oam uld-config

Use this command to display a summary of the OAM Unidirectional Link Detection (ULD) configuration groups on the chassis.

Syntax

show oam uld-config [*group-index*]

Parameters

group-index	(Optional) Specifies a port group for ULD configuration display. Each port group represents the segmentation of ULD configured chassis ports by shared resources.

Defaults

If a port group index is not specified, ULD configuration is displayed for all port groups.

Mode

All command modes.

Examples

This example shows how to display the OAM ULD configuration summary for all port groups on this device:

```
S Chassis(rw)->show port oam uld-config
Ethernet OAM ULD Port Group Entries
------------------------------------------------------------------------
Port Group Index   : 1
Maximum Fast Ports : 96
Fast Ports In Use  : 0
Group Ports        : ge.1.1-48,101-112;
Fast Ports         : none
------------------------------------------------------------------------
Port Group Index   : 3
Maximum Fast Ports : 96
Fast Ports In Use  : 0
Group Ports        : ge.3.1-48;
Fast Ports         : none
------------------------------------------------------------------------
Port Group Index   : 4
Maximum Fast Ports : 96
Fast Ports In Use  : 2
Group Ports        : ge.4.1-48;
Fast Ports         : ge.4.29-30;
------------------------------------------------------------------------
Port Group Index   : 5
Maximum Fast Ports : 96
Fast Ports In Use  : 0
```

```
Group Ports        : ge.5.1-48;
Fast Ports         : none
------------------------------------------------------------------------
Port Group Index   : 6
Maximum Fast Ports : 96
Fast Ports In Use  : 0
Group Ports        : ge.6.1-48;tg.6.101-104,201-204;
Fast Ports         : none
------------------------------------------------------------------------
Port Group Index   : 7
Maximum Fast Ports : 96
Fast Ports In Use  : 0
Group Ports        : ge.7.1-48,101-112;
Fast Ports         : none
------------------------------------------------------------------------
S Chassis(rw)->
```

Table 26-7 provides an explanation of the command output.

Table 26-7 show port oam uld-config Output Details

Output...	What it displays...
Port Group Index	A port group index value. Each configuration group represents a group of ports that share a set of resources which may limit the number of ports within the group that can be configured in the fast ULD mode.
Maximum Fast Ports	The maximum number of fast ports supported by the port group.
Fast Ports In Use	The number of fast ports currently configured for ULD in the port group.
Group Ports	The ports that belong to this port group.
Fast Ports	The ports that are configured as fast ports in this port group.

set port oam uld mode

Use this command to set the OAM Unidirectional Link Detection (ULD) mode for the specified port.

Syntax

set port oam *port-string* **uld mode** {**disable** | **standard** | **fast**}

Parameters

port-string	Specifies the port(s) to configure for ULD mode. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.
disable | **standard** | **fast**	Sets the ULD mode for the specified port: • **disable** – ULD is disabled on the specified port. • **standard** – ULD uses the standard OAM discovery protocol, which provides for the configured ULD action to occur within 5 seconds. • **fast** – ULD uses fast ULD mode which sends OAMPDUs with Fast ULD information TLVs that provide for the configured ULD action to occur within a range of 600 milliseconds to 3 seconds depending upon the ULD fast timer setting.

Defaults

ULD is disabled by default on all ports.

Mode

All command modes.

Usage

If ULD is disabled, no attempt is made to detect unidirectional operation on the link. ULD supports two modes for the detection of a unidirectional link:

- **Standard** – Uses the existing OAM discovery protocol to perform the configured ULD action on the port (set using "set port oam uld action" on page 26-43) if more than 5 seconds elapses between reception of standard information OAMPDUs on the port.
- **Fast** – Establishes a second tier of OAM discovery by transmitting information OAMPDUs with the Fast ULD information TLV. The configured ULD action is performed if more than 3 times the interval defined by the fast timer setting (using "set port oam uld fast-timer" on page 26-43) elapses between reception of a Fast ULD information TLV on the port.

The configured ULD action can be to both disable the port and send a Syslog message or to only send a Syslog message. The ULD action defaults to only sending the Syslog message.

OAM ULD requires that both link peers are configured for active OAM mode, set using "set port oam mode" on page 26-32. To prevent ULD mis-configuration, the OAM peer disregards the configured OAM mode and operates as an active peer, if ULD is configured for either standard or fast mode.

Example

This example shows how to set the OAM ULD mode to **fast** for port ge.1.2:

```
S Chassis(rw)->set port oam ge.1.2 uld mode fast
```

set port oam uld action

Use this command to set the ULD administrative action that will occur when a unidirectional link is detected on the specified port.

Syntax

set port oam *port-string* **uld action** {**disable-port** | **syslog-only**}

Parameters

port-string	Specifies the port(s) to configure for a ULD action. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.
disable-port | **syslog-only**	Sets the ULD action for the specified port: • **disable-port** – Disables the unidirectional link port and sends a Syslog message • **syslog-only** – Only sends a Syslog message when a unidirectional link is detected on the port

Defaults

The ULD administrative action defaults to only sending a Syslog message when a unidirectional link is detected.

Mode

All command modes.

Usage

The ULD administrative action that occurs when a unidirectional link is detected defaults to sending a Syslog message only. The administrative action will always generate a Syslog message. By setting the ULD administrative action to **disable-port**, the ULD administrative action is to both disable the port and send a Syslog message.

Example

This example shows how to set the port ge.1.2 ULD administrative action to both disable the port and send a Syslog message:

```
S Chassis(rw)->set port oam ge.1.2 uld action disable-port
```

set port oam uld fast-timer

Use this command to set the fast timer multiplier for transmitting Fast ULD information TLVs on the specified port.

Syntax

set port oam *port-string* **uld fast-timer** *multiplier*

Parameters

port-string	Specifies the port(s) to configure for ULD fast mode fast timer setting. For a detailed description of possible *port-string* values, refer to the "Port String Syntax Used in the CLI" discussion in the *Extreme Networks S-Series Configuration Guide*.
multiplier	Specifies the ULD fast mode timer multiplier for the specified port. Valid values are integers between **2** and **10** representing the number of 100 millisecond multiples for the timer value (timer value range of 200 milliseconds - 1000 milliseconds (1 second)). The default value is **2** (timer value of 200 milliseconds).

Defaults

The fast timer multiplier defaults to **2** (timer value of 200 milliseconds).

Mode

All command modes.

Usage

This command determines the interval between transmission of OAMPDUs with Fast ULD information TLVs, used by the ULD fast mode to detect unidirectional links. ULD fast mode is set using "set port oam uld mode" on page 26-41. ULD Fast mode establishes a second tier of OAM discovery by transmitting information OAMPDUs with the Fast ULD information TLV. If a ULD fast mode configured port does not receive the Fast ULD information TLV from its peer within three times the configured fast timer setting, ULD performs the configured ULD action configured using "set port oam uld action" on page 26-43.

Example

This example shows how to set the transmission of OAMPDUs with Fast ULD information TLVs for port ge.1.2 to 400 milliseconds:

```
S Chassis(rw)->set port oam ge.1.2 uld fast-timer 4
```

clear port oam uld

Use this command to reset OAM ULD configuration to default values for the specified port.

Syntax

set port oam *port-string* **uld** {[**mode**] [**action**] [**fast-timer**]}

Parameters

mode	(Optional) Resets the ULD mode configuration to the default value of disabled.
action	(Optional) Resets the ULD action to the default value of only sending a Syslog message.
fast-timer	(Optional) Resets the ULD fast timer multiple setting to the default value of **2** (200 milliseconds).

Defaults

- ULD **mode** defaults to disabled.
- ULD **action** defaults to only sending a Syslog message.
- ULD **fast-timer** multiplier defaults to **2** (fast timer interval of 200 milliseconds).

Mode

All command modes.

Examples

This example resets the ULD mode for all ports to the default value of disabled:

```
S Chassis(rw)->clear port oam *.*.* uld mode
```

This example resets ULD mode, action and fast timer to default values for port **ge.1.2**:

```
S Chassis(rw)->clear port oam ge.1.2 uld mode action fast-timer
```

show port operstatuscause

Use this command to display the causes configured to place operating status to a down or dormant state for one or more ports.

Syntax

show port operstatuscause [**admin** | **any** | **cos** | **dot1x** | **flowlimit** | **init** | **lag** | **linkflap** | **linkloss** | **modifiable** | **oam** | **oamlb** | **vsb** | **lstrk** | **uld** | **policy** | **self**] [*port-string*]

Parameters

port-string	(Optional) Displays causes for specific port(s).
admin	(Optional) Displays ports down due to adminStatus.
any	(Optional) Displays a table of all causes.
cos	(Optional) Displays ports down due to Class of Service constraint.
dot1x	(Optional) Displays ports dormant due to 802.1X enforcement.
flowlimit	(Optional) Displays ports down due to a flow limiting constraint.
init	(Optional) Displays ports in initialization phase.
lag	(Optional) Displays ports dormant due to Link Aggregation Group (LAG) membership.
linkflap	(Optional) Displays ports down due to link flap violation.
linkloss	(Optional) Displays ports down due to link loss.
modifiable	(Optional) Displays a table of modifiable causes.
oam	(Optional) Displays ports down due to ethernet OAM. A port's OAM operStatusCause flag will be set if the link-monitoring function determines an event has occurred on a port, and the **disable-port** option has been configured for that event using "set port oam link-monitor" on page 26-36.
oamlb	(Optional) Displays ports down due to ethernet OAM loopback. See the usage section for oamlb bit set details.

lstrk	(Optional) Displays ports down due to link state trunk.
uld	(Optional) Displays ports down due to Unidirectional Link Detection.
policy	(Optional) Displays ports down due to policy restriction.
self	(Optional) Displays ports down due to a hardware cause.

Defaults

If no options are specified, causes for all ports will be displayed.

Mode

All command modes.

Usage

There are 3 OAM loopback states for which the oamlb bit is set: initiating loopback, terminating loopback, and local loopback.

For the port that initiates or terminates remote loopback, the oamlb bit is briefly set as the port passes through the initiating or terminating loopback state, unless a problem communicating with the peer exists. Once remote loopback state is acquired or terminated, the oamlb bit clears.

The oamlb bit is also set if the peer port has initiated remote loopback, which puts the local port in local loopback. The oamlb bit is set for the client being put into loopback for the entire time that remote loopback is in effect. The oamlb bit clears once loopback is torn down between the two clients.

Example

This example shows how to display operation status causes for all ports:

```
S Chassis(rw)->show port operstatuscause
             +-----------------------------------------+
             | A  L  L              D       O     L    |
             | D  L  F  S  I  F     O       A     S    |
             | M  O  L  E  N  L  P  C  T  L  O  M  V  T  U |
             | I  S  A  L  I  O  O  O  1  A  A  L  S  R  L |
Port         | N  S  P  F  T  W  L  S  X  G  M  B  B  K  D |
-------------+-----------------------------------------+
vlan.0.101   | .  .  .  .  .  .  .  .  .  .  .  .  .     . |
vlan.0.201   | .  .  .  .  .  .  .  .  .  .  .  .  .  .  . |
vlan.0.666   | .  .  .  .  .  .  .  .  .  .  .  .  .  .  . |
vlan.0.1000  | .  .  .  .  .  .  .  .  .  .  .  .  .  .  . |
vlan.0.2000  | .  .  .  .  .  .  .  .  .  .  .  .  .  .  . |
vlan.0.4093  | .  .  .  .  .  .  .  .  .  .  .  .  .  .  . |
lo.0.1       | .  .  .  .  .  .  .  .  .  .  .  .  .  .  . |
loop.0.1     | .  .  .  .  .  .  .  .  .  .  .  .  .  .  . |
host.0.1     | .  .  .  .  .  .  .  .  .  .  .  .  .  .  . |
ge.1.1       | .  .  .  .  .  .  .  .  .  .  .  .  .  .  . |
ge.1.2       | .  X  .  .  .  .  .  .  .  .  .  X  .  .  . |
ge.1.3       | .  X  .  .  .  .  .  .  .  .  .  .  .  .  . |
ge.1.4       | .  X  .  .  .  .  .  .  .  .  .  .  .  .  . |
```

```
ge.1.5          | .  X  .  .  .  .  .  .  .  .  X  .  .  .  . |
```

clear port operstatuscause

Use this command to override the causes configured to place operating status to a down or dormant state for one or more ports.

Syntax

clear port operstatuscause [*port-string*] [**admin**] [**all**] [**cos**] [**flowlimit**] [**linkflap**] [**oam**] [**oamlb**] [**policy**]

Parameters

port-string	(Optional) Overrides causes for specific port(s).
admin	(Optional) Resets adminStatus to up.
all	(Optional) Overrides all modifiable operStatus down causes.
cos	(Optional) Overrides a Class of Service constraint.
flowlimit	(Optional) Overrides a flow limiting constraint.
linkflap	(Optional) Overrides link flap violation status.
oam	(Optional) Overrides Ethernet OAM operStatus down causes.
oamlb	(Optional) Overrides Ethernet OAM loopback operStatus down causes.
policy	(Optional) Overrides a policy restriction.

Defaults

If no options are specified, all operating status causes will be overridden for all ports.

Mode

All command modes.

Example

This example shows how to override all operational causes on all ports:

```
S Chassis(rw)->clear port operstatuscause
```

show port speed

Use this command to display the default speed setting on one or more ports.

Syntax

show port speed [*port-string*]

Parameters

port-string	(Optional) Displays default speed setting(s) for specific port(s).

Defaults

If *port-string* is not specified, default speed settings for all ports will display.

Mode

All command modes.

Example

This example shows how to display the default speed setting for GbE port 14 in slot 3:

```
S Chassis(rw)->show port speed ge.3.14
default speed is 1000 on port ge.3.14.
```

set port speed

Use this command to set the default speed of one or more ports.

Syntax

set port speed *port-string* {**10** | **100** | **1000** | **10000** | **40000**}

Parameters

port-string	Specifies the port(s) for which to set a value for default port speed.
10 | **100** | **1000** | **10000** | **40000**	Specifies the port speed. Valid values are: **10** Mbps, **100** Mbps, **1000** Mbps, **10000** Mbps, or **40000** Mbps.

Defaults

None.

Mode

All command modes.

Usage

The default port speed setting only takes effect on ports that have auto-negotiation disabled.

See the The **40Gpbs QSFP Port** discussion in the *Extreme Networks S-Series Configuration Guide* for a detailed discussion related to changing QSFP 40/10Gbps port speed.

Example

This example shows how to set Ethernet port 3 in slot 3 to a port speed of 1000 Mbps:

```
S Chassis(rw)->set port speed ge.3.3 1000
```

show port status

Use this command to display operating and admin status, speed, duplex mode and port type for one or more ports on the device.

Syntax

show port status [*port-string*] [**-interesting**]

Parameters

port-string	(Optional) Displays status for specific port(s).
-interesting	(Optional) Displays only ports with an operational status of up or dormant.

Defaults

If no options are specified, status information for all ports will be displayed.

Mode

All command modes.

Examples

This example shows how to display status information for port range ge.1.1 through 4:

```
S Chassis(rw)->show port status ge.1.1-4

Port         Alias            Oper     Admin   Speed  Duplex  Type
             (truncated)      Status   Status  (bps)
------------ ---------------- -------- ------- ------ ------- ------------------
ge.1.1                        dormant  up       1.0G full     1000-t       rj45
ge.1.2                        down     up       10.0M half    10-t         rj45
ge.1.3                        down     up       10.0M half    10-t         rj45
ge.1.4                        down     up       10.0M half    10-t         rj45
4 of 4 ports displayed, 1 port(s) with oper status 'up' or 'dormant'.
```

This example shows how to display status information for console ports:

```
S Chassis(rw)->show port status com.*.*

Port         Alias            Oper     Admin   Speed  Duplex  Type
             (truncated)      Status   Status  (bps)
------------ ---------------- -------- ------- ------ ------- ------------------
com.1.1                       up       up        9.6K         rs232        rj45
com.2.1                       up       up        9.6K         rs232        rj45
com.3.1                       up       up        9.6K         rs232        rj45
3 of 3 ports displayed, 3 port(s) with oper status 'up' or 'dormant'.
```

Table 26-8 provides an explanation of the command output.

Table 26-8 show port status Output Details

Output...	What it displays...
Port	Port designation.
Alias (truncated)	Alias configured for the port. For details on using the **set port alias** command, refer to “set port alias” on page 26-12.
Oper Status	Operating status (up or down).
Admin Status	Whether the specified port is enabled (up) or disabled (down). For details on using the **set port disable** and the **set port enable** commands to change the port status, refer to “set port” on page 26-8.

Table 26-8 show port status Output Details

Output...	What it displays...
Speed	Operational speed in Mbps or Kbps of the specified port. For details on using the **set port speed** command to change defaults, refer to "set port speed" on page 26-48.
Duplex	Duplex mode (half or full) of the specified port. For details on using the **set port duplex** command to change defaults, refer to "set port duplex" on page 26-15.
Type	Physical port and interface type.

show port transceiver

Use this command to display port transceiver information.

Syntax

show port transceiver [*port-string*] [**basic-only**] [**sensor-only**] [**all**]

Parameters

port-string	(Optional) Displays transceiver information for the specific port(s).
basic-only	(Optional) Displays basic transceiver information only for the port context.
sensor-only	(Optional) Displays sensor transceiver information only for the port context.
all	(Optional) Displays all transceiver information for the port context.

Defaults

If no options are specified, all transceiver information is displayed for all transceiver ports.

Mode

All command modes.

Examples

This example shows how to display all transceiver information, including basic data and sensor data, for tg.1.5:

```
S Chassis(rw)->show port transceiver tg.1.5

Port        Vendor           Vendor
            Name             Serial Number
----------- ---------------- ----------------
tg.1.5      AVAGO            AD1230LE0GX

Port        Sensor Data          Value      Alarm       High        High        Low         Low
            (Units)                         State       Alarm       Warning     Warning     Alarm
                                                        Threshold   Threshold   Threshold   Threshold
----------- -------------------- ---------- ----------- ----------- ----------- ----------- ---------
tg.1.5      Temp (C)             36         NORMAL      75          70          0           -5
tg.1.5      Voltage (V)          3.251      NORMAL      3.630       3.465       3.134       2.970
tg.1.5      TX Current (mA)      35.658     NORMAL      80.000      74.000      12.000      10.000
tg.1.5      TX Power (mW)        0.643      NORMAL      2.238       1.122       0.151       0.060
```

```
tg.1.5      TX Power (dBm)       -1.918     NORMAL      3.499      0.500      -8.210     -12.218
tg.1.5      RX Power (mW)        0.013      LOW ALARM   2.238      1.122      0.036      0.014
tg.1.5      RX Power (dBm)       -18.861    LOW ALARM   3.499      0.500      -14.437    -18.539
```

This example shows how to display basic information only for all ports with transceivers present:

```
S Chassis(rw)->show port transceiver basic-only

Transceiver Data (operational transceivers only)
------------------------------------------------

Port        Vendor           Vendor
            Name             Serial Number
----------- ---------------- ----------------
ge.1.23     FINISAR CORP.    PKS2XDD
ge.1.47     AGILENT          AC0548SJ102
tg.1.3      AVAGO            AD1230LE0GX
tg.1.4      AVAGO            AD1230LE0GX
tg.1.5      AVAGO            AD1230LE0GX
tg.1.6      AVAGO            AD1230LE0GX
tg.1.7      TE Connectivity2 12090001
tg.1.8      TE Connectivity2 12090001
tg.1.9      TE Connectivity2 12090001
tg.1.10     TE Connectivity2 12090001
```

This example shows how to display sensor information only for tg.1.3 and tg.1.4

```
S Chassis(rw)->show port transceiver tg.1.3-4 sensor-only

Transceiver Sensor Data (operational sensors only)
--------------------------------------------------

Port        Sensor Data          Value      Alarm       High       High       Low        Low
            (Units)                         State       Alarm      Warning    Warning    Alarm
                                                        Threshold  Threshold  Threshold  Threshold
----------- -------------------- ---------- ----------- ---------- ---------- ---------- ---------
tg.1.3      Temp (C)             36         NORMAL      75         70         0          -5
tg.1.3      Voltage (V)          3.251      NORMAL      3.630      3.465      3.134      2.970
tg.1.3      TX Current (mA)      36.126     NORMAL      80.000     74.000     12.000     10.000
tg.1.3      TX Power (mW)        0.644      NORMAL      2.238      1.122      0.151      0.060
tg.1.3      TX Power (dBm)       -1.911     NORMAL      3.499      0.500      -8.210     -12.218
tg.1.3      RX Power (mW)        0.013      LOW ALARM   2.238      1.122      0.036      0.014
tg.1.3      RX Power (dBm)       -18.861    LOW ALARM   3.499      0.500      -14.437    -18.539
tg.1.4      Temp (C)             36         NORMAL      75
```

27

Link Trap and Link Flap Detection Commands

This chapter provides detailed information for the link trap and link flap set of commands. For information about configuring link trap and link flap detection, refer to the "Port Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show port trap	27-1
set port trap	27-2
show linkflap	27-2
set linkflap globalstate	27-4
set linkflap portstate	27-5
set linkflap interval	27-6
set linkflap action	27-6
clear linkflap action	27-7
set linkflap threshold	27-7
set linkflap downtime	27-8
clear linkflap down	27-8
clear linkflap	27-9

show port trap

Use this command to display whether the port is enabled for generating an SNMP trap message if its link state changes.

Syntax

show port trap [*port-string*]

Parameters

port-string	(Optional) Displays link trap status for specific port(s).

Defaults

If *port-string* is not specified, the trap status for all ports will be displayed.

Mode

All command modes.

Example

This example shows how to display link trap status for ge.3.1 through 4:

```
S Chassis(rw)->show port trap ge.3.1-4
Link traps enabled on port ge.3.1.
Link traps enabled on port ge.3.2.
Link traps enabled on port ge.3.3.
Link traps enabled on port ge.3.4.
```

set port trap

Use this command to enable or disable ports for sending SNMP trap messages when their link status changes.

Syntax

set port trap *port-string* {**enable** | **disable**}

Parameters

port-string	Specifies the port(s) for which to enable or disable link trap messages.
enable | **disable**	Enables or disables link traps.

Defaults

None.

Mode

All command modes.

Example

This example shows how to disable link traps for slot 3, port 3:

```
S Chassis(rw)->set port trap ge.3.3 disable
```

show linkflap

Use this command to display link flap detection state and configuration information.

Syntax

show linkflap {**globalstate** | **portsupported** | **actsupported** | **maximum** | **downports**} | {**portstate** | **action** | **operstatus** | **threshold** | **interval**] | **downtime** | **currentcount** | **totalcount** | **timelapsed** | **violations** | **parameters** | **metrics**} [*port-string*]

Parameters

globalstate	Displays the global enable state of link flap detection.
portstate	Displays the port enable state of link flap detection.
portsupported	Displays ports which can support the link flap detection function.
actsupported	Displays link flap detection actions supported by system hardware.
maximum	Displays the maximum allowed linkdowns per 10 seconds supported by system hardware.
downports	Displays ports disabled by link flap detection due to a violation.
action	Displays linkflap actions taken on violating port(s).
operstatus	Displays whether linkflap has deactivated port(s).
threshold	Displays the number of allowed link down transitions before action is taken.
interval	Displays the time period for counting link down transitions.
downtime	Displays how long violating port(s) are deactivated.
currentcount	Displays how many linkdown transitions are in the current interval.
totalcount	Displays how many linkdown transitions have occurred since the last reset.
timelapsed	Displays the time period since the last link down event or reset.
violations	Displays the number of link flap violations since the last reset.
parameters	Displays the current value of settable link flap detection parameters.
metrics	Displays linkflap detection metrics.
port-string	(Optional) Displays information for specific port(s).

Defaults

- If *port-string* is not specified, information for all ports will be displayed for the specified parameter.

Mode

All command modes.

Examples

This example shows how to display the global status of the link trap detection function:

```
S Chassis(rw)->show linkflap globalstate
Linkflap feature globally disabled
```

This example shows how to display ports disabled by link flap detection due to a violation:

```
S Chassis(rw)->show linkflap downports
Ports currently held DOWN for Linkflap violations:
None.
```

This example shows how to display the link flap parameters table:

```
S Chassis(rw)->show linkflap parameters
Linkflap Port Settable Parameter Table (X means error occurred)
Port      LF Status  Actions  Threshold   Interval    Downtime
```

```
--------  ---------  -------  ----------  ----------  ----------
ge.1.1    disabled   .......  10          5           300
ge.1.2    enabled    D..S..T  3           5           300
ge.1.3    disabled   ...S..T  10          5           300
```

Table 27-1 provides an explanation of the **show linkflap parameters** command output.

Table 27-1 show linkflap parameters Output Details

Output...	What it displays...
Port	Port designation. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
LF Status	Link flap enabled state.
Actions	Actions to be taken if the port violates allowed link flap behavior. D = disabled, S = Syslog entry will be generated, T= SNMP trap will be generated.
Threshold	Number of link down transitions necessary to trigger the link flap action.
Interval	Time interval (in seconds) for accumulating link down transitions.
Downtime	Interval (in seconds) port(s) will be held down after a link flap violation.

This example shows how to display the link flap metrics table:

```
S Chassis(rw)->show linkflap metrics
Port      LinkStatus   CurrentCount  TotalCount  TimeElapsed  Violations
--------  -----------  ------------  ----------  -----------  -------------
ge.1.1    operational  0             0           241437       0
ge.1.2    disabled     4             15          147          5
ge.1.3    operational  3             3           241402       0
```

Table 27-2 provides an explanation of the **show linkflap metrics** command output.

Table 27-2 show linkflap metrics Output Details

Output...	What it displays...
Port	Port designation. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
LinkStatus	Link status according to the link flap function.
CurrentCount	Link down count accruing toward the link flap threshold.
TotalCount	Number of link downs since system start,
TimeElapsed	Time (in seconds) since the last link down event.
Violations	Number of link flap violations on listed ports since system start.

set linkflap globalstate

Use this command to globally enable or disable the link flap detection function.

Syntax

set linkflap globalstate {**disable** | **enable**}

Parameters

disable | **enable**	Globally disables or enables the link flap detection function.

Defaults

None.

Mode

All command modes.

Usage

By default, the function is disabled globally and on all ports.

Example

This example shows how to globally enable the link trap detection function:

```
S Chassis(rw)->set linkflap globalstate enable
```

set linkflap portstate

Use this command to enable or disable link flap monitoring on one or more ports.

Syntax

set linkflap portstate {**disable** | **enable**} [*port-string*]

Parameters

disable | **enable**	Disables or enables the link flap detection function.
port-string	(Optional) Specifies the port(s) on which to disable or enable monitoring.

Defaults

If *port-string* is not specified, all ports will be disabled or enabled.

Mode

All command modes.

Usage

If disabled globally after per-port settings have been configured using the commands later in this chapter, per-port settings will be retained.

Example

This example shows how to enable the link trap monitoring on all ports:

```
S Chassis(rw)->set linkflap portstate enable
```

set linkflap interval

Use this command to set the time interval (in seconds) for accumulating link down transitions.

Syntax

set linkflap interval *port-string interval_value*

Parameters

port-string	Specifies the port(s) on which to set the link flap interval.
interval_value	Specifies an interval in seconds. A value of 0 will set the interval to forever.

Defaults

interval_value = **5** seconds.

Mode

All command modes.

Example

This example shows how to set the link flap interval on port ge.1.4 to 1000 seconds:

```
S Chassis(rw)->set linkflap interval ge.1.4 1000
```

set linkflap action

Use this command to set reactions to a link flap violation.

Syntax

set linkflap action *port-string* {**disableInterface** | **gensyslogentry** | **gentrap** | **all**}

Parameters

port-string	Specifies the port(s) on which to set the link flap action.
disableInterface	Sets the reaction to disabling the interface.
gensyslogentry	Sets the reaction to generating a Syslog entry.
gentrap	Sets the reaction to generating an SNMP trap message.
all	Sets the reaction to all actions.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the link flap violation action on port ge.1.4 to generating a Syslog entry:

```
S Chassis(rw)->set linkflap action ge.1.4 gensyslogentry
```

clear linkflap action

Use this command to clear reactions to a link flap violation.

Syntax

clear linkflap action *port-string* {**disableInterface** | **gensyslogentry** | **gentrap** | **all**}

Parameters

port-string	Specifies the port(s) on which to clear the link flap action.
disableInterface	Clears the reaction of disabling the interface.
gensyslogentry	Clears the reaction of generating a Syslog entry.
gentrap	Clears the reaction of generating an SNMP trap message.
all	Clears the reaction of all actions.

Defaults

If *port-string* is not specified, actions will be cleared on all ports.

Mode

All command modes.

Example

This example shows how to clear all link flap violation actions on all ports:

```
S Chassis(rw)->clear linkflap action all
```

set linkflap threshold

Use this command to set the link flap action trigger count.

Syntax

set linkflap threshold *port-string threshold_value*

Parameters

port-string	Specifies the port(s) on which to set the link flap action trigger count.
threshold_value	Specifies the number of link down transitions necessary to trigger the link flap action. Must be a minimum value of 1.

Defaults

threshhold_value = **10** down transitions.

Mode

All command modes.

Example

This example shows how to set the link flap threshold on port ge.1.4 to 5:

```
S Chassis(rw)->set linkflap threshold ge.1.4 5
```

set linkflap downtime

Use this command to set the time interval (in seconds) one or more ports will be held down after a link flap violation.

Syntax

set linkflap downtime *port-string downtime_value*

Parameters

port-string	Specifies the port(s) on which to set the link flap downtime.
downtime_value	Specifies a downtime in seconds. A value of 0 will set the downtime to forever.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the link flap downtime on port ge.1.4 to 5000 seconds:

```
S Chassis(rw)->set linkflap downtime ge.1.4 5000
```

clear linkflap down

Use this command to toggle link flap disabled ports to operational.

Syntax

clear linkflap down [*port-string*]

Parameters

port-string	Specifies the port(s) to make operational.

Defaults

If *port-string* is not specified, all ports disabled by a link flap violation will be made operational.

Mode

All command modes.

Example

This example shows how to make disabled port ge.1.4 operational:

```
S Chassis(rw)->clear linkflap down ge.1.4
```

clear linkflap

Use this command to clear all link flap options and / or statistics on one or more ports.

Syntax

clear linkflap {**all** | **stats** [*port-string*] | **parameter** *port-string* {**threshold** | **interval** | **downtime** | **all**}

Parameters

all	Clears all down ports, actions and statistics for all ports.
stats	Clears all statistics for all or the specified port(s).
parameter	Clears link flap parameters to default values.
threshold | **interval** | **downtime** | **all**	Clears link flap threshold, interval, downtime or all parameters.
port-string	(Optional unless parameter is specified) Specifies the port(s) on which to clear settings.

Defaults

If *port-string* is not specified, settings and/or statistics will be cleared on all ports.

Mode

All command modes.

Examples

This example shows how to clear all link flap options on port ge.1.4:

```
S Chassis(rw)->clear linkflap all ge.1.4
```

This example shows how to clear downtime link flap on port ge.1.1:

```
S Chassis(rw)->clear linkflap parameter ge.1.1 downtime
```

28

Port Priority Configuration

This chapter provides detailed information for the port priority set of commands. For information about configuring port priority, refer to the "Port Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
Configuring Port Priority	28-1
Configuring Priority to Transmit Queue Mapping	28-3

Configuring Port Priority

This section describes the display and configuration of port priority characteristics, including: the display and configuration of the port default CoS transmit priority, traffic class mapping-to-priority of each port, and configuration of the port to transmit frames priority transmit queues.

For information about...	Refer to page...
show port priority	28-1
set port priority	28-2
clear port priority	28-3

show port priority

Use this command to display the 802.1D priority for one or more ports.

Syntax

show port priority [*port-string*]

Parameters

port-string	(Optional) Displays priority information for a the specified port(s).

Defaults

If *port-string* is not specified, priority for all ports will be displayed.

Mode

All command modes.

Example

This example shows how to display the port priority for the ge.2.1 through 5:

```
S Chassis(rw)->show port priority ge.2.1-5
ge.2.1 is set to 0
ge.2.2 is set to 0
ge.2.3 is set to 0
ge.2.4 is set to 0
ge.2.5 is set to 0
```

set port priority

Use this command to set the 802.1D (802.1p) Class-of-Service transmit queue priority (0 through 7) on each port.

Syntax

set port priority *port-string priority*

Parameters

port-string	Specifies the port(s) for which to set priority.
priority	Specifies a value of **0** - **7** to set the CoS port priority for the port entered in the *port-string*. Port priority value of 0 is the lowest priority.

Defaults

None.

Mode

All command modes.

Usage

For commands to to configure protocol-based policy classification to a Class-of-Service, including a CoS policy to override port transmit queue priority, refer to Chapter 45.

When CoS override is enabled using the **set policy profile** command as described in "set policy profile" on page 43-4, CoS-based classification rules will take precedence over priority settings configured with this command.

A port receiving a frame without priority information in its tag header is assigned a priority according to the priority setting on the port. For example, if the priority of a port is set to 5, the frames received through that port without a priority indicated in their tag header are classified as a priority 5. A frame with priority information in its tag header is transmitted according to that priority.

Example

This example shows how to set a default priority of 6 on ge.1.3. Frames received by this port without priority information in their frame header are set to the default setting of 6:

```
S Chassis(rw)->set port priority ge.1.3 6
```

clear port priority

Use this command to reset the current default port priority setting to 0.

Syntax

clear port priority *port-string*

Parameters

port-string	Specifies the port for which to clear priority.

Defaults

None.

Mode

All command modes.

Usage

This command will cause all frames received without a priority value in its header to be set to priority 0.

Example

This example shows how to reset ge.1.11 to the default priority:

```
S Chassis(rw)->clear port priority ge.1.11
```

Configuring Priority to Transmit Queue Mapping

This section describes the display and configuration of transmit queue port mapping.

For information about...	Refer to page...
show port priority-queue	28-3
set port priority-queue	28-4
clear port priority-queue	28-5

show port priority-queue

Use this command to display the port priority levels (0 through 7, with 0 as the lowest level) associated with the current transmit queue (0 - 11 depending on port type, with 0 being the lowest priority) for each priority of the selected port.

Syntax

show port priority-queue [*port-string*]

Parameters

port-string	(Optional) Specifies the port for which to display the priority queue.

Defaults

If *port-string* is not specified, all ports will be displayed.

Mode

All command modes.

Usage

A frame with a certain port priority is transmitted according to the settings entered using the **set priority-queue** command described in "set port priority-queue" on page 28-4.

Example

This example shows how to display priority queue information for ge.1.1. In this case, the frames shown with a priority of 0 or 3 are transmitted according to the transmit priority queue of 1 (the second lowest transmit priority); frames with 1 or 2 priority, at the lowest transmit priority of 0; frames with 4 or 5 priority, at the second highest transmit priority of 2; and frames with 6 or 7 priority, at the highest transmit priority of 3:

```
S Chassis(rw)->show port priority-queue ge.1.1
Port           P0 P1 P2 P3 P4 P5 P6 P7
-------------  -- -- -- -- -- -- -- --
ge.1.1         1  0  0  1  2  2  3  3
```

set port priority-queue

Use this command to map 802.1D (802.1p) priorities to transmit queues.

Syntax

set port priority-queue *port-string priority queue*

Parameters

port-string	Specifies the port(s) for which to set priority queue.
priority	Specifies a value of **0** - **7** (0 is the lowest level) that determines what priority frames will be transmitted at the priority queue level entered in this command.
queue	Specifies a value (0 is the lowest level) that determines when to transmit the frames with the port priority entered in this command. Number of transmit queues varies by port type. Typical values are: • 100Base-T - **4** • 1000Base-T - **4** • 1000Base-X - **8**

Defaults

None.

Mode

All command modes.

Usage

This command enables you to change the priority configured for a priority-queue (0-7, depending on port type, with 0 being the lowest priority queue) for each port priority of the selected port. You can apply the new settings to one or more ports. For example, if the priority queue is set to 3 for those frames with a port priority 4, then those frames would be transmitted before any frames contained in traffic classes 2 through 0.

Example

This example shows how to set priority 5 frames received on ge.2.12 to transmit at the lowest priority queue of 0.

```
S Chassis(rw)->set port priority-queue ge.2.12 5 0
```

clear port priority-queue

Use this command to reset port priority queue settings back to defaults for one or more ports.

Syntax

clear port priority-queue *port-string*

Parameters

port-string	Specifies the port for which to clear the priority queue setting.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear the priority queue settings on ge.2.12:

```
S Chassis(rw)->clear port priority-queue ge.2.12
```

29

Broadcast Suppression Commands

This chapter provides detailed information for the broadcast suppression set of commands. For information about configuring broadcast suppression, refer to the "Port Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show port broadcast	29-1
set port broadcast	29-2
clear port broadcast	29-3

show port broadcast

Use this command to display port broadcast suppression information for one or more ports.

Syntax

show port broadcast [*port-string*]

Parameters

port-string	(Optional) Displays broadcast status for specific port(s).

Defaults

If *port-string* is not specified, broadcast status of all ports will be displayed.

Mode

All command modes.

Example

This example shows how to display broadcast information for port ge.2.2:

```
S Chassis(rw)->show port broadcast ge.2.2
Port          Total BC       Threshold       Peak Rate    Peak Rate Time
              Packets        (pkts/s)        (pkts/s)     (ddd:hh:mm:ss)
-------------------------------------------------------------------------
ge.2.2        165            148810          8            000:05:57:37
```

Table 29-1 provides an explanation of the command output.

Table 29-1 show port broadcast Output Details

Output...	What it displays...
Port	Port designation. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
Total BC Packets	Total broadcast packets received on this port.
Threshold (pkts/s)	Current broadcast threshold in packets per second on this port.
Peak Rate (pkts/s)	Peak rate of broadcast transmission received on this port in packets per second.
Peak Rate Time (ddd:hh:mm:ss)	Time (in day, hours, minutes and seconds) the peak rate was reached on this port.

set port broadcast

Use this command to set the broadcast suppression limit, in packets per second, on one or more ports.

Syntax

set port broadcast *port-string threshold-val*

Parameters

port-string	Specifies the port(s) for which to set broadcast suppression.
threshold-val	Sets the number of packets allowed to be received per second threshold on broadcast traffic. Maximum value is 1488100. If set to the maximum value, thresholding will be disabled. Default value: **1488100**.

Defaults

None.

Mode

All command modes.

Usage

Broadcast suppression sets a threshold on the broadcast traffic that is received and switched out to other ports.

Example

This example shows how to set broadcast suppression to 800 packets per second on ports ge.1.1 through 5:

```
S Chassis(rw)->set port broadcast ge.1.1-5 800
```

clear port broadcast

Use this command to reset the broadcast threshold and/or clear the peak rate and peak time values on one or more ports.

Syntax

clear port broadcast *port-string* {[**threshold**] [**peak**]}

Parameters

port-string	Specifies the port(s) on which broadcast settings will be cleared.
threshold	(Optional) Clears the broadcast threshold setting.
peak	(Optional) Clears the broadcast peak rate and peak rate time values.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to clear all broadcast suppression settings on ports ge.1.1 through 5:

```
S Chassis(rw)->clear port broadcast ge.1.1-5 threshold peak
```

This example shows how to clear threshold broadcast suppression settings on ports ge.1.1 through 5:

```
S Chassis(rw)->clear port broadcast ge.1.1-5 threshold
```

30

Port Mirroring Commands

Caution: Port mirroring configuration should be performed only by personnel who are knowledgeable about the effects of port mirroring and its impact on network operation.

This chapter provides detailed information for the port mirroring set of commands. For information about configuring port mirroring, refer to the "Port Mirroring Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
Physical Port Mirroring	30-1
Policy Mirror Destinations	30-7

Physical Port Mirroring

This section describes how to display, create, and delete port mirrors for VLANs or ports on an S-Series device.

For information about...	Refer to page...
show port mirroring	30-1
set port mirroring	30-2
show port mirroring enhanced	30-3
set port mirroring enhanced	30-4
set port mirroring orl	30-5
clear port mirroring	30-6
clear port mirroring orl	30-6

show port mirroring

Use this command to display the source and target ports for mirroring, and whether mirroring is currently enabled or disabled for those ports.

Syntax

```
show port mirroring
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display port mirroring information:

```
S Chassis(rw)->show port mirroring
Port Mirroring
==============

 Source Port        = lag.0.60
 Target Port        = lag.0.122
 Frames Mirrored    = Rx and Tx
 Admin Status       = enabled
 Operational Status = enabled

Mirror Outbound Rate Limited Frames : Disabled
```

set port mirroring

Use this command to create a new mirroring relationship or to enable or disable an existing mirroring relationship between two ports.

Syntax

set port mirroring {**create** | **disable** | **enable**} *source destination* [**both** | **rx** | **tx**]

Parameters

create | **disable** | **enable**	Creates, disables or enables mirroring settings on the specified ports.
source	Specifies the source port designation. This is the port on which the traffic will be monitored.
destination	Specifies the target port designation. This is the port that will duplicate or "mirror" all the traffic on the monitored port.
both | **rx** | **tx**	(Optional) Specifies that frames received and transmitted by the source port, only frames received, or only frames transmitted will be mirrored.

Defaults

If not specified, **both** received and transmitted frames will be mirrored.

Mode

All command modes.

Usage

A port mirror is automatically enabled when created.

An IDS mirror is a one-to-many port mirror that has been designed for use with an Intrusion Detection System. Ten destination ports must be reserved for an IDS mirror.

To mirror VLAN traffic to a port, you must first create a VLAN MIB-2 interface to use for the SMON MIB using the **set vlan interface create** command. The resulting port is a VTAP (**vtap.0.***vlan-id*). Use the **show port vtap.0.***vlan-id* command to display the VTAP port. To create the port mirror use the **set port mirroring create** command specifying the VTAP and the mirrored port.

Examples

This example shows how to enable port mirroring of transmitted and received frames with ge.1.4 as the source port and ge.1.11 as the target (destination) port:

```
S Chassis(rw)->set port mirroring enable ge.1.4 ge.1.11 both
```

The following example command sequence creates a port mirror for all VLAN 1 traffic, both inbound and outbound on port ge.1.4, by creating the VLAN MIB-2 interface and setting the mirrored port:

```
S Chassis(rw)->set vlan interface 1 create
S Chassis(rw)->set port mirroring create vtap.0.1 ge.1.4 both
```

show port mirroring enhanced

Use this command to display ports enabled for enhanced mirroring.

Syntax

show port mirroring enhanced

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

If this command displays a disabled operational status for an enhanced port mirror, an active port mirror does not exist for this port. Use the show port mirroring command to display all active port mirrors for this device.

Example

This example shows how to enable ports ge.3.1 and ge.3.4 for enhanced port mirroring and to display enhanced port mirroring status for this device:

```
S Chassis(rw)->set port mirroring enhanced enable ge.3.1,4

S Chassis(rw)->show port mirroring enhanced
Enhanced Port Mirroring
=======================

Max Enhanced Mirror Source Ports: 4

Port         Admin Status Oper Status
------------ ------------ ------------
ge.3.1       enabled      enabled
ge.3.4       enabled      disable
S Chassis(rw)->
```

set port mirroring enhanced

Use this command to enable or disable enhanced port mirroring on the specified port(s).

Syntax

set port mirroring enhanced {**enable** | **disable**} *port-string*

Parameters

enable | **disable**	Enables or disables enhanced port mirroring on the specified port(s).
port-string	Specifies the port to enable or disable enhanced port mirroring on.

Defaults

None.

Mode

All command modes.

Usage

Enhanced port mirroring provides for following benefits that non-enhanced port mirrors do not:

- L2/L3 multicast egress frames are mirrored
- CNM (Congestion Notification Message) frames that the switch generates are mirrored
- Mirrored egress frames accurately reflect all reframing actions

A maximum of 4 ports can be enabled for enhanced port mirroring.

An IDS mirror cannot use enhanced mirroring. An enhanced port mirrored to the IDS mirror will use non-enhanced mode.

Examples

In the following example, ports ge.3.1 and ge.3.4 are enabled for enhanced port mirroring. The **show port mirroring enhanced** command displays both ports as enabled for enhanced mirroring. The operational status of ge.3.4 is **disabled** because there is no active mirror for that port as shown in the **show port mirroring** command:

```
S Chassis(rw)->set port mirroring enhanced enable ge.3.1,4

S Chassis(rw)->show port mirroring enhanced
Enhanced Port Mirroring
=======================
Max Enhanced Mirror Source Ports: 4

Port         Admin Status Oper Status
------------ ------------ ------------
ge.3.1       enabled      enabled
ge.3.4       enabled      disabled
S Chassis(rw)->show port mirroring
Port Mirroring
==============
 Source Port        = ge.3.1
 Target Port        = ge.3.2
 Frames Mirrored    = Rx and Tx
 Admin Status       = enabled
 Operational Status = enabled
S Chassis(rw)->
```

set port mirroring orl

Use this command to enable or disable port mirroring of outbound rate limited frames.

Syntax

set port mirroring orl {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables port mirroring of outbound rate limited frames. Default value: disabled.

Defaults

None.

Mode

All command modes.

Usage

Create a port mirror using the **set port mirroring create** command. See "set port mirroring" on page 30-2 for further information.

The S-Series hardware does not allow for port mirroring of an outbound rate limited frame. By default outbound rate limiting is enabled and port mirroring of an outbound rate limited frame is disabled. Use the **set port mirroring orl enable** command to enable port mirroring of outbound rate limited frames and disable outbound rate limiting for these frames. Use the **set port mirroring orl disable** command to disable port mirroring of outbound rate limited frames and enable outbound rate limiting of these frames. This command is applied to all port mirrors.

Use the **clear port mirroring orl** command to set the port mirroring behavior of outbound rate limited frames to its default behavior: disabled. See "clear port mirroring orl" on page 30-6 for further details.

Examples

This example shows how to enable port mirroring of outbound rate limited frames and disable outbound rate limiting for these frames:

```
S Chassis(rw)->set port mirroring orl enable
```

clear port mirroring

Use this command to clear a port mirroring relationship.

Syntax

clear port mirroring *source | destination*

Parameters

source	Specifies the source port of the mirroring configuration to be cleared.
destination	Specifies the target port of the mirroring configuration to be cleared.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear port mirroring between source port ge.1.4 and target port ge.1.11:

```
S Chassis(rw)->clear port mirroring ge.1.4 ge.1.11
```

clear port mirroring orl

Use this command to clear the port mirroring of outbound rate limited frames configuration.

Syntax

clear port mirroring orl

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

This command sets the **set port mirroring orl** configuration to the default value of disabled. See "set port mirroring orl" on page 30-5 for further information.

Example

This example shows how to the clear port mirroring orl configuration:

```
S Chassis(rw)->clear port mirroring orl
```

Policy Mirror Destinations

This section describes how to display, create, enable, disable, and delete mirror destinations that are associated with a specific policy rule or profile.

The mirror destination mirrors only the traffic specified in an associated policy. If a source port is associated with both a physical port mirror and a policy mirror destination, the policy mirror destination takes precedence over the physical port mirror: the source port traffic specified in the associated policy is mirrored only at the policy mirror destination port, not at the physical port mirror.

For example, consider a physical port mirror, such that the traffic received at source port ge.1.1 is mirrored on the destination port ge.1.2. Port ge.1.1 is also associated with a policy for Web traffic (TCP port 80). That policy has a policy mirror destination with ge.1.3 as the destination port. Because the policy mirror destination takes precedence over the physical port mirror, the Web traffic for port ge.1.1 is mirrored to port ge.1.3 only. Port ge.1.2 mirrors all other traffic with the exception of the Web traffic.

For information about...	Refer to page...
set mirror create	30-8
set mirror enable	30-8
set mirror disable	30-9
set mirror mirrorN	30-9
set mirror ports	30-10
set mirror	30-10
clear mirror ports	30-11
clear mirror	30-11
show mirror	30-12

set mirror create

Use this command to create a mirror destination. After you have created a mirror destination, you must assign a port to the mirror destination using the set mirror ports command and assign the mirror destination to a policy rule (using the set policy rule command) or a policy role (using the set policy profile command).

Syntax

set mirror create *control-index*

Parameters

control-index	The index number (1–255) that identifies the mirror destination. The **set policy rule** and the **set policy profile** commands refer to this number as the mirror-index.

Defaults

None.

Mode

All command modes.

Example

This example shows how to create mirror destination 1:

```
S Chassis(rw)->set mirror create 1
```

set mirror enable

Use this command to enable one or all mirror destinations.

Syntax

set mirror enable *control-index*

Parameters

control-index	The index number (1–255) that identifies the mirror destination.

Defaults

None.

Mode

All command modes.

Example

This example shows how to enable mirror destination 1:

```
S Chassis(rw)->set mirror enable 1
```

set mirror disable

Use this command to disable one or all mirror destinations.

Syntax

set mirror disable *control-index*

Parameters

control-index	The index number (1–255) that identifies the mirror destination.

Defaults

None.

Mode

All command modes.

Example

This example shows how to disable mirror destination 1:

```
S Chassis(rw)->set mirror disable 1
```

set mirror mirrorN

Use this command to specify the number of packets at the beginning of a flow to mirror.

Syntax

set mirror *control-index* **mirrorN** *mirrorN-packets*

Parameters

control-index	The index number (1–255) that identifies the mirror destination. The mirror must be a manually created mirror.
mirrorN *mirrorN-packets*	The number of packets at the beginning of a flow to mirror. The maximum value is **31** packets.

Defaults

None.

Mode

All command modes.

Example

This example shows how to mirror the first twenty packets in a flow:

```
S Chassis(rw)->set mirror 1 mirrorN 20
```

set mirror ports

Use this command to associate one or more ports with a mirror destination.

Syntax

set mirror ports *port-string control-index-list* [**append**]

Parameters

port-string	Port or range of ports to be associated with this mirror destination. You can associate physical ports or LAGs with a mirror destination, but you cannot associate both in the same mirror destination.
control-index-list	The index number (1–255) that identifies the mirror destination.
append	(Optional) Append this information to the previously entered mirror destination. Not using the append parameter will overwrite what you have previously configured for the mirror destination.

Defaults

None.

Mode

All command modes.

Example

This example shows how to associate port ge.1.1 with mirror destination 25 without overwriting any previous port associations:

```
S Chassis(rw)->set mirror ports ge.1.1 25 append
```

set mirror

Use this command to change the storage type or indicate the owner of a mirror destination.

Syntax

set mirror *control-index-list* [**storage-type** {**non-volatile** | **volatile**} | **owner** *owner*]

Parameters

control-index-list	The index number (1–255) that identifies the mirror destination.
storage-type non-volatile | **volatile**	The storage option for the mirror destination: • **non-volatile** — The mirror destination is stored in non-volatile memory. • **volatile** — The mirror destination is stored in volatile memory.
owner *owner*	Administratively assigned name of the owner of this entity.

Defaults

The default setting for **storage-type** is *non-volatile*.

Mode

All command modes.

Example

This example shows how to set the owner of mirror destination 1:

```
S Chassis(rw)->set mirror 1 owner lab
```

clear mirror ports

Use this command to clear a mirror destination from a port or ports.

Syntax

clear mirror ports *port-string control-index-list*

Parameters

port-string	Port or range of ports to be associated with this mirror destination.
control-index-list	The index number (1–255) that identifies the mirror destination.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear a port association with mirror destination 25:

```
S Chassis(rw)->clear mirror ports ge.1.1 25
```

clear mirror

Use this command to clear the storage type or the owner of a mirror destination.

Syntax

clear mirror *control-index-list* [**storage-type** {**non-volatile** | **volatile**} | **owner** *owner*]

Parameters

control-index-list	The index number (1–255) that identifies the mirror destination.
storage-type non-volatile | **volatile**	The storage option for the mirror destination: • **non-volatile** — The mirror destination is stored in non-volatile memory. • **volatile** — The mirror destination is stored in volatile memory.
owner *owner*	Administratively assigned name of the owner of this entity.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear mirror destination 1:

```
S Chassis(rw)->clear mirror 1
```

show mirror

Use this command to display one or all mirror destinations.

Syntax

show mirror [*control-index*]

Parameters

control-index	(Optional) The mirror index to display.

Defaults

If *control-index* is not specified, all mirrors are displayed.

Mode

All command modes.

Example

This example shows how to show the policy mirror destination:

```
S Chassis(rw)->show mirror
Mirror Destination

Max local mirrors                   : 4
Max local mirror destination ports  : 40352

S Chassis(su)->show mirror 1
Mirror Destination

Index  Port           Status         Storage Type  Owner
-----  -------------  -------------  ------------  ----------------------------
    1                 Active         non-volatile
```

31

LACP Commands

This chapter provides detailed information for the Link Aggregation Control Protocol (LACP) set of commands. For information about configuring LACP, refer to the "Link Aggregation Control Protocol (LACP) Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show lacp	31-2
set lacp	31-3
clear lacp state	31-4
set lacp asyspri	31-4
set lacp aadminkey	31-5
clear lacp	31-5
set lacp static	31-6
clear lacp static	31-7
show lacp singleportlag	31-7
set singleportlag	31-8
clear singleportlag	31-8
show port lacp	31-9
set port lacp	31-10
clear port lacp	31-12
show lacp flowRegeneration	31-13
set lacp flowRegeneration	31-13
clear lacp flowRegeneration	31-14
show lacp outportAlgorithm	31-14
set lacp outportAlgorithm	31-15
clear lacp outportAlgorithm	31-15

show lacp

Use this command to display the global LACP enable state, or to display information about one or more aggregator ports.

Syntax

show lacp [**state** | *port-string*]

Parameters

state	(Optional) Displays the global LACP enable state.
port-string	(Optional) Displays LACP information for specific LAG port(s). Valid port designations are lag.0.1-48.

Defaults

- If **state** is not specified, aggregator information will be displayed for specified ports.
- If *port-string* is not specified, link aggregation information for all ports will be displayed.

Mode

All command modes.

Usage

Each Extreme Networks S-Series module provides 48 virtual link aggregator ports, which are designated in the CLI as **lag.0.1** through **lag.0.48** . Once underlying physical ports (i.e., **ge.x.x**) are associated with an aggregator port, the resulting aggregation will be represented as one Link Aggregation Group (LAG) with a **lag.x.x** port designation.

Example

This example shows how to display information for aggregator port 107:

```
S Chassis(rw)->show lacp lag.0.107
Global Link Aggregation state: enabled
Single Port LAGs:              enabled

Aggregator:  lag.0.107
                           Actor                 Partner
System Identifier:  00:1f:45:9a:6c:b7      00:00:00:00:00:00
  System Priority:              32768                  32768
        Admin Key:              32768
         Oper Key:              32768                  32768
   Attached Ports:  None.
    Standby Ports:  None.
```

Table 31-1 provides an explanation of the command output.

Table 31-1 show lacp Output Details

Output...	What it displays...
Global Link Aggregation state	Link Aggregation state.

Table 31-1 show lacp Output Details (continued)

Output...	What it displays...
Single Port LAGs	Single port LAG feature. By default, a LAG must contain two or more actor and partner port pairs for the LAG to be initiated by this device. The single port LAG feature allows for the creation of a single port LAG.
Aggregator	LAG port designation. Each Extreme Networks S-Series module provides 48 virtual link aggregator ports, which are designated in the CLI as **lag.0.1** through **lag.0.48**. Once underlying physical ports (i.e., **ge.x.x**) are associated with an aggregator port, the resulting Link Aggregation Group (LAG) is represented with a **lag.x.x** port designation.
Actor	Local device participating in LACP negotiation.
Partner	Remote device participating in LACP negotiation.
System Identifier	MAC addresses for actor and partner.
System Priority	System priority value which determines aggregation precedence. Only one LACP system priority can be set on a Extreme Networks S-Series device, using either the **set lacp asyspri** command ("set lacp asyspri" on page 31-4), or the **set port lacp** command ("set port lacp" on page 31-10).
Admin Key	The LAG port's administratively assigned key.
Oper Key	The LAG port's operational key, derived from the admin key. Only underlying physical ports with oper keys matching the aggregator's will be allowed to aggregate.
Attached Ports	Underlying physical ports associated with this aggregator.
Standby Ports	List of standby ports. An available aggregatable port for a LAG with all resources depleted or a speed mismatch is placed in LACP standby state. If a port is in standby mode, the **show port lacp port status detail** command (see "show port lacp" on page 31-9) displays the reason the port is in standby mode.

set lacp

Use this command to disable or enable the Link Aggregation Control Protocol (LACP) on the device. LACP is enabled by default.

Syntax

```
set lacp {disable | enable}
```

Parameters

disable | **enable**	Disables or enables LACP. LACP is enabled by default.

Defaults

None.

Mode

All command modes.

Example

This example shows how to disable LACP:

```
S Chassis(rw)->set lacp disable
```

clear lacp state

Use this command to reset LACP to the default state of enabled.

Syntax

clear lacp state

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset LACP to enabled:

```
S Chassis(rw)->clear lacp state
```

set lacp asyspri

Use this command to set the LACP system priority.

Syntax

set lacp asyspri *value*

Parameters

value	Specifies a system priority value. Valid values are **0** to **65535**, with precedence given to lower values.

Defaults

None.

Mode

All command modes.

Usage

Only one LACP system priority can be set on a Extreme Networks S-Series device, using either this command, or the **set port lacp** command (“set port lacp” on page 31-10).

LACP uses this value to determine aggregation precedence. If there are two partner devices competing for the same aggregator, LACP compares the LAG IDs for each grouping of ports. The LAG with the lower LAG ID is given precedence and will be allowed to use the aggregator.

Example

This example shows how to set the LACP system priority to 1000:

```
S Chassis(rw)->set lacp asyspri 1000
```

set lacp aadminkey

Use this command to set the administratively assigned key for one or more aggregator ports. LACP will use this value to form an oper key.

Syntax

set lacp aadminkey *port-string value*

Parameters

port-string	Specifies the LAG port(s) on which to assign an admin key.
value	Specifies an admin key value to set. Valid values are **0** to **65535**.

Defaults

None.

Mode

All command modes.

Usage

Only underlying physical ports with oper keys matching those of their aggregators will be allowed to aggregate.

LACP commands and parameters beginning with an "a" (such as **aadminkey**) set actor values. Actor refers to the local device participating in LACP negotiation.

Example

This example shows how to set the LACP admin key to 2000 for LAG port 48:

```
S Chassis(rw)->set lacp aadminkey lag.0.48 2000
```

clear lacp

Use this command to clear LACP system priority or admin key settings.

Syntax

clear lacp {[**asyspri**] [**aadminkey** *port-string*]}

Parameters

asyspri	Clears system priority.
aadminkey *port-string*	Clears admin keys for one or more ports.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear the actor admin key for LAG port 48:

```
S Chassis(rw)->clear lacp aadminkey lag.0.48
```

set lacp static

Use this command to assign one or more underlying physical ports to a Link Aggregation Group (LAG).

Syntax

set lacpstatic *lagportstring* [*key*] *port-string*

Parameters

lagportstring	Specifies the LAG aggregator port to which new ports will be assigned.
key	(Optional) Specifies the new member port and LAG port aggregator admin key value. Only ports with matching keys are allowed to aggregate. Valid values are **0** - **65535**. **Notes:** This key value must be unique. If ports other than the desired underlying physical ports share the same admin key value, aggregation will fail or undesired aggregations will form.
port-string	Specifies the member port(s) to add to the LAG.

Defaults

If not specified, a *key* will be assigned according to the specified aggregator. For example a key of 4 would be assigned to lag.0.4.

Mode

All command modes.

Usage

At least two ports need to be assigned to a LAG port for a Link Aggregation Group to form and attach to the specified LAG port.

The same usage considerations for dynamic LAGs apply to statically created LAGs. See the *Extreme Networks S-Series Configuration Guide* for details.

Static LAG configuration should be performed by personnel who are knowledgeable about Link Aggregation. Misconfiguration can result in LAGs not being formed, or in ports attaching to the wrong LAG port, affecting proper network operation.

Example

This example shows how to add port ge.1.6 to the LAG of aggregator port 48:

```
S Chassis(rw)->set lacp static lag.0.48 ge.1.6
```

clear lacp static

Use this command to remove specific ports from a Link Aggregation Group.

Syntax

clear lacp static *lagportstring port-string*

Parameters

lagportstring	Specifies the LAG aggregator port from which ports will be removed.
port-string	Specifies the port(s) to remove from the LAG.

Defaults

None.

Mode

All command modes.

Example

This example shows how to remove port ge.1.6 from the LAG of aggregator port 48:

```
S Chassis(rw)->clear lacp static lag.0.48 ge.1.6
```

show lacp singleportlag

Use this command to display the status of the single port LAG function.

Syntax

show lacp singleportlag

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the status of the single port LAG function:

```
S Chassis(rw)->show lacp singleportlag
Single Port LAGs:              enabled
```

set singleportlag

Use this command to enable or disable the formation of single port LAGs.

Syntax

set lacp singleportlag {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables the formation of single port LAGs.

Defaults

None.

Mode

All command modes.

Usage

When enabled, this maintains LAGs when only one port is receiving protocol transmissions from a partner.

Example

This example shows how to enable single port LAGs:

```
S Chassis(rw)->set lacp singleportlag enable
```

clear singleportlag

Use this command to reset the single port LAG function back to the default state of disabled.

Syntax

clear lacp singleportlag

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the single port LAG function back to the default of disabled:

```
S Chassis(rw)->clear lacp singleportlag
```

show port lacp

Use this command to display link aggregation information for one or more underlying physical ports.

Syntax

show port lacp port *port-string* {[**status** {**detail** | **summary**}] | [**counters**]} [**sort** {**port** | **lag**}]

Parameters

port *port-string*	Displays LACP information for specific port(s).
status detail | **summary**	Displays LACP status in detailed or summary information.
counters	Displays LACP counter information.
sort port | **lag**	(Optional) When **summary** is specified, sorts display by port designation or LAG ID.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to display detailed LACP status information for port ge.1.12:

```
S Chassis(rw)-> show port lacp port ge.2.1 status detail

Global Link Aggregation state : enabled

Port Instance:                ge.2.1  Port enable state:               Disabled
ActorPort:                       513  PartnerAdminPort:                     513
ActorSystemPriority:           32768  PartnerOperPort:                      513
ActorPortPriority:             32768  PartnerAdminSystemPriority:         32768
ActorAdminKey:                 32768  PartnerOperSystemPriority:          32768
ActorOperKey:                  32768  PartnerAdminPortPriority:           32768
ActorAdminState:            -----GlA  PartnerOperPortPriority:            32768
ActorOperState:             -F---GlA  PartnerAdminKey:                      513
ActorSystemID:     00-1f-45-9a-6c-b7  PartnerOperKey:                       513
SelectedAggID:                 none  PartnerAdminState:                --DCS-lp
AttachedAggID:                 none  PartnerOperState:                  --DCS-lp
MuxState:                  Detached  PartnerAdminSystemID:    00-00-00-00-00-00
DebugRxState:              Defaulted PartnerOperSystemID:    00-00-00-00-00-00
portStandbyReason:          resource
```

Note: State definitions, such as ActorAdminState and Partner AdminState, are indicated with letter abbreviations. If the **show port lacp** command displays one or more of the following letters, it means the state is true for the associated actor or partner ports:
E = Expired; **F** = Defaulted; **D** = Distributing (tx enabled); **C** = Collecting (rx enabled);
S = Synchronized (actor and partner agree); **G** = Aggregation allowed; **S/I** = Short/Long LACP timeout; **A/p** = Active/Passive LACP.

For more information about these states, refer to set port lacp (

For more information about these states, refer to **set port lacp** (“set port lacp” on page 31-10) and the IEEE 802.3 2002 specification.

This example shows how to display summarized LACP status information for port ge.1.12:

```
S Chassis(rw)->show port lacp port ge.1.12 status summary
Port     AggrActor System   Partner System
                 Pri:   System ID:  Key:  Pri: System ID:     Key:
ge.1.12    none [(32768,00e0639db587,32768),(32768,000000000000, 1411)]
```

This example shows how to display LACP counters for port ge.1.12:

```
S Chassis(rw)->show port lacp port ge.1.12 counters
Port Instance:                          ge.1.12
LACPDUsRx:                         0  MarkerPDUsRX:                          0
LACPDUsTx:                         0  MarkerPDUsTx:                          0
IllegalRx:                         0  MarkerResponsePDUsRx:                  0
UnknownRx:                         0  MarkerResponsePDUsTx:                  0
ActorSyncTransitionCount:          0  PartnerSyncTransitionCount:            0
ActorChangeCount:                  1  PartnerChangeCount:                    0
ActorChurnCount:                   0  PartnerChurnCount:                     0
ActorChurnState:       ChurnMonitor  PartnerChurnState:          ChurnMonitor
MuxState:                  detached
MuxReason:                           BEGIN = TRUE
```

set port lacp

Use this command to set link aggregation parameters for one or more ports.

Syntax

set port lacp port *port-string* {[**aadminkey** *aadminkey*] [**aportpri** *aportpri*] [**aadminstate** {**lacpactive** | **lacptimeout** | **lacpagg** | **lacpsync** | **lacpcollect** | **lacpdist** | **lacpdef** | **lacpexpire**}] [**padminsyspri** *padminsyspri*] [**padminsysid** *padminsysid*] [**padminkey** *padminkey*] [**padminportpri** *padminportpri*] [**padminport** *padminport*] [**padminstate** {**lacpactive** | **lacptimeout** | **lacpagg** | **lacpsync** | **lacpcollect** | **lacpdist** | **lacpdef** | **lacpexpire**}] [**enable** | [**disable**]}

Parameters

port *port-string*	Specifies the physical port(s) on which to configure LACP.
aadminkey *aadminkey*	Sets the port’s actor admin key. LACP will use this value to form an oper key and will determine which underlying physical ports are capable of aggregating by comparing oper keys. Aggregator ports allow only underlying ports with oper keys matching theirs to join their LAG. Valid values are **1** - **65535**.
aportpri *aportpri*	Sets the port’s actor port priority. Valid values are **0** - **65535**, with lower values designating higher priority.

aadminstate lacpactive | lacptimeout | lacpagg | lacpsync | lacpcollect | lacpdist | lacpdef | lacpexpire	Sets the port's actor LACP administrative state to allow for: • **lacpactive -** Transmitting LACP PDUs. • **lacptimeout -** Transmitting LACP PDUs every 1 sec. vs 30 sec. (default). • **lacpagg -** Aggregation on this port. • **lacpsync -** Transition to synchronization state. • **lacpcollect -** Transition to collection state. • **lacpdist -** Transition to distribution state. • **lacpdef** - Transition to defaulted state. • **lacpexpire -** Transition to expired state.
padminsyspri *padminsyspri*	Sets a default value to use as the port's partner priority. Valid values are **0** - **65535**, with lower values given higher priority.
padminsysid *padminsysid*	Sets a default value to use as the port's partner system ID. This is a MAC address.
padminkey *padminkey*	Sets a default value to use as the port's partner admin key. Only ports with matching admin keys are allowed to aggregate. Valid values are **1** - **65535**.
padminportpri *padminportpri*	Sets a default value to use as the port's partner port priority. Valid values are **0** - **65535**, with lower values given higher priority.
padminport *padminport*	Sets a default value to use as the port's partner admin value. Valid values are **1** - **65535**.
padminstate lacpactive | lacptimeout | lacpagg | lacpsync | lacpcollect | lacpdist | lacpdef | lacpexpire	Sets a port's partner LACP administrative state. See **aadminstate** for valid options.
enable	(Optional) Enables LACPDU processing on this port.
disable	(Optional) Disables LACPDU processing on this port. Disabled by default.

Defaults

- At least one parameter must be entered per *port-string.*
- If **enable** or **disable** are not specified, port(s) will be disabled with the LACP parameters entered.

Mode

All command modes.

Usage

These settings will determine the specified underlying physical ports' ability to join a LAG, and their administrative state once aggregated.

LACP commands and parameters beginning with an "a" (such as **aadminkey**) set actor values. Corresponding commands and parameters beginning with a "p" (such as **padminkey**) set corresponding partner values. Actor refers to the local device participating in LACP negotiation,

while partner refers to its remote device partner at the other end of the negotiation. Actors and partners maintain current status of the other via LACPDUs containing information about their ports' LACP status and operational state.

Example

This example shows how to set the actor admin key to 3555 for port ge.3.16:

```
S Chassis(rw)->set port lacp port ge.3.16 aadminkey 3555
```

clear port lacp

Use this command to clear link aggregation settings for one or more ports.

Syntax

clear port lacp port *port-string* {[**aadminkey**] [**aportpri**] [**asyspri**] [**aadminstate** {**lacpactive** | **lacptimeout** | **lacpagg** | **lacpsync** | **lacpcollect** | **lacpdist** | **lacpdef** | **lacpexpire** | **all**}] [**padminsyspri**] [**padminsysid**] [**padminkey**] [**padminportpri**] [**padminport**] [**padminstate** {**lacpactive** | **lacptimeout** | **lacpagg** | **lacpsync** | **lacpcollect** | **lacpdist** | **lacpdef** | **lacpexpire** | **all**}]}

Parameters

port *port-string*	Specifies the physical port(s) on which LACP settings will be cleared.
aadminkey	Clears a port's actor admin key.
aportpri	Clears a port's actor port priority.
asyspri	Clears the port's actor system priority.
aadminstate lacpactive | **lacptimeout** | **lacpagg** | **lacpsync** | **lacpcollect** | **lacpdist** | **lacpdef** | **lacpexpire** | **all**	Clears a port's specific actor admin state, or all actor admin state(s). For descriptions of specific states, refer to the **set port lacp** command ("set port lacp" on page 31-10.)
padminsyspri	Clears the port's default partner priority value.
padminsysid	Clears the port's default partner system ID.
padminkey	Clears the port's default partner admin key.
padminportpri	Clears the port's default partner port priority.
padminport	Deletes a partner port from the LACP configuration.
padminstate lacpactive | **lacptimeout** | **lacpagg** | **lacpsync** | **lacpcollect** | **lacpdist** | **lacpdef** | **lacpexpire** | **all**	Clears the port's specific partner admin state, or all partner admin state(s).

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear all link aggregation parameters for port ge.3.16:

```
S Chassis(rw)->clear port lacp port ge.3.16
```

show lacp flowRegeneration

Use this command to display the LACP flow regeneration state.

Syntax

show lacp flowRegeneration

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the current LACP flow regeneration state:

```
S Chassis(rw)->show lacp flowRegeneration
disable
```

set lacp flowRegeneration

Use this command to enable or disable LACP flow regeneration.

Syntax

set lacp flowRegeneration {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables LACP flow regeneration

Defaults

Disabled.

Mode

All command modes.

Usage

When enabled and a new port joins a link aggregation group (LAG), LACP will redistribute all existing flows over the LAG. It will also attempt to load balance existing flows to take advantage of ports added to the LAG. When flow regeneration is disabled and a new port joins a LAG, LACP will only distribute new flows over the increased number of ports in the LAG and will leave existing flows intact.

Example

This example shows how to enable LACP flow regeneration:

```
S Chassis(rw)->set lacp flowRegeneration enable
```

clear lacp flowRegeneration

Use this command to reset LACP flow regeneration to its default state (disabled).

Syntax

`clear lacp flowRegeneration`

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset LACP flow regeneration to disabled:

```
S Chassis(rw)->clear lacp flowRegeneration
```

show lacp outportAlgorithm

Use this command to display the current LACP outport algorithm.

Syntax

`show lacp outportAlgorithm`

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the current LACP output algorithm:

```
S Chassis(rw)->show lacp outportAlgorithmoutport algorithm
dip-sip
```

set lacp outportAlgorithm

Use this command to set the algorithm LACP will use for outport determination.

Syntax

```
set lacp outportAlgorithm {dip-sip | da-sa | round-robin}
```

Parameters

dip-sip	Specifies that destination and source IP addresses will determine the LACP outport.
da-sa	Specifies that destination and source MAC addresses will determine the LACP outport.
round-robin	Specifies that the round-robin algorithm will determine the LACP outport.

Defaults

DIP-SIP.

Mode

All command modes.

Usage

The outport algorithm defaults to **DIP-SIP**.

Example

This example shows how to set the LACP outport algorithm to DA-SA:

```
S Chassis(rw)->set lacp outportalgorithm da-sa
```

clear lacp outportAlgorithm

Use this command to reset LACP to DIP-SIP, its default outport algorithm.

Syntax

```
clear lacp outportAlgorithm
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the LACP outport algorithm to DIP-SIP:

```
S Chassis(rw)->clear lacp outportAlgorithm
```

32

SNMP User, Group, and Community Commands

This chapter provides detailed information for the SNMP user, group, and community set of commands. SNMP user, group, and community functionality includes configuring group access and SNMP access rights. For information about configuring SNMP users, groups, and communities, refer to the "Simple Network Management Protocol (SNMP) Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
Configuring SNMP Users, Groups, and Communities	32-1
Configuring SNMP Access Rights	32-10

Configuring SNMP Users, Groups, and Communities

The commands in this section are used to review and configure SNMPv3 users, groups, and v1 and v2 communities. By definition:

- User — A person registered in SNMPv3 to access SNMP management.
- Group — A collection of users who share the same SNMP access privileges.
- Community — A name used to authenticate SNMPv1 and v2 users.

For information about...	Refer to page...
show snmp user	32-2
set snmp user	32-3
clear snmp user	32-4
set snmp engineid	32-5
clear snmp engineid	32-5
show snmp group	32-6
set snmp group	32-7
clear snmp group	32-8
show snmp community	32-8
set snmp community	32-9
clear snmp community	32-10

show snmp user

Use this command to display information about SNMPv3 users. SNMP users are people registered to access SNMP management.

Syntax

show snmp user [**list**] | [*user*] | [**remote** *remote*] [**volatile** | **nonvolatile** | **read-only**]

Parameters

list	(Optional) Displays a list of registered SNMP user names.
user	(Optional) Displays information about a specific user.
remote *remote*	(Optional) Displays information about users on a specific remote SNMP engine.
volatile | **nonvolatile** | **read-only**	(Optional) Displays user information for a specified storage type.

Defaults

- If **list** is not specified, detailed SNMP information will be displayed.
- If *user* is not specified, information about all SNMP users will be displayed.
- If **remote** is not specified, user information about the local SNMP engine will be displayed.
- If not specified, user information for all storage types will be displayed.

Mode

All command modes.

Examples

This example shows how to display an SNMP user list:

```
S Chassis(rw)->show snmp user list
--- SNMP user information ---
--- List of registered users:
Guest
admin1
admin2
netops
```

This example shows how to display information for the SNMP “guest” user:

```
S Chassis(rw)->show snmp user guest
--- SNMP user information ---
EngineId:  00:00:00:63:00:00:00:a1:00:00:00:00
Username                = Guest
Auth protocol           = usmNoAuthProtocol
Privacy protocol        = usmNoPrivProtocol
Storage type            = nonVolatile
Row status              = active
```

Table 32-1 shows a detailed explanation of the command output.

Table 32-1 show snmp user Output Details

Output...	What it displays...
EngineId	SNMP engine identifier associated with the user.
Username	SNMPv1 or v2 community name or SNMPv3 user name.
Auth protocol	Type of authentication protocol applied to this user.
Privacy protocol	Whether a privacy protocol is applied when authentication protocol is in use.
Storage type	Whether entry is stored in **volatile**, **nonvolatile,** or **read-only** memory.
Row status	Status of this entry: **active**, **notInService,** or **notReady**.

set snmp user

Use this command to create a new SNMPv3 user.

Syntax

```
set snmp user user [remote remoteid] [authentication {md5 | sha}] [encryption {des
| aes}][privacy privpassword] [volatile | nonvolatile]
```

Parameters

user	Specifies a name for the SNMPv3 user.
remote *remoteid*	(Optional) Registers the user on a specific remote SNMP engine.
authentication md5 | **sha**	(Optional) Specifies the authentication type required for this user as MD5 or SHA. The MD5 option is not available if the security mode is set to C2. In C2 security mode, authentication is not an optional parameter.
encryption {**des** | **aes**}	(Optional) Sets the privacy protocol to Advanced Encryption Standard (AES) or Data Encryption Standard (DES). The DES encryption option is not available if the security mode is set to C2. In C2 security mode, encryption is not an optional parameter.
privacy *privpassword*	(Optional) Applies encryption and specifies an encryption password. Minimum of 8 characters.
volatile | **nonvolatile**	(Optional) Specifies a storage type for this user entry.

Defaults

- If **remote** is not specified, the user will be registered for the local SNMP engine.
- In normal security mode, if **authentication** is not specified, no authentication will be applied.
- In normal security mode, if **encryption** is not specified, the **aes** privacy protocol will be applied.
- If **privacy** is not specified, no encryption will be applied.
- If storage type is not specified, **nonvolatile** will be applied.

Mode

All command modes. If security profile mode is set to C2: Super-User (su) management access only.

Usage

The authentication password and encryption privacy password are interactively entered and are not part of the CLI entry. Both the authentication and privacy passwords must be at least 8 characters in length.

In C2 security mode, both authentication and encryption are not optional parameters. Both parameters must be entered.

In C2 security mode, you can not create, delete, or modify an SNMP user while in Read-Write user mode.

Examples

This example shows how to create a new SNMP user named "netops**".** By default, this user will be registered on the local SNMP engine without authentication and encryption. Entries related to this user will be stored in permanent (nonvolatile) memory:

```
S Chassis(su)->set snmp user netops
```

This example shows how to configure SNMP user **doc** to be authenticated using SHA-1 authentication and AES encryption. You are interactively required to enter and re-enter both

```
S Chassis(su)->set snmp user doc authentication sha encryption aes
Please enter authentication password:xxxxxxx
Please re-enter authentication password:xxxxxxx
Please enter privacy password:
Please re-enter privacy password:
```

clear snmp user

Use this command to remove a user from the SNMPv3 security-model list.

Syntax

clear snmp user *user* [**remote** *remote*]

Parameters

user	Specifies an SNMPv3 user to remove.
remote *remote*	(Optional) Removes the user from a specific remote SNMP engine.

Defaults

If **remote** is not specified, the user will be removed from the local SNMP engine.

Mode

All command modes.

Usage

In C2 security mode, you can not remove an SNMP user while in Read-Write user mode.

Example

This example shows how to remove the SNMP user named “bill”:

```
S Chassis(rw)->clear snmp user bill
```

set snmp engineid

Use this command to administratively set an SNMP engine ID.

Syntax

set snmp engineid *id*

Parameters

id	Specifies a new SNMP engine ID for this device. Valid values are up to 27 bytes of text or hex characters. For example **sys1** or **15:f8:3a**.

Defaults

None.

Mode

All command modes.

Usage

Changes to the SNMP engine ID require a device reset to take effect. All SNMP user configuration must be removed before resetting the SNMP engine ID.

If C2 security mode is enabled, you can not create, modify, or delete an SNMP engine ID configuration while in Read-Write user mode.

Example

This example shows how to reset the SNMP engine ID to **Documentation**S-Series**1eng1**:

```
S Chassis(rw)->set snmp engineid DocumentationS-Series1eng1
Warning: Changes to the Engine ID require a device reset to take effect.
Warning: All SNMP user configuration must be removed before resetting.
S Chassis(rw)->
```

clear snmp engineid

Use this command to administratively clear an SNMP engine ID.

Syntax

set snmp engineid

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

Changes to the SNMP engine ID require a device reset to take effect. All SNMP user configuration must be removed before resetting the SNMP engine ID.

If C2 security mode is enabled, you can not clear an SNMP engine ID configuration while in Read-Write user mode.

Example

This example shows how to reset the SNMP engine ID to **Documentation**S-Series**1eng1**:

```
S Chassis(rw)->set snmp engineid DocumentationS-Series1eng1
Warning: Changes to the Engine ID require a device reset to take effect.
Warning: All SNMP user configuration must be removed before resetting.
S Chassis(rw)->
```

show snmp group

Use this command to display an SNMP group configuration. An SNMP group is a collection of SNMPv3 users who share the same access privileges.

Syntax

show snmp group [**groupname** *groupname*] [**user** *user*] [**security-model** {**v1** | **v2c** | **usm**}] [**volatile** | **nonvolatile** | **read-only**]

Parameters

groupname *groupname*	(Optional) Displays information for a specific SNMP group.
user *user*	(Optional) Displays information about users within the specified group.
security-model v1 | **v2c** | **usm**	(Optional) Displays information about groups assigned to a specific security SNMP model.
volatile | **nonvolatile** | **read-only**	(Optional) Displays SNMP group information for a specified storage type.

Defaults

- If *groupname* is not specified, information about all SNMP groups will be displayed.
- If *user* is not specified, information about all SNMP users will be displayed.
- If **security-model** is not specified, user information about all SNMP versions will be displayed.
- If no storage types are specified, information for all storage types will be displayed.

Mode

All command modes.

Example

This example shows how to display SNMP group information:

```
S Chassis(rw)->show snmp group
--- SNMP group information ---
Security model          = SNMPv1
Security/user name      = public
Group name              = Anyone
Storage type            = nonVolatile
Row status              = active

Security model          = SNMPv1
Security/user name      = public.router
Group name              = Anyone
Storage type            = nonVolatile
Row status              = active
```

Table 32-2 shows a detailed explanation of the command output.

Table 32-2 show snmp group Output Details

Output...	What it displays...
Security model	SNMP version associated with this group.
Security/user name	User belonging to the SNMP group.
Group name	Name of SNMP group.
Storage type	Whether entry is stored in **volatile**, **nonvolatile** or **read-only** memory.
Row status	Status of this entry: **active**, **notInService**, or **notReady**.

set snmp group

Use this command to create an SNMP group. This associates SNMPv3 users to a group that shares common access privileges.

Syntax

set snmp group *groupname* **user** *user* **security-model** {**v1** | **v2c** | **usm**} [**volatile** | **nonvolatile**]

Parameters

groupname	Specifies an SNMP group name to create.
user *user*	Specifies an SNMPv3 user name to assign to the group.
security-model v1 | **v2c** | **usm**	Specifies an SNMP security model to assign to the group.
volatile | **nonvolatile**	(Optional) Specifies a storage type for SNMP entries associated with the group.

Defaults

If storage type is not specified, **nonvolatile** storage will be applied.

Mode

All command modes.

Example

This example shows how to create an SNMP group called “anyone”, assign a user named “public” and assign SNMPv3 security to the group:

```
S Chassis(rw)->set snmp group anyone user public security-model usm
```

clear snmp group

Use this command to clear SNMP group settings globally or for a specific SNMP group and user.

Syntax

clear snmp group *groupname user* [**security-model** {**v1** | **v2c** | **usm**}]

Parameters

groupname	Specifies the SNMP group to be cleared.
user	Specifies the SNMP user to be cleared.
security-model v1 | **v2c** | **usm**	(Optional) Clears the settings associated with a specific security model.

Defaults

If a **security model** is not specified, settings related to all security models will be cleared.

Mode

All command modes.

Example

This example shows how to clear all settings assigned to the “public” user within the SNMP group “anyone”:

```
S Chassis(rw)->clear snmp group anyone public
```

show snmp community

Use this command to display SNMP community names and status. In SNMPv1 and v2, community names act as passwords to remote management.

Syntax

show snmp community [*name*]

Parameters

name	(Optional) Displays SNMP information for a specific community name.

Defaults

If *name* is not specified, information will be displayed for all SNMP communities.

Mode

All command modes.

Example

This example shows how to display information about the SNMP "public" community name. For a description of this output, refer to "set snmp community" on page 32-9:

```
S Chassis(rw)->show snmp community public

Name            = public
Security name   = public
Context         =
Transport tag   =
Storage type    = nonVolatile
Status          = active
```

set snmp community

Use this command to configure an SNMP community group.

Syntax

set snmp community *community* [**securityname** *securityname*] [**context** *context*] [**transport** *transport*] [**volatile** | **nonvolatile**]

Parameters

community	Specifies a community group name.
securityname *securityname*	(Optional) Specifies an SNMP security name to associate with this community. Default: If no security name is specified, the community name is used.
context *context*	(Optional) Specifies a subset of management information this community will be allowed to access. Valid values are full or partial context names of either MIB object IDs or **router** (the system designated router mode module). Default: All MIB objects. To review all contexts configured for the device, use the **show snmp context** command. **Note:** Beginning with Release 6.0, do not specify the routing module ID as part of the *context*. You must specify router for the system designated router mode module.
transport *transport*	(Optional) Specifies the set of transport endpoints from which SNMP request with this community name will be accepted. Makes a link to a target address table. Default: None.
volatile | **nonvolatile**	(Optional) Specifies the storage type for these entries. Default: nonvolatile.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to set an SNMP community name called “vip”:

```
S Chassis(rw)->set snmp community vip
```

This example shows how to grant SNMP management privileges to “vip” community from the routing module operating in router mode:

```
S Chassis(rw)->set snmp community vip context router
```

clear snmp community

Use this command to delete an SNMP community name.

Syntax

clear snmp community *name*

Parameters

name	Specifies the SNMP community name to clear.

Defaults

None.

Mode

All command modes.

Example

This example shows how to delete the community name “vip.”

```
S Chassis(rw)->clear snmp community vip
```

Configuring SNMP Access Rights

The commands in this section are used to review and configure SNMP access rights and assign viewing privileges and security levels to SNMP user groups.

For information about...	Refer to page...
show snmp access	32-11
set snmp access	32-12
clear snmp access	32-14

show snmp access

Use this command to display access rights and security levels configured for SNMP one or more groups.

Syntax

show snmp access [*groupname*] [**security-model** {**v1** | **v2c** | **usm**}] [**noauthentication** | **authentication** | **privacy**] [**context** *context*] [**volatile** | **nonvolatile** | **read-only**]

Parameters

groupname	(Optional) Displays access information for a specific SNMPv3 group.
security-model v1 | **v2c** | **usm**	(Optional) Displays access information for SNMP security model version 1, 2c or 3 (usm).
noauthentication | **authentication** | **privacy**	(Optional) Displays access information for a specific security level.
context *context*	(Optional) Displays access information for a specific context. For a description of how to specify SNMP contexts, refer to the *Extreme Networks S-Series Configuration Guide*.
volatile | **nonvolatile** | **read-only**	(Optional) Displays access entries for a specific storage type.

Defaults

- If *groupname* is not specified, access information for all SNMP groups will be displayed.
- If **security-mode**l is not specified, access information for all SNMP versions will be displayed.
- If **noauthentication**, **authentication** or **privacy** are not specified, access information for all security levels will be displayed.
- If **context** is not specified, all contexts will be displayed.
- If **volatile**, **nonvolatile** or **read-only** are not specified, all entries of all storage types will be displayed.

Mode

All command modes.

Example

This example shows how to display SNMP access information:

```
S Chassis(rw)->show snmp access
Group           = SystemAdmin
Security model  = USM
Security level  = noAuthNoPriv
Read View       = All
Write View      =
Notify View     = All
Context match   = exact match
Storage type    = nonVolatile
Row status      = active
```

```
Group           = NightOperator
Security model  = USM
Security level  = noAuthNoPriv
Read View       = All
Write View      =
Notify View     = All
Context match   = exact match
Storage type    = nonVolatile
Row status      = active
```

Table 32-3 shows a detailed explanation of the command output.

Table 32-3 show snmp access Output Details

Output...	What it displays...
Group	SNMP group name.
Security model	Security model applied to this group. Valid types are: **SNMPv1**, **SNMPv2c**, and **SNMPv3** (User based - **USM**).
Security level	Security level applied to this group. Valid levels are: noAuthNoPrivacy (**no authentication** required) AuthNoPrivacy (**authentication** required) authPriv (**privacy** -- most secure level)
Read View	Name of the view that allows this group to view SNMP MIB objects.
Write View	Name of the view that allows this group to configure the contents of the SNMP agent.
Notify View	Name of the view that allows this group to send an SNMP trap message.
Context match	Whether or not SNMP context match must be exact (full context name match) or a partial match with a given prefix.
Storage type	Whether access entries for this group are stored in **volatile**, **nonvolatile** or **read-only** memory.
Row status	Status of this entry: **active**, **notInService**, or **notReady**.

set snmp access

Use this command to set an SNMP access configuration.

Syntax

set snmp access *groupname* **security-model** {**v1** | **v2c** | **usm**} [**noauthentication** | **authentication** | **privacy**] [**context** *context*] [**exact** | **prefix**] [**read** *read*] [**write** *write*] [**notify** *notify*] [**volatile** | **nonvolatile**]

Parameters

groupname	Specifies a name for an SNMPv3 group.
security-model v1 | **v2c** | **usm**	Specifies SNMP version 1, 2c or 3 (usm).

noauthentication | **authentication** | **privacy**	(Optional) Applies SNMP security level as no authentication, authentication (without privacy) or privacy. Privacy specifies that messages sent on behalf of the user are protected from disclosure.
context *context* **exact** | **prefix**	(Optional) Sets the context for this access configuration and specifies that the match must be exact (matching the whole context string) or a prefix match only. Context is a subset of management information this SNMP group will be allowed to access. Valid values are full or partial MIB object context names and **router** for the module operating in router mode. To review all contexts configured for the device, use the **`show snmp context`** command. **Note:** Beginning with Release 6.0, do not specify the routing module ID as part of the *context*. You must specify **router** for the system designated router mode module.
read *read*	(Optional) Specifies a read access view.
write *write*	(Optional) Specifies a write access view.
notify *notify*	(Optional) Specifies a notify access view.
volatile | **nonvolatile** | **read-only**	(Optional) Stores associated SNMP entries as temporary or permanent, or read-only.

Defaults

- If security level is not specified, no authentication will be applied.
- If **context** is not specified, access will be enabled for the default context. If **context** is specified without a context match, **exact** match will be applied.
- If **read** view is not specified none will be applied.
- If **write** view is not specified, none will be applied.
- If **notify** view is not specified, none will be applied.
- If storage type is not specified, entries will be stored as permanent and will be held through device reboot.

Mode

All command modes.

Usage

In C2 security mode, you can not create, delete, or modify SNMP access while in Read-Write user mode.

Examples

This example permits the “powergroup” to manage all MIBs via SNMPv3:

```
S Chassis(rw)->set snmp access powergroup security-model usm
```

This example grants the “powergroup” SNMPv3 management access from all router modules when operating in router mode:

```
S Chassis(rw)->set snmp access powergroup security-model usm context router prefix
```

clear snmp access

Use this command to clear the SNMP access entry of a specific group, including its currently configured SNMP security-model and level of security.

Syntax

clear snmp access *groupname* **security-model** {**v1** | **v2c** | **usm**} [**noauthentication** | **authentication** | **privacy**] [**context** *context*]

Parameters

groupname	Specifies the name of the SNMP group for which to clear access.
security-model v1 | **v2c** | **usm**	Specifies the security model to be cleared for the SNMP access group.
noauthentication | **authentication** | **privacy**	(Optional) Clears a specific security level for the SNMP access group.
context *context*	(Optional) Clears a specific context for the SNMP access group. Enter / - / to clear the default context.

Defaults

- If security level is not specified, all levels will be cleared.
- If **context** is not specified, none will be applied.

Mode

All command modes.

Usage

In C2 security mode, you can not clear an SNMP access entry while in Read-Write user mode.

Example

This example shows how to clear SNMP version 3 access for the “mis-group” using the authentication protocol:

```
S Chassis(rw)->clear snmp access mis-group security-model usm authentication
```

33

SNMP MIB View Commands

This chapter provides detailed information for the SNMP MIB set of commands. SNMP views map SNMP objects to access rights. For information about configuring SNMP MIB views, refer to the "Simple Network Management Protocol (SNMP) Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show snmp view	33-1
show snmp context	33-2
set snmp view	33-3
clear snmp view	33-4

show snmp view

Use this command to display the MIB configuration for SNMPv3 view-based access (VACM).

Syntax

show snmp view [*viewname*] [**subtree** *oid-or-mibobject*] [**volatile** | **nonvolatile** | **read-only**]

Parameters

viewname	(Optional) Displays information for a specific MIB view.
subtree *oid-or-mibobject*	(Optional) Displays information for a specific MIB subtree when *viewname* is specified.
volatile | **nonvolatile** | **read-only**	(Optional) Displays entries for a specific storage type.

Defaults

If no parameters are specified, all SNMP MIB view configuration information will be displayed.

Mode

All command modes.

Example

This example shows how to display SNMP MIB view configuration information:

```
S Chassis(rw)->show snmp view
View Name       = All
Subtree OID     = 1
Subtree mask    =
View Type       = included
Storage type    = nonVolatile
Row status      = active

View Name       = All
Subtree OID     = 0.0
Subtree mask    =
View Type       = included
Storage type    = nonVolatile
Row status      = active
```

Table 33-1 provides an explanation of the command output. For details on using the **set snmp view** command to assign variables, refer to "set snmp view" on page 33-3.

Table 33-1 show snmp view Output Details

Output...	What it displays...
View Name	Name assigned to a MIB view.
Subtree OID	Name identifying a MIB subtree.
Subtree mask	Bitmask applied to a MIB subtree.
View Type	Whether or not subtree use must be **included** or **excluded** for this view.
Storage type	Whether storage is in **nonVolatile** or **Volatile** memory.
Row status	Status of this entry: **active**, **notInService**, or **notReady**.

show snmp context

Use this command to display the context list configuration for SNMP's view-based access control.

Syntax

show snmp context

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

An SNMP context is a collection of management information that can be accessed by an SNMP agent or entity. The default context allows all SNMP agents to access all management information (MIBs). When created using the **set snmp access** command, other contexts can be applied to limit access to a subset of management information and to permit SNMP access from one or more routing modules.

Example

This example shows how to display a list of all SNMP contexts known to the device:

```
S Chassis(rw)->show snmp context

--- Configured contexts:
default context (all MIBs)
router
```

set snmp view

Use this command to set a MIB configuration for SNMPv3 view-based access (VACM).

Syntax

set snmp view viewname *viewname* **subtree** *subtree* [**mask** *mask*] [**included** | **excluded**] [**volatile** | **nonvolatile**]

Parameters

viewname *viewname*	Specifies a name for a MIB view.
subtree *subtree*	Specifies a MIB subtree name.
mask *mask*	(Optional) Specifies a bitmask for a subtree.
included | **excluded**	(Optional) Specifies subtree use (default) or no subtree use.
volatile | **nonvolatile**	(Optional) Specifies the use of temporary or permanent (default) storage.

Defaults

- If not specified, **mask** will be set to **255.255.255.255**.
- If not specified, subtree use will be **included**.
- If storage type is not specified, **nonvolatile** (permanent) will be applied.

Mode

All command modes.

Usage

In C2 security mode, you can not create, delete, or modify a MIB configuration for SNMPv3 view-based access while in Read-Write user mode.

Example

This example shows how to set an SNMP MIB view to “public” with a subtree name of 1.3.6.1 included:

```
S Chassis(rw)->set snmp view viewname public subtree 1.3.6.1 included
```

clear snmp view

Use this command to delete an SNMPv3 MIB view.

Syntax

clear snmp view *viewname subtree*

Parameters

viewname	Specifies the MIB view name to be deleted.
subtree	Specifies the subtree name of the MIB view to be deleted.

Defaults

None.

Mode

All command modes.

Usage

In C2 security mode, you can not delete a MIB configuration for SNMPv3 view-based access while in Read-Write user mode.

Example

This example shows how to delete SNMP MIB view “public”:

```
S Chassis(rw)->clear snmp view public 1.3.6.1
```

34

SNMP Parameter and Review Commands

This chapter provides detailed information for the SNMP parameter and review set of commands. SNMP parameter and review functionality includes the setting of SNMP target parameters, target addresses, and notification parameters, the display of SNMP statistics, and the configuration of MIB walk behavior. For information about configuring and reviewing SNMP parameters, refer to the "Simple Network Management Protocol (SNMP) Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
Configuring SNMP Target Parameters	34-1
Configuring SNMP Target Addresses	34-4
Configuring SNMP Notification Parameters	34-7
Configuring SNMP MIB Walk Behavior	34-14
Reviewing SNMP Statistics	34-16

Configuring SNMP Target Parameters

These commands are used to review and configure SNMP target parameters, which control where and under what circumstances SNMP notifications will be sent. A target parameter entry can be bound to a target IP address that is allowed to receive SNMP notification messages with the **set snmp targetaddr** command.

For information about...	Refer to page...
show snmp targetparams	34-1
set snmp targetparams	34-3
clear snmp targetparams	34-4

show snmp targetparams

Use this command to display the SNMP parameters that will be used to generate and send notifications to a target.

Syntax

show snmp targetparams [*targetParams*] [**volatile** | **nonvolatile** | **read-only**]

Parameters

targetParams	(Optional) Displays entries for a specific target parameter.
volatile | **nonvolatile** | **read-only**	(Optional) Displays target parameter entries for a specific storage type.

Defaults

- If *targetParams* is not specified, entries associated with all target parameters will be displayed.
- If storage type is not specified, entries of all storage types will be displayed.

Mode

All command modes.

Example

This example shows how to display SNMP target parameters information:

```
S Chassis(rw)->show snmp targetparams
Target Parameter Name   = v1ExampleParams
Security Name           = public
Message Proc. Model     = SNMPv1
Security Level          = noAuthNoPriv
Storage type            = nonVolatile
Row status              = active

Target Parameter Name   = v2cExampleParams
Security Name           = public
Message Proc. Model     = SNMPv2c
Security Level          = noAuthNoPriv
Storage type            = nonVolatile
Row status              = active

Target Parameter Name   = v3ExampleParams
Security Name           = CharlieDChief
Message Proc. Model     = USM
Security Level          = authNoPriv
Storage type            = nonVolatile
Row status              = active
```

Table 34-1 shows a detailed explanation of the command output.

Table 34-1 show snmp targetparams Output Details

Output...	What it displays...
Target Parameter Name	Unique identifier for the parameter in the SNMP target parameters table. Maximum length is 32 bytes.
Security Name	Security string definition.
Message Proc. Model	SNMP version.

Table 34-1 show snmp targetparams Output Details (continued)

Output...	What it displays...
Security Level	Type of security level (**auth**: security level is set to use authentication protocol, **noauth**: security level is not set to use authentication protocol, or **privacy**).
Storage type	Whether entry is stored in **volatile**, **nonvolatile**, or **read-only** memory.
Row status	Status of this entry: **active**, **notInService**, or **notReady**.

set snmp targetparams

Use this command to set SNMP target parameters, a named set of security/authorization criteria used to generate and send notifications to a target.

Syntax

```
set snmp targetparams paramsname user user security-model {v1 | v2c | usm}
message-processing {v1 | v2c | v3} [noauthentication | authentication | privacy]
[volatile | nonvolatile]
```

Parameters

paramsname	Specifies a name identifying parameters used to generate SNMP messages to a particular target.
user *user*	Specifies an SNMPv1 or v2 community name or an SNMPv3 user name. Maximum length is 32 bytes.
security-model v1 | **v2c** | **usm**	Specifies the SNMP security model applied to this target parameter as version 1, 2c or 3 (usm).
message-processing v1 | **v2c** | **v3**	Specifies the SNMP message processing model applied to this target parameter as version 1, 2c or 3.
noauthentication | **authentication** | **privacy**	(Optional) Specifies the SNMP security level applied to this target parameter as no authentication, authentication (without privacy) or privacy. Privacy specifies that messages sent on behalf of the user are protected from disclosure.
volatile | **nonvolatile**	(Optional) Specifies the storage type applied to this target parameter.

Defaults

- If not specified, security level will be set to **noauthentication**.
- If not specified, storage type will be set to **nonvolatile**.

Mode

All command modes.

Usage

In C2 security mode, you can not create, delete, or modify an SNMP target parameters configuration access while in Read-Write user mode.

Example

This example shows how to set SNMP target parameters named "v1ExampleParams" for a user named "fred" using the SNMPv3 security model, message processing, and authentication:

```
S Chassis(rw)->set snmp targetparams v1ExampleParams user fred security-model usm
message-processing v3 authentication
```

clear snmp targetparams

Use this command to clear the SNMP target parameter configuration.

Syntax

clear snmp targetparams *targetParams*

Parameters

targetParams	Specifies the name of the parameter in the SNMP target parameters table to be cleared.

Defaults

None.

Mode

All command modes.

Usage

In C2 security mode, you can not clear an SNMP target parameters configuration while in Read-Write user mode.

Example

This example shows how to clear SNMP target parameters named "v1ExampleParams":

```
S Chassis(rw)->clear snmp targetparams v1ExampleParams
```

Configuring SNMP Target Addresses

The commands in this section are used to review and configure SNMP target addresses which will receive SNMP notification messages. An address configuration can be linked to optional SNMP transmit, or target, parameters (such as timeout, retry count, and UDP port) with parameters that have been set with the **set snmp targetparams** command.

For information about...	Refer to page...
show snmp targetaddr	34-5
set snmp targetaddr	34-6
clear snmp targetaddr	34-7

show snmp targetaddr

Use this command to display SNMP target address information.

Syntax

show snmp targetaddr [*targetAddr*] [**volatile** | **nonvolatile** | **read-only**]

Parameters

targetAddr	(Optional) Displays information for a specific target address name.
volatile | **nonvolatile** | **read-only**	(Optional) When target address is specified, displays target address information for a specific storage type.

Defaults

- If *targetAddr* is not specified, entries for all target address names will be displayed.
- If not specified, entries of all storage types will be displayed for a target address.

Mode

All command modes.

Example

This example shows how to display SNMP target address information:

```
S Chassis(rw)->show snmp targetaddr
Target Address Name     = labmachine
Tag List                = v2cTrap
IP Address              = 10.2.3.116
UDP Port#               = 162
Target Mask             = 255.255.255.255
Timeout                 = 1500
Retry count             = 4
Parameters              = v2cParams
Storage type            = nonVolatile
Row status              = active
```

Table 34-2 shows a detailed explanation of the command output.

Table 34-2 show snmp targetaddr Output Details

Output...	What it displays...
Target Address Name	Unique identifier in the snmpTargetAddressTable.
Tag List	Tags a location to the target address as a place to send notifications.
IP Address	Target IP address.
UDP Port#	Number of the UDP port of the target host to use.
Target Mask	Target IP address mask.
Timeout	Timeout setting for the target address.
Retry count	Retry setting for the target address.

Table 34-2 show snmp targetaddr Output Details (continued)

Output...	What it displays...
Parameters	Entry in the snmpTargetParamsTable.
Storage type	Whether entry is stored in **volatile**, **nonvolatile**, or **read-only memory**.
Row status	Status of this entry: **active**, **notInService**, or **notReady**.

set snmp targetaddr

Use this command to configure an SNMP target address.

Syntax

set snmp targetaddr *targetaddr ipaddr* **param** *param* [**udpport** *udpport*] [**mask** *mask*] [**timeout** *timeout*] [**retries** *retries*] [**taglist** *taglist*] [**volatile** | **nonvolatile**]

Parameters

targetaddr	Specifies a unique identifier to index the snmpTargetAddrTable. Maximum length is 32 bytes.
ipaddr	Specifies the IP address of the target.
param *param*	Specifies an entry in the SNMP target parameters table, which is used when generating a message to the target. Maximum length is 32 bytes.
udpport *udpport*	(Optional) Specifies which UDP port of the target host to use. Default value is 162.
mask mask	(Optional) Specifies the IP mask of the target. Default value is 255.255.255.255.
timeout *timeout*	(Optional) Specifies the maximum round trip time allowed to communicate to this target address. This value is in .01 seconds and the default is 1500 (15 seconds.)
retries *retries*	(Optional) Specifies the number of message retries allowed if a response is not received. Default is 3.
taglist *taglist*	(Optional) Specifies a list of SNMP notify tag values. This tags a location to the target address as a place to send notifications. List must be enclosed in quotes and tag values must be separated by a space (i.e.: **"tag 1 tag 2"**)
volatile | **nonvolatile**	(Optional) Specifies temporary (default), or permanent storage for SNMP entries. Default is nonvolatile.

Defaults

- If not specified, *udpport* will be set to **162**.
- If not specified, *mask* will be set to **255.255.255.255**
- If not specified, *timeout* will be set to **1500**.
- If not specified, number of *retries* will be set to **3**.
- If **taglist** is not specified, none will be set.
- If not specified, storage type will be set to **nonvolatile**.

Mode

All command modes.

Usage

The target address is a unique identifier and a specific IP address that will receive SNMP notification messages and determine which community strings will be accepted. This address configuration can be linked to optional SNMP transmit parameters (such as timeout, retry count, and UDP port).

In C2 security mode, you can not create, delete, or modify an SNMP target address configuration while in Read-Write user mode.

Example

This example shows how to configure a trap notification called "**TrapSink.**" This trap notification will be sent to the workstation 192.168.190.80 (which is target address "tr"). It will use security and authorization criteria contained in a target parameters entry called "v2cExampleParams". For more information on creating a basic SNMP trap, refer to the S-Series *Configuration Guide*.

```
S Chassis(rw)->set snmp targetaddr tr 192.168.190.80 param v2cExampleParams
taglist TrapSink
```

clear snmp targetaddr

Use this command to delete an SNMP target address entry.

Syntax

clear snmp targetaddr *targetAddr*

Parameters

targetAddr	Specifies the target address entry to delete.

Defaults

None.

Mode

All command modes.

Usage

In C2 security mode, you can not delete an SNMP target address configuration while in Read-Write user mode.

Example

This example shows how to clear SNMP target address entry "targetaddr1":

```
S Chassis(rw)->clear snmp targetaddr targetaddr1
```

Configuring SNMP Notification Parameters

These commands are used to configure SNMP notification parameters and optional filters. Notification parameters are entities which handle the generation of SNMP v1 and v2 "trap" or

SNMP v3 “inform” messages to selected management targets. Optional notification filters identify which targets should not receive notifications. For a sample SNMP trap configuration showing how SNMP notification parameters are associated with security and authorization criteria (target parameters) and mapped to a management target address, see the *Extreme Networks S-Series Configuration Guide*.

About SNMP Notify Filters

Profiles indicating which targets should not receive SNMP notification messages are kept in the NotifyFilter table. If this table is empty, meaning that no filtering is associated with any SNMP target, then no filtering will take place. “Trap” or “inform” notifications will be sent to all destinations in the SNMP targetAddrTable that have tags matching those found in the NotifyFilter Table.

When the NotifyFilter table contains profile entries, the SNMP agent will find any filter profile name that corresponds to the target parameter name contained in an outgoing notification message. It will then apply the appropriate subtree-specific filter when generating notification messages.

For information about...	Refer to page...
show snmp notify	34-8
set snmp notify	34-9
clear snmp notify	34-10
show snmp notifyfilter	34-11
set snmp notifyfilter	34-11
clear snmp notifyfilter	34-12
show snmp notifyprofile	34-13
set snmp notifyprofile	34-13
clear snmp notifyprofile	34-14

show snmp notify

Use this command to display the SNMP notify configuration, which determines which management targets will receive SNMP notifications.

Syntax

show snmp notify [*notify*] [**volatile** | **nonvolatile** | **read-only**]

Parameters

notify	(Optional) Displays notify entries for a specific notify name.
volatile | **nonvolatile** | **read-only**	(Optional) Displays notify entries for a specific storage type.

Defaults

- If a *notify* name is not specified, all entries will be displayed.
- If **volatile**, **nonvolatile**, or **read-only** are not specified, all storage type entries will be displayed.

Mode

All command modes.

Example

This example shows how to display the SNMP notify information:

```
S Chassis(rw)->show snmp notify
Notify name     = 1
Notify Tag      = Console
Notify Type     = trap
Storage type    = nonVolatile
Row status      = active

Notify name     = 2
Notify Tag      = TrapSink
Notify Type     = trap
Storage type    = nonVolatile
Row status      = active
```

Table 34-3 shows a detailed explanation of the command output.

Table 34-3 show snmp notify Output Details

Output...	What it displays...
Notify name	A unique identifier used to index the SNMP notify table.
Notify Tag	Name of the entry in the SNMP notify table.
Notify Type	Type of notification: SNMPv1 or v2 trap or SNMPv3 InformRequest message.
Storage type	Whether access entry is stored in **volatile**, **nonvolatile**, or **read-only** memory.
Row status	Status of this entry: **active**, **notInService**, or **notReady**.

set snmp notify

Use this command to set the SNMP notify configuration.

Syntax

set snmp notify *notify* **tag** *tag* [**trap** | **inform**] [**volatile** | **nonvolatile**]

Parameters

notify	Specifies an SNMP notify name.
tag *tag*	Specifies an SNMP notify tag. This binds the notify name to the SNMP target address table.
trap | **inform**	(Optional) Specifies SNMPv1 or v2 Trap messages (default) or SNMP v3 InformRequest messages.
volatile | **nonvolatile**	(Optional) Specifies temporary (default), or permanent storage for SNMP entries.

Defaults

- If not specified, message type will be set to **trap**.
- If not specified, storage type will be set to **nonvolatile**.

Mode

All command modes.

Usage

This creates an entry in the SNMP notify table, which is used to select management targets who should receive notification messages. This command's **tag** parameter can be used to bind each entry to a target address using the **set snmp targetaddr** command ("set snmp targetaddr" on page 34-6).

In C2 security mode, you can not create, delete, or modify an SNMP notify configuration in Read-Write user mode.

Example

This example shows how to set an SNMP notify configuration with a notify name of "hello" and a notify tag of "world". Notifications will be sent as trap messages and storage type will automatically default to permanent:

```
S Chassis(rw)->set snmp notify hello tag world trap
```

clear snmp notify

Use this command to clear an SNMP notify configuration.

Syntax

clear snmp notify *notify*

Parameters

notify	Specifies an SNMP notify name to clear.

Defaults

None.

Mode

All command modes.

Usage

In C2 security mode, you can not clear an SNMP notify configuration while in Read-Write user mode.

Example

This example shows how to clear the SNMP notify configuration for "hello":

```
S Chassis(rw)->clear snmp notify hello
```

show snmp notifyfilter

Use this command to display SNMP notify filter information and determine which SNMP profiles will not receive SNMP notifications.

Syntax

show snmp notifyfilter [*profile*] [**subtree** *oid-or-mibobject*] [**volatile** | **nonvolatile** | **read-only**]

Parameters

profile	(Optional) Displays a specific notify filter.
subtree *oid-or-mibobject*	(Optional) Displays a notify filter within a specific subtree.
volatile | **nonvolatile** | **read-only**	(Optional) Displays notify filter entries of a specific storage type.

Defaults

If no parameters are specified, all notify filter information will be displayed.

Mode

All command modes.

Example

This example shows how to display SNMP notify filter information. In this case, the notify profile "pilot1" in subtree 1.3.6 will not receive SNMP notification messages:

```
S Chassis(rw)->show snmp notifyfilter
Profile         = pilot1
Subtree         = 1.3.6
Subtree mask    = ff:02:e7:45
Filter type     = included
Storage type    = nonVolatile
Row status      = active
```

set snmp notifyfilter

Use this command to create an SNMP notify filter configuration that will determine which SNMP profiles will not receive SNMP notifications.

Syntax

set snmp notifyfilter *profile* **subtree** *oid-or-mibobject* [**mask** *mask*] [**included** | **excluded**] [**volatile** | **nonvolatile**]

Parameters

profile	Specifies an SNMP filter notify name.
subtree *oid-or-mibobject*	Specifies a MIB subtree ID target for the filter.

mask *mask*	(Optional) Applies a subtree mask.
included | **excluded**	(Optional) Specifies that subtree is included or excluded.
volatile | **nonvolatile**	(Optional) Specifies a storage type.

Defaults

- If not specified, *mask* is not set.
- If not specified, **subtree** will be included.
- If storage type is not specified, **nonvolatile** (permanent) will be applied.

Mode

All command modes.

Usage

This identifies which management targets should NOT receive notification messages, which is useful for fine-tuning the amount of SNMP traffic generated.

Example

This example shows how to create an SNMP notify filter called "pilot1" with a MIB subtree ID of 1.3.6:

```
S Chassis(rw)->set snmp notifyfilter pilot1 subtree 1.3.6
```

clear snmp notifyfilter

Use this command to delete an SNMP notify filter configuration.

Syntax

clear snmp notifyfilter *profile* **subtree** *oid-or-mibobject*

Parameters

profile	Specifies an SNMP filter notify name to delete.
subtree *oid-or-mibobject*	Specifies a MIB subtree ID containing the filter to be deleted.

Defaults

None.

Mode

All command modes.

Example

This example shows how to delete the SNMP notify filter "pilot1":

```
S Chassis(rw)->clear snmp notifyfilter pilot1 subtree 1.3.6
```

show snmp notifyprofile

Use this command to display SNMP notify profile information.

Syntax

show snmp notifyprofile [*profile*] [**targetparam** *targetparam*] [**volatile** | **nonvolatile** | **read-only**]

Parameters

profile	(Optional) Displays a specific notify profile.
targetparam *targetparam*	(Optional) Displays entries for a specific target parameter.
volatile | **nonvolatile** | **read-only**	(Optional) Displays notify filter entries of a specific storage type.

Defaults

If no parameters are specified, all notify profile information will be displayed.

Mode

All command modes.

Example

This example shows how to display SNMP notify information for the profile named "area51":

```
S Chassis(rw)->show snmp notifyprofile area51
Notify Profile  = area51
TargetParam     = v3ExampleParams
Storage type    = nonVolatile
Row status      = active
```

set snmp notifyprofile

Use this command to create an SNMP notify filter profile configuration.

Syntax

set snmp notifyprofile *profile* **targetparam** *targetparam* [**volatile** | **nonvolatile**]

Parameters

profile	Specifies an SNMP filter notify name.
targetparam *targetparam*	Specifies an associated entry in the SNMP Target Params Table.
volatile | **nonvolatile**	(Optional) Specifies a storage type.

Defaults

If storage type is not specified, **nonvolatile** (permanent) will be applied.

Mode

All command modes.

Usage

This associates an existing notification filter, created with the **set snmp notifyfilter** command ("set snmp notifyfilter" on page 34-11), to a set of SNMP target parameters to determine which management targets should not receive SNMP notifications.

Example

This example shows how to create an SNMP notify profile named area51 and associate a target parameters entry.

```
S Chassis(rw)->set snmp notifyprofile area51 targetparam v3ExampleParams
```

clear snmp notifyprofile

Use this command to delete an SNMP notify profile configuration.

Syntax

clear snmp notifyprofile *profile* **targetparam** *targetparam*

Parameters

profile	Specifies an SNMP filter notify name to delete.
targetparam *targetparam*	Specifies an associated entry in the snmpTargetParamsTable.

Defaults

None.

Mode

All command modes.

Example

This example shows how to delete SNMP notify profile "area51":

```
S Chassis(rw)->clear snmp notifyprofile area51 targetparam v3ExampleParams
```

Configuring SNMP MIB Walk Behavior

These commands are used to configure SNMP MIB walk behavior.

For information about...	Refer to page...
set snmp timefilter break	34-15
clear snmp timefilter break	34-15
show snmp timefilter	34-16

set snmp timefilter break

Use this command to set SNMP to exit the MIB walk after the first entry it returns if the index includes a timestamp.

Syntax

```
set snmp timefilter break {enable | disable}
```

Parameters

enable	Configures the MIB walk behavior to exit after the first entry is returned when the getNext object index contains a timestamp.
disable	Configures the MIB walk behavior to only exit when the current time is reached when the getNext object index contains a timestamp.

Defaults

Disabled.

Mode

All command modes.

Usage

When an index contains a timestamp, by default the getNext walk continues to return values until the current time is reached, which may not ever occur, leaving the user with the impression that the walk is in a loop. Enabling this command will exit the walk after the first entry is returned.

Example

This example enables the SNMP timestamp filter break for this router:

```
S Chassis(rw)->set snmp timefilter break enable
```

clear snmp timefilter break

Use this command to reset the SNMP MIB walk timestamp exit behavior state to its default setting of disabled.

Syntax

```
clear snmp timefilter break
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

When the SNMP timefilter break state is cleared, its state is set to disabled.

Example

This example resets the SNMP MIB walk timestamp exit behavior state for this router:

```
S Chassis(rw)->clear snmp timefilter break
```

show snmp timefilter

Use this command to display the current state of the SNMP MIB walk timestamp exit behavior.

Syntax

show snmp timefilter

Parameters

None.

Defaults

None

Mode

All command modes.

Example

This example displays the state of the SNMP MIB walk timestamp exit behavior for this router:

```
S Chassis(rw)->show snmp timefilter
timefilter = enabled
```

Reviewing SNMP Statistics

These commands are used to review SNMP statistics.

For information about...	Refer to page...
show snmp engineid	34-16
show snmp counters	34-17

show snmp engineid

Use this command to display the SNMP local engine ID. This is the SNMP v3 engine's administratively unique identifier.

Syntax

show snmp engineid

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display SNMP engine properties:

```
S Chassis(rw)->show snmp engineid
EngineId: 80:00:15:f8:03:00:e0:63:9d:b5:87
Engine Boots    = 12
Engine Time     = 162181
Max Msg Size    = 2048
```

Table 34-4 shows a detailed explanation of the command output.

Table 34-4 show snmp engineid Output Details

Output...	What it displays...
EngineId	String identifying the SNMP agent on the device.
Engine Boots	Number of times the SNMP engine has been started or reinitialized.
Engine Time	Time in seconds since last reboot.
Max Msg Size	Maximum accepted length, in bytes, of SNMP frame.

show snmp counters

Use this command to display SNMP traffic counter values.

Syntax

show snmp counters

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display SNMP counter values.

```
S Chassis(rw)->show snmp counters

--- mib2 SNMP group counters:
snmpInPkts              = 396601
snmpOutPkts             = 396601
snmpInBadVersions       = 0
snmpInBadCommunityNames = 0
snmpInBadCommunityUses  = 0
snmpInASNParseErrs      = 0
snmpInTooBigs           = 0
snmpInNoSuchNames       = 0
snmpInBadValues         = 0
snmpInReadOnlys         = 0
snmpInGenErrs           = 0
snmpInTotalReqVars      = 403661
snmpInTotalSetVars      = 534
snmpInGetRequests       = 290
snmpInGetNexts          = 396279
snmpInSetRequests       = 32
snmpInGetResponses      = 0
snmpInTraps             = 0
snmpOutTooBigs          = 0
snmpOutNoSuchNames      = 11
snmpOutBadValues        = 0
snmpOutGenErrs          = 0
snmpOutGetRequests      = 0
snmpOutGetNexts         = 0
snmpOutSetRequests      = 0
snmpOutGetResponses     = 34
snmpOutTraps            = 0
snmpSilentDrops         = 0
snmpProxyDrops          = 0

--- USM Stats counters:
usmStatsUnsupportedSecLevels = 0
usmStatsNotInTimeWindows     = 0
usmStatsUnknownUserNames     = 0
usmStatsUnknownEngineIDs     = 0
usmStatsWrongDigests         = 0
usmStatsDecryptionErrors     = 0
```

Table 34-5 shows a detailed explanation of the command output.

Table 34-5 show snmp counters Output Details

Output...	What it displays...
snmpInPkts	Number of messages delivered to the SNMP entity from the transport service.
snmpOutPkts	Number of SNMP messages passed from the SNMP protocol entity to the transport service.
snmpInBadVersions	Number of SNMP messages delivered to the SNMP entity for an unsupported SNMP version.
snmpInBadCommunityNames	Number of SNMP messages delivered to the SNMP entity that used an SNMP community name not known to the entity.
snmpInBadCommunityUses	Number of SNMP messages delivered to the SNMP entity that represented an SNMP operation not allowed by the SNMP community named in the message.
snmpInASNParseErrs	Number of ASN.1 (Abstract Syntax Notation) or BER (Basic Encoding Rules) errors encountered by the SNMP entity when decoding received SNMP messages.
snmpInTooBigs	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “tooBig.”
snmpInNoSuchNames	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “noSuchName.”
snmpInBadValues	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “badValue.”
snmpInReadOnlys	Number of valid SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “readOnly.”
snmpInGenErrs	Number of SNMP PDUs delivered to the SNMP protocol entity with the value of the error-status field as “genErr.”
snmpInTotalReqVars	Number of MIB objects retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
snmpInTotalSetVars	Number of MIB objects altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.
snmpInGetRequests	Number of SNMP Get-Request PDUs accepted and processed by the SNMP protocol entity.
snmpInGetNexts	Number of SNMP Get-Next PDUs accepted and processed by the SNMP protocol entity.
snmpInSetRequests	Number of SNMP Set-Request PDUs accepted and processed by the SNMP protocol entity.
snmpInGetResponses	Number of SNMP Get-Response PDUs accepted and processed by the SNMP protocol entity.
snmpInTraps	Number of SNMP Trap PDUs accepted and processed by the SNMP protocol entity.
snmpOutTooBigs	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status field as “tooBig.”
snmpOutNoSuchNames	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status as “noSuchName.”

Table 34-5 show snmp counters Output Details (continued)

Output...	What it displays...
snmpOutBadValues	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status field as “badValue.”
snmpOutGenErrs	Number of SNMP PDUs generated by the SNMP protocol entity with the value of the error-status field as “genErr.”
snmpOutGetRequests	Number of SNMP Get-Request PDUs generated by the SNMP protocol entity.
snmpOutGetNexts	Number of SNMP Get-Next PDUs generated by the SNMP protocol entity.
snmpOutSetRequests	Number of SNMP Set-Request PDUs generated by the SNMP protocol entity.
snmpOutGetResponses	Number of SNMP Get-Response PDUs generated by the SNMP protocol entity.
snmpOutTraps	Number of SNMP Trap PDUs generated by the SNMP protocol entity.
snmpSilentDrops	Number of SNMP Get, Set, or Inform request error messages that were dropped because the reply was larger than the requestor’s maximum message size.
snmpProxyDrops	Number of SNMP Get, Set, or Inform request error messages that were dropped because the reply was larger than the proxy target’s maximum message size.
usmStatsUnsupportedSec Levels	Number of packets received by the SNMP engine that were dropped because they requested a security level that was unknown to the SNMP engine or otherwise unavailable.
usmStatsNotInTimeWindows	Number of packets received by the SNMP engine that were dropped because they appeared outside of the authoritative SNMP engine's window.
usmStatsUnknownUserNames	Number of packets received by the SNMP engine that were dropped because they referenced a user that was not known to the SNMP engine.
usmStatsUnknownEngineIDs	Number of packets received by the SNMP engine that were dropped because they referenced an snmpEngineID that was not known to the SNMP engine.
usmStatsWrongDigests	Number of packets received by the SNMP engine that were dropped because they did not contain the expected digest value.
usmStatsDecriptionErrors	Number of packets received by the SNMP engine that were dropped because they could not be decrypted.

35

Spanning Tree Bridge Commands

This chapter provides detailed information for the Spanning Tree bridge set of commands. Spanning tree bridge functionality includes the display and setting of Spanning Tree bridge parameters, including device priorities, hello time, maximum wait time, forward delay, path cost, and topology change trap suppression. For information about configuring Spanning Tree, refer to the "Spanning Tree Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

Note: The term "bridge" is used as an equivalent to the term "switch" or "device" in this document.

For information about...	Refer to page...
show spantree stats	35-3
show spantree version	35-6
set spantree version	35-7
clear spantree version	35-7
show spantree stpmode	35-8
set spantree stpmode	35-8
clear spantree stpmode	35-9
show spantree maxconfigurablestps	35-9
set spantree maxconfigurablestps	35-10
clear spantree maxconfigurablestps	35-10
show spantree mstilist	35-11
set spantree msti	35-11
clear spantree msti	35-12
show spantree mstmap	35-12
set spantree mstmap	35-13
clear spantree mstmap	35-13
show spantree vlanlist	35-14
show spantree mstcfgid	35-14
set spantree mstcfgid	35-15
clear spantree mstcfgid	35-16
show spantree bridgeprioritymode	35-16

For information about...	Refer to page...
set spantree bridgeprioritymode	35-17
clear spantree bridgeprioritymode	35-17
show spantree priority	35-18
set spantree priority	35-18
clear spantree priority	35-19
show spantree bridgehellomode	35-20
set spantree bridgehellomode	35-20
clear spantree bridgehellomode	35-21
show spantree hello	35-21
set spantree hello	35-22
clear spantree hello	35-22
show spantree maxage	35-23
set spantree maxage	35-23
clear spantree maxage	35-24
show spantree fwddelay	35-24
set spantree fwddelay	35-25
clear spantree fwddelay	35-25
show spantree autoedge	35-26
set spantree autoedge	35-26
clear spantree autoedge	35-27
show spantree legacypathcost	35-27
set spantree legacypathcost	35-28
clear spantree legacypathcost	35-28
show spantree tctrapsuppress	35-29
set spantree tctrapsuppress	35-29
clear spantree tctrapsuppress	35-30
show spantree txholdcount	35-30
set spantree txholdcount	35-31
clear spantree txholdcount	35-31
show spantree maxhops	35-32
set spantree maxhops	35-32
clear spantree maxhops	35-33
show spantree spanguard	35-33
set spantree spanguard	35-34
clear spantree spanguard	35-34
show spantree spanguardtimeout	35-35

For information about...	Refer to page...
set spantree spanguardtimeout	35-35
clear spantree spanguardtimeout	35-36
show spantree spanguardlock	35-36
clear / set spantree spanguardlock	35-37
show spantree spanguardtrapenable	35-37
set spantree spanguardtrapenable	35-38
clear spantree spanguardtrap enable	35-38
show spantree backuproot	35-39
set spantree backuproot	35-39
clear spantree backuproot	35-40
show spantree backuproottrapendable	35-40
set spantree backuproottrapenable	35-41
clear spantree backuproottrapenable	35-41
show spantree newroottrapendable	35-42
set spantree newroottrapenable	35-42
clear spantree newroottrapenable	35-43
clear spantree default	35-43
show spantree debug	35-44
clear spantree debug	35-46

show spantree stats

Use this command to display Spanning Tree information for one or more ports.

Syntax

show spantree stats [**port** *port-string*] [**sid** *sid*] [**active**]

Parameters

port *port-string*	(Optional) Displays information for the specified port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
sid *sid*	(Optional) Displays information for a specific Spanning Tree identifier. If not specified, SID 0 is assumed.
active	(Optional) Displays information for ports that have received STP BPDUs since boot.

Defaults

- If *port-string* is not specified, Spanning Tree information for all ports will be displayed.
- If *sid* is not specified, information for Spanning Tree 0 will be displayed.

- If **active** is not specified information for all ports will be displayed regardless of whether or not they have received BPDUs.

Mode

All command modes.

Example

This example shows how to display the device's Spanning Tree configuration:

```
S Chassis(rw)->show spantree stats

Spanning tree status          - enabled
Spanning tree instance        - 0
Designated Root MacAddr       - 00-e0-63-9d-c1-c8
Designated Root Priority      - 0
Designated Root Cost          - 10000
Designated Root Port          - lag.0.1
Root Max Age                  - 20 sec
Root Hello Time               - 2  sec
Root Forward Delay            - 15 sec
Bridge ID MAC Address         - 00-01-f4-da-5e-3d
Bridge ID Priority            - 32768
Bridge Max Age                - 20 sec
Bridge Hello Time             - 2  sec
Bridge Forward Delay          - 15 sec
Topology Change Count         - 7
Time Since Top Change         - 00 days 03:19:15
Max Hops                      - 20
```

Table 35-1 shows a detailed explanation of command output.

Table 35-1 show spantree Output Details

Output...	What it displays...
Spanning tree instance	Spanning Tree ID.
Spanning tree status	Whether Spanning Tree is enabled or disabled.
Designated Root MacAddr	MAC address of the designated Spanning Tree root bridge.
Designated Root Port	Port through which the root bridge can be reached.
Designated Root Priority	Priority of the designated root bridge.
Designated Root Cost	Total path cost to reach the root.
Root Max Age	Amount of time (in seconds) a BPDU packet should be considered valid.
Root Hello Time	Interval (in seconds) at which the root device sends BPDU (Bridge Protocol Data Unit) packets.
Root Forward Delay	Amount of time (in seconds) the root device spends in listening or learning mode.

Table 35-1 show spantree Output Details (continued)

Output...	What it displays...
Bridge ID MAC Address	Unique bridge MAC address, recognized by all bridges in the network.
Bridge ID Priority	Bridge priority, which is a default value, or is assigned using the **set spantree priority** command. For details, refer to "set spantree priority" on page 35-18.
Bridge Max Age	Maximum time (in seconds) the bridge can wait without receiving a configuration message (bridge "hello") before attempting to reconfigure. This is a default value, or is assigned using the **set spantree maxage** command. For details, refer to "set spantree maxage" on page 35-23.
Bridge Hello Time	Amount of time (in seconds) the bridge sends BPDUs. This is a default value, or is assigned using the **set spantree hello** command. For details, refer to "set spantree hello" on page 35-22.
Bridge Forward Delay	Amount of time (in seconds) the bridge spends in listening or learning mode. This is a default value, or is assigned using the **set spantree fwddelay** command. For details, refer to "set spantree fwddelay" on page 35-25.
Topology Change Count	Number of times topology has changed on the bridge.
Time Since Top Change	Amount of time (in days, hours, minutes and seconds) since the last topology change.
Max Hops	Maximum number of hops information for a particular Spanning Tree instance may traverse (via relay of BPDUs within the applicable MST region) before being discarded. This is a default value, or is assigned using the **set spantree maxhops** command. For details, refer to "set spantree maxhops" on page 35-32.

Example

This example shows how to display port-specific Spanning Tree information for port ge.1.1.

```
S Chassis(rw)->show spantree stats port ge.1.1

Spanning tree status          - enabled
Spanning tree instance        - 0
Designated Root MacAddr       - 00-e0-63-93-79-0f
Designated Root Priority      - 0
Designated Root Cost          - 0
Designated Root Port          - 0
Root Max Age                  - 20 sec
Root Hello Time               - 2  sec
Root Forward Delay            - 15 sec
Bridge ID MAC Address         - 00-e0-63-93-79-0f
Bridge ID Priority            - 0
Bridge Max Age                - 20 sec
Bridge Hello Time             - 2  sec
Bridge Forward Delay          - 15 sec
Topology Change Count         - 5
Time Since Top Change         - 00 days 03:16:54
```

```
Max Hops                    - 20

SID   Port         State              Role          Cost        Priority
---   ----------   ----------------   -----------   --------    --------
0     ge.1.1       Blocking           Disabled      20000       128
```

Table 35-2 describes the port-specific information displayed.

Table 35-2 Port-Specific show spantree stats Output Details

Output...	What it displays...
SID	The Spanning Tree instance.
Port	The port name.
State	The Spanning Tree forwarding state of the port. This value can be Blocking, Forwarding, Listening, or Learning. If the port/SID has been placed in a non-forwarding state for a reason other than normal Spanning Tree protocol operation, an asterisk will be displayed next to the state. You can use the show spantree nonforwardingreason command (page 37-13) to display the specific reason.
Role	The Spanning Tree role of the port. The port role is assigned by the Spanning Tree protocol and determines the behavior of the port — either sending or receiving BPDUs, and forwarding or blocking data traffic.
Cost	The port cost.
Priority	The priority of the link in a Spanning Tree bridge. This value can be set with the set spantree portpri command (page 36-8).

show spantree version

Use this command to display the current version of the Spanning Tree protocol running on the device.

Syntax

show spantree version

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display Spanning Tree version information for the device:

```
S Chassis(rw)->show spantree version
Force Version is mstp
```

set spantree version

Use this command to set the version of the Spanning Tree protocol to MSTP (Multiple Spanning Tree Protocol), RSTP (Rapid Spanning Tree Protocol) or to STP 802.1D-compatible.

Syntax

```
set spantree version {mstp | stpcompatible | rstp}
```

Parameters

mstp	Sets the version to STP 802.1s-compatible (Version 3).
stpcompatible	Sets the version to STP 802.1D-compatible (Version 2).
rstp	Sets the version to 802.1w-compatible (Version 0).

Defaults

Spanning Tree version defaults to version 3.

Mode

All command modes.

Usage

In most networks, Spanning Tree version should not be changed from its default setting of **mstp** (Multiple Spanning Tree Protocol) mode. MSTP mode is fully compatible and interoperable with legacy STP 802.1D and Rapid Spanning Tree (RSTP) bridges. Setting the version to **stpcompatible** mode will cause the bridge to transmit only 802.1D BPDUs, and will prevent non-edge ports from rapidly transitioning to forwarding state.

Example

This example shows how to globally change the Spanning Tree version from the default of MSTP to RSTP:

```
S Chassis(rw)->set spantree version rstp
```

clear spantree version

Use this command to reset the Spanning Tree version to MSTP mode.

Syntax

```
clear spantree version
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the Spanning Tree version:

```
S Chassis(rw)->clear spantree version
```

show spantree stpmode

Use this command to display the Spanning Tree Protocol (STP) mode setting.

Syntax

show spantree stpmode

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the STP mode:

```
S Chassis(rw)->show spantree stpmode
Bridge Stp Mode is set to ieee8021
```

set spantree stpmode

Use this command to globally enable or disable the Spanning Tree Protocol (STP) mode.

Syntax

set spantree stpmode {**none** | **ieee8021**}

Parameters

none	Disables Spanning Tree.
ieee8021	Enables 802.1 Spanning Tree mode.

Defaults

None.

Mode

All command modes.

Example

This example shows how to disable Spanning Tree:

```
S Chassis(rw)->set spantree stpmode none
```

clear spantree stpmode

Use this command to reset the Spanning Tree protocol mode to the default setting of IEEE802.1. This re-enables Spanning Tree.

Syntax

clear spantree stpmode

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to enable Spanning Tree by resetting the STP mode to IEEE 802.1:

```
S Chassis(rw)->clear spantree stpmode
```

show spantree maxconfigurablestps

Use this command to display the setting for the maximum number of user-configurable Spanning Tree instances.

Syntax

show spantree maxconfigurablestps

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the setting for the maximum number of user-configurable STP instances:

```
S Chassis(rw)->show spantree maxconfigurablestps
Max user configurable stps is set to 33
```

set spantree maxconfigurablestps

Use this command to set the maximum number of user configurable Spanning Tree instances.

Syntax

set spantree maxconfigurablestps *numstps*

Parameters

numstps	Specifies the maximum number of user configured STPs to be allowed on this bridge. Valid values are 1 - 34. Default value is 33.

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the maximum number of user-configurable STP instances to 8:

```
S Chassis(rw)->set spantree maxconfigurablestps 8
```

clear spantree maxconfigurablestps

Use this command to clear the setting for the maximum number of user configurable Spanning Tree instances.

Syntax

clear spantree maxconfigurablestps

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

This command resets the maximum number of user configurable Spanning Tree instances to the default value of **33**.

Example

This example shows how to clear setting for the maximum number of user-configurable STP instances:

```
S Chassis(rw)->clearspantree maxconfigurablestps
```

show spantree mstilist

Use this command to display a list of Multiple Spanning Tree (MST) instances configured on the device.

Syntax

show spantree mstilist

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display a list of MST instances. In this case, SID 2 has been configured:

```
S Chassis(rw)->show spantree mstilist
 Configured Multiple Spanning Tree instances: 2
```

set spantree msti

Use this command to create or delete a Multiple Spanning Tree instance.

Syntax

set spantree msti sid *sid* {**create** | **delete**}

Parameters

sid *sid*	Sets the Multiple Spanning Tree ID. Valid values are **1** - **4094**. **Notes:** 65
create | **delete**	Creates or deletes an MST instance.

Defaults

None.

Mode

All command modes.

Example

This example shows how to create MST instance 2:

```
S Chassis(rw)->set spantree msti sid 2 create
```

clear spantree msti

Use this command to delete a Multiple Spanning Tree instance.

Syntax

clear spantree msti *sid*

Parameters

sid	Specifies a Multiple Spanning Tree ID to be deleted.

Defaults

None.

Mode

All command modes.

Example

This example shows how to delete MST instance 1:

```
S Chassis(rw)->clear spantree msti 1
```

show spantree mstmap

Use this command to display the mapping of a filtering database ID (FID) to a Spanning Tree. Since VLANs are mapped to FIDs, this shows to which SID a VLAN is mapped.

Syntax

show spantree mstmap [**fid** *fid*]

Parameters

fid *fid*	(Optional) Displays information for specific FIDs.

Defaults

If *fid* is not specified, information for all assigned FIDs will be displayed.

Mode

All command modes.

Example

This example shows how to display SID to FID mapping information for FID 1. In this case, no new mappings have been configured:

```
S Chassis(rw)->show spantree mstmap fid 1
FID:       SID:
1          0
```

set spantree mstmap

Use this command to map one or a range of filtering database IDs (FIDs) to a SID. Since VLANs are mapped to FIDs, this essentially maps one or more VLAN IDs to a Spanning Tree (SID).

Syntax

set spantree mstmap *fid* [**sid** *sid*]

Parameters

fid	Specifies one or a range of FIDs to assign to the MST. Valid values are **1** - **4093**, and **4095**, and must correspond to a VLAN ID created using the **set vlan** command.
sid *sid*	(Optional) Specifies a Multiple Spanning Tree ID. Valid values are **1** - **4094**, and must correspond to a SID created using the **set msti** command as described in "set spantree msti" on page 35-11.

Defaults

If *sid* is not specified, FID(s) will be mapped to Spanning Tree 0.

Mode

All command modes.

Examples

This example shows how to map FID 3 to SID 2:

```
S Chassis(rw)->set spantree mstmap 3 sid 2
```

This example shows how to map FIDs 1 through 3 to SID 2:

```
S Chassis(rw)->set spantree mstmap 1-3 sid 2
```

clear spantree mstmap

Use this command to map a FID back to SID 0.

Syntax

clear spantree mstmap *fid*

Parameters

fid	Specifies one or more FIDs to reset to 0.

Defaults

None.

Mode

All command modes.

Example

This example shows how to map FID 2 back to SID 0:

```
S Chassis(rw)->clear spantree mstmap 2
```

show spantree vlanlist

Use this command to display the VLAN ID(s) assigned to one or more Spanning Trees.

Syntax

show spantree vlanlist [*vlan-list*]

Parameters

vlan-list	(Optional) Displays information for specific VLAN(s).

Defaults

If not specified, SID assignment will be displayed only for VLANs assigned to any SID other than SID 0.

Mode

All command modes.

Example

This example shows how to display assignments for all VLANs assigned to any SID other than SID 0:

```
S Chassis(rw)->show spantree vlanlist
Vlan 104 is mapped to Sid 104
Vlan 105 is mapped to Sid 105
Vlan 106 is mapped to Sid 106
Vlan 107 is mapped to Sid 107
```

show spantree mstcfgid

Use this command to display the MST configuration identifier elements, including format selector, configuration name, revision level, and configuration digest.

Syntax

show spantree mstcfgid

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the MST configuration identifier elements. In this case, the default revision level of 0, and the default configuration name (a string representing the bridge MAC address) have not been changed. For information on using the **set spantree mstcfgid** command to change these settings, refer to "set spantree mstcfgid" on page 35-15:

```
S Chassis(rw)->show spantree mstcfgid
 MST Configuration Identifier:
  Format Selector: 0
  Configuration Name: 00:01:f4:89:51:94
  Revision Level: 0
  Configuration Digest: ac:36:17:7f:50:28:3c:d4:b8:38:21:d8:ab:26:de:62
```

set spantree mstcfgid

Use this command to set the MST configuration name and/or revision level.

Syntax

set spantree mstcfgid {[**cfgname** *name*] [**rev** *level*]}

Parameters

cfgname *name*	Specifies an MST configuration name. The MST configuration name defaults to the device MAC address.
rev *level*	Specifies an MST revision level. Valid values are **0** - **65535**.

Defaults

If the MST configuration name is not specified, an MST configuration name defaults to the bridge MAC address.

If the MST revision level is not specified, an MST revision level defaults to **0**.

Mode

All command modes.

Usage

This command allows you to configure either the MST region name or revision level or both. Any device that wishes to belong to the same MST region as another device must be administratively configured with the same region name and revision level. The MST region name defaults to the

bridge MAC address. The MST revision level is an arbitrary administratively defined value that defaults to **0**.

Example

This example shows how to set the MST configuration name to “mstconfig”:

```
S Chassis(rw)->set spantree mstcfgid cfgname mstconfig
```

clear spantree mstcfgid

Use this command to clear the MST configuration name and revision level.

Syntax

clear spantree mstcfgid

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

This command resets both the MST region name to the default value of the bridge MAC address and the MST revision level to the default value of **0**.

Example

This example shows how to reset the MST configuration identifier elements to default values:

```
S Chassis(rw)->clear spantree mstcfgid
```

show spantree bridgeprioritymode

Use this command to display the Spanning Tree bridge priority mode setting.

Syntax

show spantree bridgeprioritymode

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the Spanning Tree bridge priority mode setting:

```
S Chassis(rw)->show spantree bridgeprioritymode
Bridge Priority Mode is set to IEEE802.1t mode.
```

set spantree bridgeprioritymode

Use this command to set the Spanning Tree bridge priority mode to 802.1D (legacy) or 802.1t. This will affect the range of priority values used to determine which device is selected as the Spanning Tree root as described in **set spantree priority** (page 35-18).

Syntax

set spantree bridgeprioritymode {**8021d** | **8021t**}

Parameters

8021d	Sets the bridge priority mode to use 802.1D (legacy) values of values, which are 0 - 65535.
8021t	Sets the bridge priority mode to use 802.1t values, which are 0 - 61440, in increments of 4096. Values will be rounded up or down, depending on the 802.1t value to which the entered value is closest.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the bridge priority mode to 802.1D:

```
S Chassis(rw)->set spantree bridgeprioritymode 8021d
```

clear spantree bridgeprioritymode

Use this command to reset the Spanning Tree bridge priority mode to the default setting of 802.1t.

Syntax

clear spantree bridgeprioritymode

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the bridge priority mode to 802.1t:

```
S Chassis(rw)->clear spantree bridgeprioritymode
```

show spantree priority

Use this command to display the Spanning Tree bridge priority.

Syntax

show spantree priority [*sid*]

Parameters

sid	(Optional) Displays the priority for a specific Spanning Tree. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If *sid* is not specified, priority will be shown for Spanning Tree 0.

Mode

All command modes.

Example

This example shows how to show the bridge priority for Spanning Tree 0

```
S Chassis(rw)->show spantree priority
Bridge Priority is set to 4096 on sid 0
```

set spantree priority

Use this command to set the device's Spanning Tree priority.

Syntax

set spantree priority *priority* [*sid*]

Parameters

priority	Specifies the priority of the bridge. Valid values are from **0** to **65535,** with the numerical value of 0 indicating highest priority and the numerical value 65535 indicating lowest priority. When 802.1t is selected as the bridge priority mode, as described in "set spantree bridgeprioritymode" on page 35-17, values will be rounded up or down, depending on the 802.1t value to which the entered value is closest, in increments of 4096.
sid	(Optional) Sets the priority on a specific Spanning Tree. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If *sid* is not specified, priority will be set on Spanning Tree 0.

Mode

All command modes.

Usage

The device with the highest priority (lowest numerical value) becomes the Spanning Tree root device. If all devices have the same priority, the device with the lowest MAC address will then become the root device. Depending on the **set bridgepriority mode** setting as described in "set spantree bridgeprioritymode" on page 35-17, some priority values may be translated, and the translation will display in the CLI output as shown in the examples in this section.

Examples

This example shows how to set the bridge priority to 1 on all SIDs with 8021t priority mode enabled:

```
S Chassis(rw)->set spantree priority 1
Bridge Priority has been translated to incremental step of 4096
```

This example shows how to set the bridge priority to 15 on all SIDs with 8021t priority mode enabled:

```
S Chassis(rw)->set spantree priority 15
Bridge Priority has been translated to incremental step of 61440
```

This example shows how to set the bridge priority to 4000 on all SIDs with 8021t priority mode enabled:

```
S Chassis(rw)->set spantree priority 4000
Bridge Priority has been rounded up to 4096 from 4000
```

This example shows how to set the bridge priority to 10000 on all SIDs with 8021t priority mode enabled:

```
S Chassis(rw)->set spantree priority 10000
Bridge Priority has been rounded down to 8192 from 10000
```

This example shows how to set the bridge priority to 1000 on all SIDs with 8021t priority mode enabled:

```
S Chassis(rw)->set spantree priority 1000
Bridge Priority has been rounded down to 0 from 1000
```

clear spantree priority

Use this command to reset the Spanning Tree priority to the default value of 32768.

Syntax

clear spantree priority [*sid*]

Parameters

sid	(Optional) Resets the priority on a specific Spanning Tree. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If *sid* is not specified, priority will be reset on Spanning Tree 0.

Mode

All command modes.

Example

This example shows how to reset the bridge priority on SID 1:

```
S Chassis(rw)->clear spantree priority 1
```

show spantree bridgehellomode

Use this command to display the status of bridge hello mode on the device.

Syntax

```
show spantree bridgehellomode
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

When enabled, a single bridge administrative hello time is being used. When disabled, per-port administrative hello times are being used.

Example

This example shows how to display the Spanning Tree bridge hello mode. In this case, a single bridge hello mode has been enabled using "set spantree bridgehellomode" on page 35-20:

```
S Chassis(rw)->show spantree bridgehellomode
 Bridge Hello Mode is currently enabled.
```

set spantree bridgehellomode

Use this command to enable or disable bridge hello mode on the device.

Syntax

```
set spantree bridgehellomode {enable | disable}
```

Parameters

enable	Enables single Spanning Tree bridge hello mode.
disable	Disables single Spanning Tree bridge hello mode, allowing for the configuration of per-port hello times.

Defaults

None.

Mode

All command modes.

Example

This example shows how to disable single Spanning Tree hello mode on the device. Per-port hello times can now be configured using the **set spantree porthellomode** command as described in "set spantree porthello" on page 36-9:

```
S Chassis(rw)->set spantree bridgehellomode disable
```

clear spantree bridgehellomode

Use this command to reset the Spanning Tree administrative hello mode to enabled.

Syntax

clear spantree bridgehellomode

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the Spanning Tree bridge hello mode to enabled:

```
S Chassis(rw)->clear spantree bridgehellomode
```

show spantree hello

Use this command to display the Spanning Tree hello time.

Syntax

show spantree hello

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the Spanning Tree hello time:

```
S Chassis(rw)->show spantree hello
 Bridge Hello Time is set to 2 seconds
```

set spantree hello

Use this command to set the device's Spanning Tree hello time.

Syntax

set spantree hello *interval*

Parameters

interval	Specifies the number of seconds the system waits before broadcasting a bridge hello message (a multicast message indicating that the system is active). Valid values are **1** - **10**.

Defaults

None.

Mode

All command modes.

Usage

This is the time interval (in seconds) the device will transmit BPDUs indicating it is active.

Example

This example shows how to globally set the Spanning Tree hello time to 10 seconds:

```
S Chassis(rw)->set spantree hello 10
```

clear spantree hello

Use this command to reset the Spanning Tree hello time to the default value.

Syntax

clear spantree hello

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to globally reset the Spanning Tree hello time:

```
S Chassis(rw)->clear spantree hello
```

show spantree maxage

Use this command to display the Spanning Tree maximum aging time.

Syntax

show spantree maxage

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the Spanning Tree maximum aging time:

```
S Chassis(rw)->show spantree maxage
 Bridge Max Age Time is set to 20 seconds
```

set spantree maxage

Use this command to set the bridge maximum aging time.

Syntax

set spantree maxage *agingtime*

Parameters

agingtime	Specifies the maximum number of seconds that the system retains the information received from other bridges through STP. Valid values are **6** - **40**.

Defaults

None

Mode

All command modes.

Usage

Maximum aging time is the maximum time (in seconds) a device can wait without receiving a configuration message (bridge "hello") before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STP information provided in the last configuration message becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

Example

This example shows how to set the maximum aging time to 25 seconds:

```
S Chassis(rw)->set spantree maxage 25
```

clear spantree maxage

Use this command to reset the maximum aging time for a Spanning Tree to the default value.

Syntax

`clear spantree maxage`

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to globally reset the maximum aging time:

```
S Chassis(rw)->clear spantree maxage
```

show spantree fwddelay

Use this command to display the Spanning Tree forward delay time.

Syntax

`show spantree fwddelay`

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the Spanning Tree forward delay time:

```
S Chassis(rw)->show spantree fwddelay
 Bridge Forward Delay is set to 15 seconds
```

set spantree fwddelay

Use this command to set the Spanning Tree forward delay.

Syntax

set spantree fwddelay *delay*

Parameters

delay	Specifies the number of seconds for the bridge forward delay. Valid values are **4** - **30**.

Defaults

None.

Mode

All command modes.

Usage

Spanning Tree forward delay is the maximum time (in seconds) the root device will wait before changing states (for example: from listening, to learning, to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result.

Example

This example shows how to globally set the bridge forward delay to 16 seconds:

```
S Chassis(rw)->set spantree fwddelay 16
```

clear spantree fwddelay

Use this command to reset the Spanning Tree forward delay to the default setting of 15 seconds.

Syntax

clear spantree fwddelay

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to globally reset the bridge forward delay:

```
S Chassis(rw)->clear spantree fwddelay
```

show spantree autoedge

Use this command to display the status of automatic edge port detection.

Syntax

```
show spantree autoedge
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the status of the automatic edge port detection function:

```
S Chassis(rw)->show spantree autoedge
 autoEdge is currently enabled.
```

set spantree autoedge

Use this command to enable or disable the automatic edge port detection function.

Syntax

```
set spantree autoedge {disable | enable}
```

Parameters

disable | enable	Disables or enables automatic edge port detection.

Defaults

None.

Mode

All command modes.

Example

This example shows how to disable automatic edge port detection:

```
S Chassis(rw)->set spantree autoedge disable
```

clear spantree autoedge

Use this command to reset automatic edge port detection to the default state of enabled.

Syntax

clear spantree autoedge

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset automatic edge port detection to enabled:

```
S Chassis(rw)->clear spantree autoedge
```

show spantree legacypathcost

Use this command to display the default Spanning Tree path cost setting.

Syntax

show spantree legacypathcost

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the default Spanning Tree path cost setting:

```
S Chassis(rw)->show spantree legacypathcost
Legacy Path Cost is disabled
```

set spantree legacypathcost

Use this command to enable or disable legacy (802.1D) path cost values.

Syntax

```
set spantree legacypathcost {disable | enable}
```

Parameters

disable | **enable**	Enables or disables legacy (802.1D) path cost values.

Defaults

None.

Mode

All command modes.

Usage

By default, legacy path cost is disabled. Enabling the device to calculate legacy path costs affects the range of valid values that can be entered using "set spantree adminpathcost" on page 36-11.

Example

This example shows how to set the default path cost values to 802.1D:

```
S Chassis(rw)->set spantree legacypathcost enable
```

clear spantree legacypathcost

Use this command to set the Spanning Tree default value for legacy path cost to 802.1t values.

Syntax

```
clear spantree legacypathcost
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the default path cost values to 802.1t:

```
S Chassis(rw)->clear spantree legacypathcost
```

show spantree tctrapsuppress

Use this command to display the status of topology change trap suppression on Rapid Spanning Tree edge ports.

Syntax

show spantree tctrapsuppress

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the status of topology change trap suppression:

```
S Chassis(rw)->show spantree tctrapsuppress
Topology change trap suppression is currently enabled.
```

set spantree tctrapsuppress

Use this command to disable or enable topology change trap suppression on Rapid Spanning Tree edge ports.

Syntax

set spantree tctrapsupress {**disable** | **enable** | **edgedisable**}

Parameters

disable | **enable**	Disables or enables topology change trap suppression.
edgedisable	Disables sending topology change traps on edge ports.

Defaults

None.

Mode

All command modes.

Usage

By default, RSTP non-edge (bridge) ports that transition to forwarding or blocking cause the switch to issue a topology change trap. When topology change trap suppression is enabled, which is the device default, edge ports (such as end station PCs) are prevented from sending topology change traps. This is because there is usually no need for network management to monitor edge port STP transition states, such as when PCs are powered on. When topology change trap suppression is disabled, all ports, including edge and bridge ports, will transmit topology change traps.

Example

This example shows how to allow Rapid Spanning Tree edge ports to transmit topology change traps:

```
S Chassis(rw)->set spantree tctrapsuppress disable
```

clear spantree tctrapsuppress

Use this command to clear topology change trap suppression settings.

Syntax

clear spantree tctrapsuppress

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear topology change trap suppression settings:

```
S Chassis(rw)->clear spantree tctrapsuppress
```

show spantree txholdcount

Use this command to display the maximum BPDU transmission rate.

Syntax

show spantree txholdcount

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the transmit hold count setting:

```
S Chassis(rw)->show spantree txholdcount
Tx hold count = 3.
```

set spantree txholdcount

Use this command to set the maximum BPDU transmission rate.

Syntax

set spantree txholdcount *txholdcount*

Parameters

txholdcount	Specifies the maximum number of BPDUs to be transmitted before transmissions are subject to a one-second timer. Valid values are **1** - **10**. Default value is **6**.

Defaults

None.

Mode

All command modes.

Usage

Maximum BPDU transmission rate is the number of BPDUs which will be transmitted before transmissions are subject to a one-second timer.

Example

This example shows how to globally set the transmit hold count to 5:

```
S Chassis(rw)->set spantree txholdcount 5
```

clear spantree txholdcount

Use this command to reset the transmit hold count to the default value of 6.

Syntax

clear spantree txholdcount

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the transmit hold count:

```
S Chassis(rw)->clear spantree txholdcount
```

show spantree maxhops

Use this command to display the Spanning Tree maximum hop count.

Syntax

show spantree maxhops

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the Spanning Tree maximum hop count:

```
S Chassis(rw)->show spantree maxhops
Bridge Max Hop count is set to 20
```

set spantree maxhops

Use this command to set the Spanning Tree maximum hop count.

Syntax

set spantree maxhops *max_hop_count*

Parameters

max_hop_count	Specifies the maximum number of hops allowed. Valid values are **0** to **255**. Default value is **20**.

Defaults

None.

Mode

All command modes.

Usage

Spanning Tree maximum hop count is the maximum number of hops that the information for a particular Spanning Tree instance may traverse (via relay of BPDUs within the applicable MST region) before being discarded.

Example

This example shows how to set the maximum hop count to 40:

```
S Chassis(rw)->set spantree maxhops 40
```

clear spantree maxhops

Use this command to reset the maximum hop count to the default value of 20.

Syntax

clear spantree maxhops

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the maximum hop count to 20:

```
S Chassis(rw)->clear spantree maxhops
```

show spantree spanguard

Use this command to display the status of the Spanning Tree span guard function.

Syntax

show spantree spanguard

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the span guard function status:

```
S Chassis(rw)->show spantree spanguard
 spanguard is currently disabled.
```

set spantree spanguard

Use this command to enable or disable the Spanning Tree span guard function.

Syntax

```
set spantree spanguard {enable | disable}
```

Parameters

enable | **disable**	Enables or disables the span guard function.

Defaults

None.

Mode

All command modes.

Usage

When enabled, this prevents an unauthorized bridge from becoming part of the active Spanning Tree topology. It does this by disabling a port that receives a BPDU when that port has been defined as an edge (user) port (as described in "set spantree adminedge" on page 36-13). This port will remain disabled until the amount of time defined by "set spantree spanguardtimeout" on page 35-35 has passed since the last seen BPDU or the port is manually unlocked (as described in "clear / set spantree spanguardlock" on page 35-37).

Example

This example shows how to enable the span guard function:

```
S Chassis(rw)->set spantree spanguard enable
```

clear spantree spanguard

Use this command to reset the status of the Spanning Tree span guard function to disabled.

Syntax

```
clear spantree spanguard
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the status of the span guard function to disabled:

```
S Chassis(rw)->clear spantree spanguard
```

show spantree spanguardtimeout

Use this command to display the Spanning Tree span guard timeout setting.

Syntax

show spantree spanguardtimeout

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the span guard timeout setting:

```
S Chassis(rw)->show spantree spanguardtimeout
 spanguard timeout is set at 300 seconds.
```

set spantree spanguardtimeout

Use this command to set the amount of time (in seconds) an edge port will remain locked by the span guard function.

Syntax

set spantree spanguardtimeout *timeout*

Parameters

timeout	Specifies a timeout value in seconds. Valid values are **0** (forever) to **65535**.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the span guard timeout to 600 seconds:

```
S Chassis(rw)->set spantree spanguardtimeout 600
```

clear spantree spanguardtimeout

Use this command to reset the Spanning Tree span guard timeout to the default value of 300 seconds.

Syntax

clear spantree spanguardtimeout

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the span guard timeout to 300 seconds:

```
S Chassis(rw)->clear spantree spanguardtimeout
```

show spantree spanguardlock

Use this command to display the span guard lock status of one or more ports.

Syntax

show spantree spanguardlock *port-string*

Parameters

port-string	Specifies the port(s) for which to show span guard lock status. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the span guard lock status for ge.2.1:

```
S Chassis(rw)->show spantree spanguardlock ge.2.1
 spanguard status for port ge.2.1 is UNLOCKED.
```

clear / set spantree spanguardlock

Use either of these commands to unlock one or more ports locked by the Spanning Tree span guard function.

Syntax

clear spantree spanguardlock *port-string*

set spantree spanguardlock *port-string*

Parameters

port-string	Specifies port(s) to unlock. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Usage

When span guard is enabled, it locks ports that receive BPDUs when those ports have been defined as edge (user) ports (as described in "set spantree adminedge" on page 36-13).

Example

This example shows how to unlock port ge.1.16:

```
S Chassis(rw)->clear spantree spanguardlock ge.1.16
```

show spantree spanguardtrapenable

Use this command to displays the state of the Spanning Tree span guard trap function.

Syntax

show spantree spanguardtrapenable

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the state of the span guard trap function:

```
S Chassis(rw)->show spantree spanguardtrapenable
 Span Guard Trap is set to enable
```

set spantree spanguardtrapenable

Use this command to enable or disable the sending of an SNMP trap message when span guard detects that an unauthorized port has tried to join the Spanning Tree.

Syntax

set spantree spanguardtrapenable {**disable** | **enable**}

Parameters

disable | **enable**	Disables or enables the span guard trap function.

Defaults

None.

Mode

All command modes.

Example

This example shows how to disable the span guard trap function:

```
S Chassis(rw)->set spantree spanguardtrapenable disable
```

clear spantree spanguardtrap enable

Use this command to reset the Spanning Tree span guard trap function back to the default state of enabled.

Syntax

clear spantree spanguardtrapenable

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the span guard trap function to enabled:

```
S Chassis(rw)->clear spantree spanguardtrapenable
```

show spantree backuproot

Use this command to display the state of the Spanning Tree backup root function.

Syntax

show spantree backuproot [*sid*]

Parameters

sid	(Optional) Displays status for a specific Spanning Tree. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If *sid* is not specified, status will be shown for Spanning Tree 0.

Mode

All command modes.

Example

This example shows how to display the status of the backup root function on SID 0:

```
S Chassis(rw)->show spantree backuproot
Backup Root is set to disable on sid 0
```

set spantree backuproot

Use this command to enable or disable the Spanning Tree backup root function.

Syntax

set spantree backuproot *sid* {**enable** | **disable**}

Parameters

sid	Specifies the Spanning Tree on which to enable or disable the backup root function. Valid values are **0** - **4094**.
enable | **disable**	Enables or disables the backup root function.

Defaults

None.

Mode

All command modes.

Usage

Enabled by default on bridge(s) directly connected to the root bridge, this prevents stale Spanning Tree information from circulating in the event the root bridge is lost. If this happens, the backup root will dynamically lower its bridge priority so that it will be selected as the new root over the lost root bridge.

Example

This example shows how to enable the backup root function on SID 2:

```
S Chassis(rw)->set spantree backuproot 2 enable
```

clear spantree backuproot

Use this command to reset the Spanning Tree backup root function to the default state of disabled.

Syntax

clear spantree backuproot *sid*

Parameters

sid	Specifies the Spanning Tree on which to reset the backup root function. Valid values are **0** - **4094**.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the backup root function to disabled on SID 2:

```
S Chassis(rw)->clear spantree backuproot 2
```

show spantree backuproottrapendable

Use this command to display the state of the Spanning Tree backup root trap function.

Syntax

show spantree backuproottrapenable

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the status of the backup root trap function:

```
S Chassis(rw)->show spantree backuproottrapenable
Backup Root Trap is set to enable
```

set spantree backuproottrapenable

Use this command to enable or disable the Spanning Tree backup root trap function.

Syntax

set spantree backuproottrapenable {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables the backup root trap function.

Defaults

None.

Mode

All command modes.

Usage

When SNMP trap messaging is configured, this sends a trap message when the back up root function makes a Spanning Tree the new root of the network.

Example

This example shows how to enable the backup root trap function:

```
S Chassis(rw)->set spantree backuproottrapenable enable
```

clear spantree backuproottrapenable

Use this command to reset the Spanning Tree backup root trap function to the default state of disabled.

Syntax

clear spantree backuproottrapenable

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the backup root trap function:

```
S Chassis(rw)->clear spantree backuproottrapenable
```

show spantree newroottrapendable

Use this command to display the state of the Spanning Tree new root trap function.

Syntax

show spantree newroottrapenable

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the status of the new root trap function:

```
S Chassis(rw)->show spantree newroottrapenable
New Root Trap is set to enable
```

set spantree newroottrapenable

Use this command to enable or disable the Spanning Tree new root trap function.

Syntax

set spantree newroottrapenable {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables the backup root trap function.

Defaults

None.

Mode

All command modes.

Usage

When SNMP trap messaging is configured, this sends a trap message when a Spanning Tree becomes the new root of the network.

Example

This example shows how to enable the new root trap function:

```
S Chassis(rw)->set spantree newroottrapenable enable
```

clear spantree newroottrapenable

Use this command to reset the Spanning Tree new root trap function back to the default state of enabled.

Syntax

clear spantree newroottrapenable

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the new root trap function to enabled:

```
S Chassis(rw)->clear spantree newroottrapenable
```

clear spantree default

Use this command to restore default values to a Spanning Tree.

Syntax

clear spantree default [*sid*]

Parameters

sid	(Optional) Restores defaults on a specific Spanning Tree. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If *sid* is not specified, defaults will be restored on Spanning Tree 0.

Mode

All command modes.

Example

This example shows how to restore Spanning Tree defaults on SID 1:

```
S Chassis(rw)->clear spantree default 1
```

show spantree debug

Use this command to display Spanning Tree debug counters for one or more ports.

Syntax

show spantree debug [**port** *port-string*] [**sid** *sid*] [**active**]

Parameters

port *port-string*	(Optional) Displays debug counters for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
sid *sid*	(Optional) Displays the debug counters for a specific Spanning Tree identifier. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.
active	(Optional) Displays only the debug counters for ports that have received at least one configuration or RSTP BPDU.

Defaults

- If *port-string* is not specified, no port information will be displayed.
- If *sid* is not specified, debug counters will be displayed for Spanning Tree 0.

Mode

All command modes.

Example

This example shows how to display Spanning Tree debug counters for link aggregation port 1, SID 0:

```
S Chassis(rw)->show spantree debug port lag.0.1

SID: 0, Bridge ID: 80-00-00-01-f4-5b-5e-8f, Time Since TC: 00 days 00:42:49

Root Priority Vector
---------------------------------------------------------------
Root ID                      - 40-00-00-e0-63-93-74-a7
External Cost                - 66666
Regional Root ID             - 80-00-00-01-f4-5b-5e-8f
Internal Cost                - 0
Designated Bridge ID         - 40-00-00-e0-63-93-74-a7
Designated Port              - 8700
Receive Port                 - 8002      (lag.0.1)

Alternate Ports          Designated Bridge
---------------------------------------------------------------
(none)

Ports with Received TC BPDUs         Count
```

```
------------------------------------------------------------
lag.0.1                                  2
ge.4.10                                  4

Ports with Message Age Expired       Count
------------------------------------------------------------
(none)

Ports with Exceptional Condition    Reason
------------------------------------------------------------
(none)

STP Diagnostic Common Counters
------------------------------------------------------------
Topology Change Count        - 2
Message Expiration Count     - 0
Invalid BPDU Count           - 0
Disputed BPDU Count          - 0
STP BPDU Rx Count            - 0
STP BPDU Tx Count            - 0
STP TCN BPDU Rx Count        - 0
STP TCN BPDU Tx Count        - 0
STP TC BPDU Rx Count         - 0
STP TC BPDU Tx Count         - 0
RST BPDU Rx Count            - 0
RST BPDU Tx Count            - 0
RST TC BPDU Rx Count         - 0
RST TC BPDU Tx Count         - 0
MST BPDU Rx Count            - 2582
MST BPDU Tx Count            - 2592
MST CIST TC BPDU Rx Count    - 6
MST CIST TC BPDU Tx Count    - 6

STP Diagnostic Root History Table for SID 0
------------------------------------------------------------
Index       Root Bridge ID          Date       Time
------------------------------------------------------------
01     40-00-00-e0-63-93-74-a7   07-07-2009, 09:50:56
02     00-00-00-00-00-00-00-00   07-07-2009, 09:50:19

STP Port Data for SID 0 Port lag.0.1
------------------------------------------------------------
Role                         - root
State                        - forwarding
NonFwd Reason                - none
```

```
Edge Port                    - false
Boundary Port                - true
Root ID                      - 40-00-00-e0-63-93-74-a7
External Cost                - 0
Regional Root ID             - 40-00-00-e0-63-93-74-a7
Internal Cost                - 0
Designated Bridge ID         - 40-00-00-e0-63-93-74-a7
Designated Port              - 8700
Port Id                      - 8002
Forward Transitions Count    - 1

STP Diagnostic Port Counters for SID 0 Port lag.0.1
-----------------------------------------------------------
Message Expiration Count     - 0
Invalid BPDU Count           - 0
Disputed BPDU Count          - 0
STP BPDU Rx Count            - 0
STP BPDU Tx Count            - 0
STP TCN BPDU Rx Count        - 0
STP TCN BPDU Tx Count        - 0
STP TC BPDU Rx Count         - 0
STP TC BPDU Tx Count         - 0
RST BPDU Rx Count            - 0
RST BPDU Tx Count            - 0
RST TC BPDU Rx Count         - 0
RST TC BPDU Tx Count         - 0
MST BPDU Rx Count            - 1287
MST BPDU Tx Count            - 4
MST CIST TC BPDU Rx Count    - 2
MST CIST TC BPDU Tx Count    - 2
```

clear spantree debug

Use this command to clear Spanning Tree debug counters.

Syntax

clear spantree debug

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear Spanning Tree debug counters:

```
S Chassis(rw)->clear spantree debug
```

36

Spanning Tree Port Commands

This chapter provides detailed information for the Spanning Tree port set of commands. Spanning tree port functionality includes the displaying and setting of Spanning Tree port parameters, including enabling or disabling the Spanning Tree algorithm on one or more ports, displaying designated bridge, port and root information, displaying blocked ports, displaying and setting Spanning Tree port priorities and costs, configuring edge port parameters, and setting point-to-point protocol mode. For information about configuring Spanning Tree, refer to the "Spanning Tree Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show spantree portenable	36-2
set spantree portenable	36-2
clear spantree portenable	36-3
show spantree portadmin	36-3
set spantree portadmin	36-4
clear spantree portadmin	36-5
set spantree protomigration	36-5
show spantree portstate	36-6
show spantree blockedports	36-6
show spantree portpri	36-7
set spantree portpri	36-8
clear spantree portpri	36-8
set spantree porthello	36-9
clear spantree porthello	36-9
show spantree portcost	36-10
show spantree adminpathcost	36-10
set spantree adminpathcost	36-11
clear spantree adminpathcost	36-12
show spantree adminedge	36-12
set spantree adminedge	36-13
clear spantree adminedge	36-13
show spantree operedge	36-14

For information about...	Refer to page...
show spantree adminpoint	36-14
show spantree operpoint	36-15
set spantree adminpoint	36-16
clear spantree adminpoint	36-16
show spantree restrictedtcn	36-17
set spantree restrictedtcn	36-17
clear spantree restrictedtcn	36-18
show spantree restrictedrole	36-19
set spantree restrictedrole	36-19
clear spantree restrictedrole	36-20

show spantree portenable

Use this command to display the port status on one or more Spanning Tree ports.

Syntax

show spantree portenable [**port** *port-string*]

Parameters

port *port-string*	(Optional) Displays status for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, status will be displayed for all ports.

Mode

All command modes.

Example

This example shows how to display status for port ge.1.12:

```
S Chassis(rw)->show spantree portenable port ge.1.12
Port ge.1.12    has a Port Status of Enabled on SID 0
```

set spantree portenable

Use this command to set the port status on one or more Spanning Tree ports.

Syntax

set spantree portenable *port-string* {**enable** | **disable**}

Parameters

port-string	Specifies the port(s) to enable or disable. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
enable | **disable**	Enables or disables the Spanning Tree port.

Defaults

None.

Mode

All command modes.

Example

This example shows how to enable Spanning Tree port ge.1.12:

```
S Chassis(rw)->set spantree portenable ge.1.12 enable
```

clear spantree portenable

Use this command to reset the default value for one or more Spanning Tree ports to enabled.

Syntax

clear spantree portenable *port-string*

Parameters

port-string	Specifies port(s) to reset. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the default Spanning Tree port status value to enabled on ge.1.12:

```
S Chassis(rw)->clear spantree portenable ge.1.12
```

show spantree portadmin

Use this command to display the status of the Spanning Tree algorithm on one or more ports.

Syntax

show spantree portadmin [**port** *port-string*]

Parameters

port *port-string*	(Optional) Displays status for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, status will be displayed for all ports.

Mode

All command modes.

Example

This example shows how to display port admin status for ge.1.7:

```
S Chassis(rw)->show spantree portadmin port ge.1.7
Port ge.1.7 has portadmin set to enable on SID 0
```

set spantree portadmin

Use this command to disable or enable the Spanning Tree algorithm on one or more ports.

Syntax

set spantree portadmin *port-string* **{disable | enable}**

Parameters

port-string	Specifies the port(s) for which to enable or disable Spanning Tree. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
disable | **enable**	Disables or enables the Spanning Tree algorithm on the specified port(s).

Defaults

None.

Mode

All command modes.

Example

This example shows how to disable Spanning Tree on ge.1.5:

```
S Chassis(rw)->set spantree portadmin ge.1.5 disable
```

clear spantree portadmin

Use this command to reset the default Spanning Tree admin status to enable on one or more ports.

Syntax

clear spantree portadmin *port-string*

Parameters

port-string	Resets the default admin status on specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the default Spanning Tree admin state to enable on ge.1.12:

```
S Chassis(rw)->clear spantree portadmin ge.1.12
```

set spantree protomigration

Use this command to reset the port protocol migration state machine for one or more Spanning Tree ports. When operating in RSTP mode, this forces a port to transmit MSTP BPDUs.

Syntax

set spantree protomigration *port-string* **true**

Parameters

port-string	Specifies the port(s) for which protocol migration mode will be enabled. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
true	Enables protocol migration mode.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the port protocol migration state machine on ge.1.12:

```
S Chassis(rw)->set spantree protomigration ge.1.12 true
```

show spantree portstate

Use this command to display the state (blocking, forwarding, etc.) for a port on one or more Spanning Trees.

Syntax

show spantree portstate [**port** *port-string*] [**sid** *sid*]

Parameters

port *port-string*	(Optional) Displays the Spanning Tree state for specific Spanning Tree port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
sid *sid*	(Optional) Displays the state for a specific Spanning Tree identifier. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

- If *port-string* is not specified, current state will be displayed for all Spanning Tree ports.
- If *sid* is not specified, current port state will be displayed for Spanning Tree 0.

Mode

All command modes.

Example

This example shows how to display the Spanning Tree state for ge.1.7:

```
S Chassis(rw)->show spantree portstate port ge.1.7
Port ge.1.7 has a Port State of Forwarding on SID 0
```

show spantree blockedports

Use this command to display the blocked ports in a Spanning Tree.

Syntax

show spantree blockedports [*sid*]

Parameters

sid	(Optional) Displays blocked ports on a specific Spanning Tree. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If *sid* is not specified, blocked ports will be displayed for Spanning Tree 0.

Mode

All command modes.

Usage

A port in this state does not participate in the transmission of frames, thus preventing duplication arising through multiple paths existing in the active topology of the bridged LAN. It receives Spanning Tree configuration messages, but does not forward packets.

Example

This example shows how to display blocked ports on SID 1:

```
S Chassis(rw)->show spantree blockedports 1

SID   Port
---   ---------
1     ge.1.1
1     ge.1.3
1     ge.1.5

Number of blocked ports in SID 1 : 3
```

show spantree portpri

Use this command to show the Spanning Tree priority for one or more ports. Port priority is a component of the port ID, which is one element used in determining Spanning Tree port roles.

Syntax

show spantree portpri [**port** *port-string*] [**sid** *sid*]

Parameters

port *port-string*	(Optional) Specifies the port(s) for which to display Spanning Tree priority. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
sid *sid*	(Optional) Displays port priority for a specific Spanning Tree identifier. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

- If *port-string* is not specified, port priority will be displayed for all Spanning Tree ports.
- If *sid* is not specified, port priority will be displayed for Spanning Tree 0.

Mode

All command modes.

Example

This example shows how to display the port priority for ge.2.7:

```
S Chassis(rw)->show spantree portpri port ge.2.7
Port ge.2.7 has a Port Priority of 128 on SID 0
```

set spantree portpri

Use this command to set a port's Spanning Tree priority.

Syntax

set spantree portpri *port-string priority* [**sid** *sid*]

Parameters

port-string	Specifies the port(s) for which to set Spanning Tree port priority. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
priority	Specifies a number that represents the priority of a link in a Spanning Tree bridge. Valid values are from **0** to **240 (in increments of 16)** with 0 indicating high priority.
sid *sid*	(Optional) Sets port priority for a specific Spanning Tree identifier. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If *sid* is not specified, port priority will be set for Spanning Tree 0.

Mode

All command modes.

Example

This example shows how to set the priority of ge.1.3 to 240 on SID 1.

```
S Chassis(rw)->set spantree portpri ge.1.3 240 sid 1:
```

clear spantree portpri

Use this command to reset the bridge priority of a Spanning Tree port to the default value of 128.

Syntax

clear spantree portpri *port-string* [**sid** *sid*]

Parameters

port-string	Specifies the port(s) for which to set Spanning Tree port priority. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
sid *sid*	(Optional) Resets the port priority for a specific Spanning Tree identifier. Valid values are **0** - **4094**. If not specified, SID 0 will be assumed.

Defaults

If *sid* is not specified, port priority will be set for Spanning Tree 0.

Mode

All command modes.

Example

This example shows how to reset the priority of ge.1.3 to 128 on SID 1:

```
S Chassis(rw)->clear spantree portpri ge.1.3 sid 1:
```

set spantree porthello

Use this command to set the hello time for one or more Spanning Tree ports. This is the time interval (in seconds) the port(s) will transmit BPDUs.

Syntax

set spantree porthello *port-string interval*

Parameters

port-string	Specifies the port(s) for which to set hello time.
interval	Specifies the number of seconds the system waits before broadcasting a bridge hello message. Valid values are **1** - **10.**

Defaults

None.

Mode

All command modes.

Usage

This command can be executed only if bridge hello mode is disabled. For information on using the **set spantree bridgehellomode** command, refer to "set spantree bridgehellomode" on page 35-20.

Example

This example shows how to set the hello time to 3 seconds for port ge.1.4:

```
S Chassis(rw)->set spantree porthello ge.1.4 3
```

clear spantree porthello

Use this command to reset the hello time for one or more Spanning Tree ports to the default of 2 seconds.

Syntax

clear spantree porthello *port-string*

Parameters

port-string	Specifies the port(s) for which to reset hello time.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the hello time to 2 seconds for port ge.1.4:

```
S Chassis(rw)->clear spantree porthello ge.1.4
```

show spantree portcost

Use this command to display cost values assigned to one or more Spanning Tree ports.

Syntax

show spantree portcost [**port** *port-string*] [**sid** *sid*]

Parameters

port *port-string*	(Optional) Displays cost values for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
sid *sid*	(Optional) Displays port cost for a specific Spanning Tree identifier. Valid values are **0** - **4094**. If not specified, SID 0 will be assumed.

Defaults

- If *port-string* is not specified, port cost will be displayed for all Spanning Tree ports.
- If *sid* is not specified, port cost will be displayed for all Spanning Trees.

Mode

All command modes.

Example

This example shows how to display the port cost for ge.2.5:

```
S Chassis(rw)->show spantree portcost port ge.2.5
Port ge.2.5 has a Port Path Cost of 2000000 on SID 0
```

show spantree adminpathcost

Use this command to display the admin path cost for a port on one or more Spanning Trees.

Syntax

show spantree adminpathcost [**port** *port-string*] [**sid** *sid*]

Parameters

port *port-string*	(Optional) Displays the admin path cost value for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
sid *sid*	(Optional) Displays the admin path cost for a specific Spanning Tree identifier. Valid values are **0** - **4094**. If not specified, SID 0 will be assumed.

Defaults

- If *port-string* is not specified, admin path cost for all Spanning Tree ports will be displayed.
- If *sid* is not specified, admin path cost for Spanning Tree 0 will be displayed.

Mode

All command modes.

Example

This example shows how to display the admin path cost for ge.3.4 on SID 1:

```
S Chassis(rw)->show spantree adminpathcost port ge.3.4 sid 1
Port ge.3.4 has a Port Admin Path Cost of 0 on SID 1
```

set spantree adminpathcost

Use this command to set the administrative path cost on a port and one or more Spanning Trees.

Syntax

set spantree adminpathcost *port-string cost* [**sid** *sid*]

Parameters

port-string	Specifies the port(s) on which to set an admin path cost. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
cost	Specifies the port path cost. Va1id values are: • **0** - **65535** if legacy path cost is enabled. • **0** - **200000000** if legacy path cost is disabled.
sid *sid*	(Optional) Sets the admin path cost for a specific Spanning Tree identifier. Valid values are **0** - **4094**. If not specified, SID 0 will be assumed.

Defaults

If *sid* is not specified, admin path cost will be set for Spanning Tree 0.

Mode

All command modes.

Usage

By default, this value is set to 0, which forces the port to recalculate Spanning Tree path cost based on the speed of the port and whether or not legacy path cost is enabled. For details on using the **set spantree legacypathcost** command, refer to "set spantree legacypathcost" on page 35-28.

Example

This example shows how to set the admin path cost to 200 for ge.3.2 on SID 1:

```
S Chassis(rw)->set spantree adminpathcost ge.3.2 200 sid 1
```

clear spantree adminpathcost

Use this command to reset the Spanning Tree default value for port admin path cost to 0.

Syntax

clear spantree adminpathcost *port-string* [**sid** *sid*]

Parameters

port-string	Specifies the port(s) for which to reset admin path cost. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
sid *sid*	(Optional) Resets the admin path cost for specific Spanning Tree(s). Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If *sid* is not specified, admin path cost will be reset for Spanning Tree 0.

Mode

All command modes.

Example

This example shows how to reset the admin path cost to 0 for ge.3.2 on SID 1:

```
S Chassis(rw)->clear spantree adminpathcost ge.3.2 sid 1
```

show spantree adminedge

Use this command to display the edge port administrative status for a port.

Syntax

show spantree adminedge [**port** *port-string*]

Parameters

port *port-string*	(Optional) Displays edge port administrative status for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified edge port administrative status will be displayed for all Spanning Tree ports.

Mode

All command modes.

Example

This example shows how to display the edge port status for ge.3.2:

```
S Chassis(rw)->show spantree adminedge port ge.3.2
Port ge.3.2 has a Port Admin Edge of Edge-Port
```

set spantree adminedge

Use this command to set the edge port administrative status on a Spanning Tree port.

Syntax

set spantree adminedge *port-string* **{true | false}**

Parameters

port-string	Specifies the edge port. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
true | **false**	Enables (**true**) or disables (**false**) the specified port as a Spanning Tree edge port.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set ge.1.11 as an edge port:

```
S Chassis(rw)->set spantree adminedge ge.1.11 true
```

clear spantree adminedge

Use this command to reset a Spanning Tree port to non-edge status.

Syntax

clear spantree adminedge *port-string*

Parameters

port-string	Specifies port(s) on which to reset edge port status. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset ge.1.11 as a non-edge port:

```
S Chassis(rw)->clear spantree adminedge ge.1.11
```

show spantree operedge

Use this command to display the Spanning Tree edge port operating status for a port.

Syntax

show spantree operedge [**port** *port-string]*

Parameters

port *port-string*	(Optional) Displays edge port operating status for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified edge port operating status will be displayed for all Spanning Tree ports.

Mode

All command modes.

Example

This example shows how to display the edge port status for ge.2.7:

```
S Chassis(rw)->show spantree operedge port ge.2.7
Port ge.2.7 has a Port Oper Edge of Edge-Port
```

show spantree adminpoint

Use this command to display the administrative point-to-point status of the LAN segment attached to a Spanning Tree port.

Syntax

show spantree adminpoint [**port** *port-string]*

Parameters

port *port-string*	(Optional) Displays point-to-point status for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, status will be displayed for all Spanning Tree port(s).

Mode

All command modes.

Example

This example shows how to display the point-to-point status of the LAN segment attached to ge.2.7:

```
S Chassis(rw)->show spantree adminpoint port ge.2.7
Port ge.2.7 has a Port Admin Point to Point of Auto
```

show spantree operpoint

Use this command to display the operating point-to-point status of the LAN segment attached to a port.

Syntax

show spantree operpoint [**port** *port-string]*

Parameters

port *port-string*	(Optional) Displays point-to-point operating status for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If not specified, status will be displayed for all ports.

Mode

All command modes.

Example

This example shows how to display the point-to-point status operating of the LAN segment attached to ge.2.7:

```
S Chassis(rw)->show spantree operpoint port ge.2.7
Port ge.2.7 has a Port Oper Point to Point of False on SID 1
```

set spantree adminpoint

Use this command to set the administrative point-to-point status of the LAN segment attached to a Spanning Tree port.

Syntax

set spantree adminpoint *port-string* {**true** | **false** | **auto**}

Parameters

port-string	Specifies the port on which to set point-to-point protocol status. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
true | **false** | **auto**	Specifies the point-to-point status of the LAN attached to the specified port. • **true** forces the port to be considered point-to-point. • **false** forces the port to be considered non point-to-point. • **auto** (the default setting) allows the firmware to determine the port's point-to-point status.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the LAN attached to ge.1.3 as a point-to-point segment:

```
S Chassis(rw)->set spantree adminpoint ge.1.3 true
```

clear spantree adminpoint

Use this command to reset the administrative point-to-point status of the LAN segment attached to a Spanning Tree port to auto mode.

Syntax

clear spantree adminpoint *port-string*

Parameters

port-string	Specifies port(s) on which to reset point-to-point protocol status. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset point-to-point status to auto on ge.2.3:

```
S Chassis(rw)->clear spantree adminpoint ge.2.3
```

show spantree restrictedtcn

Use this command to display the restricted Topology Change Notification (TCN) status on the specified port(s) or all ports on the device.

Syntax

show spantree restrictedtcn [**port** *port-string*]

Parameters

port *port-string*	(Optional) Displays Restricted TCN status for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If the **port** *port-string* option is not specified, status will be displayed for all ports.

Mode

All command modes.

Example

This example shows how to display the Restricted TCN status for port ge.2.1:

```
S Chassis(rw)->show spantree restrictedtcn port ge.2.1
Port ge.2.1     has restrictedTcn set to False
```

set spantree restrictedtcn

Use this command to allow or disallow Topology Change Notification (TCN) propagation on the specified port(s).

Syntax

set spantree restrictedtcn *port-string* {**true** | **false**}

Parameters

port-string	Specifies the port(s) on which to allow or disallow TCN propagation. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

true | **false**	Specifies whether TCN propagation is allowed or not allowed on the specified port(s). Restricted TCN is set to **false** (not restricted) by default. • **true** – TCN propagation is not allowed on the specified port(s) • **false** – TCN propagation is allowed on the specified port(s).

Defaults

None.

Mode

All command modes.

Usage

Setting this command to true prevents unnecessary address flushing in the core region of the network caused by activation of bridges external to the core. When set to true, temporary loss of connectivity can occur after changes in a Spanning Tree's active topology, due to persistent, incorrectly learned, station location information. A possible reason for not allowing TCN propagation is when bridges are not under the full control of the administrator or because MAC_Operational for the attached LANs transitions frequently.

TCN propagation is set to **false** by default: the port propagates received TCNs and topology changes to other ports.

Example

This example shows how to allow TCN propagation on ports ge.2.1-3:

```
S Chassis(rw)->set spantree restrictedtcn ge.2.1-3 true
```

clear spantree restrictedtcn

Use this command to reset the port TCN propagation behavior to the default setting for the specified port(s).

Syntax

clear spantree restrictedtcn *port-string*

Parameters

port-string	Specifies port(s) on which to reset the port TCN propagation setting to the default value of **false**. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the port TCN propagation behavior to the default setting for port ge.2.3:

```
S Chassis(rw)->clear spantree restrictedtcn ge.2.3
```

show spantree restrictedrole

Use this command to display the Restricted Role status on the specified port(s) or all ports on the device.

Syntax

show spantree restrictedrole [**port** *port-string*]

Parameters

port *port-string*	(Optional) Displays Restricted Role status for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If the **port** *port-string* option is not specified, status will be displayed for all ports.

Mode

All command modes.

Example

This example shows how to display the Restricted Role status for port ge.2.1:

```
S Chassis(rw)->show spantree restrictedrole port ge.2.1
Port ge.2.1     has restrictedRole set to False
```

set spantree restrictedrole

Use this command to allow or disallow the root role on the specified port(s) on the device.

Syntax

set spantree restrictedrole *port-string* {**true** | **false**}

Parameters

port-string	Specifies the port(s) on which to allow or not allow the root role. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
true | **false**	Specifies whether the root role is allowed or not allowed on the specified port(s). Restricted role is set to **false** by default. • **true** – Root role is not allowed on the specified port(s) • **false** – Root role is allowed on the specified port(s).

Defaults

None.

Mode

All command modes.

Usage

When Restricted Role is set to true, the port will not be selected as the root port for the common instance Spanning Tree or any multiple Spanning Tree instance, even if it has the best Spanning Tree priority. The Restricted Role port set to true is selected as an alternate port after the root port has been selected. If set to true, Restricted Role can cause lack of Spanning Tree connectivity. Setting Restricted Role to true prevents bridges, external to a core region of the network, from influencing the Spanning Tree active topology. You may wish to use Restricted Role when bridges are not under your full control.

Restricted role is set to **false** (root role is allowed) by default.

Example

This example shows how to not allow root role on ports ge.2.1-3:

```
S Chassis(rw)->set spantree restrictedrole ge.2.1-3 true
```

clear spantree restrictedrole

Use this command to reset the port Restricted Role feature to the default setting for the specified port(s).

Syntax

clear spantree restrictedrole *port-string*

Parameters

port-string	Specifies port(s) on which to reset the restricted role feature setting to the default value of **false**. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the port Restricted Role feature to the default setting for port ge.2.3:

```
S Chassis(rw)->clear spantree restrictedrole ge.2.3
```

37

Spanning Tree Loop Protect Commands

This chapter provides detailed information for the spanning tree loop protect set of commands. Spanning tree loop protect functionality includes the display and setting of Spanning Tree Loop Protect parameters, including the global parameters of Loop Protect threshold, window, enabling traps, and disputed BPDU threshold, as well as per port and port/SID parameters. For information about configuring Spanning Tree Loop Protect, refer to the "Spanning Tree Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

The Loop Protect feature prevents or short circuits loop formation in a network with redundant paths by requiring ports to receive type 2 BPDUs (RSTP/MSTP) on point-to-point inter-switch links (ISLs) before their states are allowed to become forwarding. Further, if a BPDU timeout occurs on a port, its state becomes listening until a BPDU is received.

In this way, both upstream and downstream facing ports are protected. When a root or alternate port loses its path to the root bridge due to a message age expiration it takes on the role of designated port. It will not forward traffic until a BPDU is received. When a port is intended to be the designated port in an ISL it constantly proposes and will not forward until a BPDU is received, and will revert to listening if it fails to get a response. This protects against misconfiguration and protocol failure by the connected bridge.

By default, the Loop Protect feature is globally disabled on Extreme Networks S-Series devices and must be globally enabled to operate on all ports. For configuration information, refer to the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
set spantree lp	37-2
show spantree lp	37-3
clear spantree lp	37-3
show spantree lplock	37-4
clear spantree lplock	37-5
set spantree lpcapablepartner	37-5
show spantree lpcapablepartner	37-6
clear spantree lpcapablepartner	37-7
set spantree lpthreshold	37-7
show spantree lpthreshold	37-8
clear spantree lpthreshold	37-8
set spantree lpwindow	37-9
show spantree lpwindow	37-9

For information about...	Refer to page...
clear spantree lpwindow	37-10
set spantree lptrapenable	37-10
show spantree lptrapenable	37-11
clear spantree lptrapenable	37-11
set spantree disputedbpduthreshold	37-12
show spantree disputedbpduthreshold	37-12
clear spantree disputedbpduthreshold	37-13
show spantree nonforwardingreason	37-13

set spantree lp

Use this command to enable or disable the Loop Protect feature per port and optionally, per SID.

Syntax

set spantree lp *port-string* {**enable** | **disable**} [**sid** *sid*]

Parameters

port-string	Specifies port(s) on which to enable or disable the Loop Protect feature. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
enable | **disable**	Enables or disables the feature on the specified port.
sid *sid*	(Optional) Enables or disables the feature for specific Spanning Tree(s). Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If no SID is specified, SID 0 is assumed.

Mode

All command modes.

Usage

The Loop Protect feature is disabled by default. See the *Extreme Networks S-Series Configuration Guide* for more information.

Loop Protect takes precedence over per port STP enable/disable (portAdmin). Normally portAdmin disabled would cause a port to go immediately to forwarding. If Loop Protect is enabled, that port should go to listening and remain there.

Note: The Loop Protect enable/disable settings for an MSTI port should match those for the CIST port.

Example

This example shows how to enable Loop Protect on ge.2.3:

```
S Chassis(rw)->set spantree lp enable ge.2.3
```

show spantree lp

Use this command to display the Loop Protect status per port and/or per SID.

Syntax

show spantree lp [**port** *port-string*] [**sid** *sid*]

Parameters

port-string	(Optional) Specifies port(s) for which to display the Loop Protect feature status. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
sid *sid*	(Optional) Specifies the specific Spanning Tree(s) for which to display the Loop Protect feature status. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If no *port-string* is specified, status is displayed for all ports.

If no SID is specified, SID 0 is assumed.

Mode

All command modes.

Example

This example shows how to display Loop Protect status on ge.2.3:

```
S Chassis(rw)->show spantree lp port ge.2.3
LoopProtect is enabled on port ge.2.3    , SID 0
```

clear spantree lp

Use this command to return the Loop Protect status per port and optionally, per SID, to its default state of disabled.

Syntax

clear spantree lp *port-string* [**sid** *sid*]

Parameters

port-string	Specifies port(s) for which to clear the Loop Protect feature status. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
sid *sid*	(Optional) Specifies the specific Spanning Tree(s) for which to clear the Loop Protect feature status. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If no SID is specified, SID 0 is assumed.

Mode

All command modes.

Example

This example shows how to return the Loop Protect state on ge.2.3 to disabled:

```
S Chassis(rw)->clear spantree lp port ge.2.3
```

show spantree lplock

Use this command to display the Loop Protect lock status per port and/or per SID.

Syntax

show spantree lplock [**port** *port-string*] [**sid** *sid*]

Parameters

port-string	(Optional) Specifies port(s) for which to display the Loop Protect lock status. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
sid *sid*	(Optional) Specifies the specific Spanning Tree(s) for which to display the Loop Protect lock status. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If no *port-string* is specified, status is displayed for all ports.

If no SID is specified, SID 0 is assumed.

Mode

All command modes.

Usage

A port can become locked if a configured number of Loop Protect events occur during the configured window of time. See the set spantree lpthreshold and set spantree lpwindow commands. Once a port is forced into blocking (locked), it remains locked until manually unlocked with the clear spantree lplock command.

Example

This example shows how to display Loop Protect lock status on ge.1.1:

```
S Chassis(rw)->show spantree lplock port ge.1.1
LoopProtect Lock status for port ge.1.1    , SID 0   is UNLOCKED.
```

clear spantree lplock

Use this command to manually unlock a blocked port and optionally, per SID.

Syntax

clear spantree lplock *port-string* [**sid** *sid*]

Parameters

port-string	Specifies port(s) for which to clear the Loop Protect lock. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
sid *sid*	(Optional) Specifies the specific Spanning Tree(s) for which to clear the Loop Protect lock. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If no SID is specified, SID 0 is assumed.

Mode

All command modes.

Usage

The default state is unlocked.

Example

This example shows how to clear Loop Protect lock from ge.1.1:

```
S Chassis(rw)->show spantree lplock port ge.1.1
LoopProtect Lock status for port ge.1.1    , SID 0   is LOCKED.
S Chassis(rw)->clear spantree lplock ge.1.1
S Chassis(rw)->show spantree lplock port ge.1.1
LoopProtect Lock status for port ge.1.1    , SID 0   is UNLOCKED.
```

set spantree lpcapablepartner

Use this command to specify per port whether the link partner is Loop Protect capable.

Syntax

set spantree lpcapablepartner *port-string* {**true** | **false**}

Parameters

port-string	Specifies port(s) for which to configure a Loop Protect capable link partner. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
true | **false**	Specifies whether the link partner is capable (true) or not (false).

Defaults

None.

Mode

All command modes.

Usage

The default value for Loop Protect capable partner is false. If the port is configured with a Loop Protect capable partner (true), then the full functionality of the Loop Protect feature is used. If the value is false, then there is some ambiguity as to whether an Active Partner timeout is due to a loop protection event or is a normal situation due to the fact that the partner port does not transmit Alternate Agreement BPDUs. Therefore, a conservative approach is taken in that designated ports will not be allowed to forward unless receiving agreements from a port with root role.

This type of timeout will not be considered a loop protection event. Loop protection is maintained by keeping the port from forwarding but since this is not considered a loop event it will not be factored into locking the port.

Refer to the *Extreme Networks S-Series Configuration Guide* for more information.

Example

This example shows how to set the Loop Protect capable partner to true for ge.1.1:

```
S Chassis(rw)->set spantree lpcapablepartner ge.1.1 true
```

show spantree lpcapablepartner

Use this command to the Loop Protect capability of a link partner for one or more ports.

Syntax

show spantree lpcapablepartner [**port** *port-string*]

Parameters

port-string	(Optional) Specifies port(s) for which to display Loop Protect capability for its link partner. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If no *port-string* is specified, Loop Protect capability for link partners is displayed for all ports.

Mode

All command modes.

Example

This example shows how to display the Loop Protect partner capability for ge.1.1:

```
S Chassis(rw)->show spantree lpcapablepartner port ge.1.1
Link partner of port ge.1.1     is not LoopProtect-capable.
```

clear spantree lpcapablepartner

Use this command to reset the Loop Protect capability of port link partners to the default state of false.

Syntax

clear spantree lpcapablepartner *port-string*

Parameters

port-string	Specifies port(s) for which to clear their link partners' Loop Protect capability (reset to false). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the Loop Protect partner capability for ge.1.1:

```
S Chassis(rw)->clear spantree lpcapablepartner ge.1.1
```

set spantree lpthreshold

Use this command to set the Loop Protect event threshold.

Syntax

set spantree lpthreshold *value*

Parameters

value	Specifies the number of events that must occur during the event window in order to lock a port/SID. The default value is 3 events. A threshold of 0 specifies that ports will never be locked.

Defaults

None. The default event threshold is 3.

Mode

All command modes.

Usage

The LoopProtect event threshold is a global integer variable that provides protection in the case of intermittent failures. The default value is 3. If the event counter reaches the threshold within a given period (the event window), then the port, for the given SID, becomes locked (that is, held indefinitely in the blocking state). If the threshold is 0, the ports are never locked.

Example

This example shows how to set the Loop Protect threshold value to 4:

```
S Chassis(rw)->set spantree lpthreshold 4
```

show spantree lpthreshold

Use this command to display the current value of the Loop Protect event threshold.

Syntax

show spantree lpthreshold

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the current Loop Protect threshold value:

```
S Chassis(rw)->show spantree lpthreshold
LoopProtect event threshold is set to 4
```

clear spantree lpthreshold

Use this command to return the Loop Protect event threshold to its default value of 3.

Syntax

clear spantree lpthreshold

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the Loop Protect event threshold to the default of 3:

```
S Chassis(rw)->clear spantree lpthreshold
```

set spantree lpwindow

Use this command to set the Loop Protect event window value in seconds.

Syntax

set spantree lpwindow *value*

Parameters

value	Specifies the number of seconds that comprise the period during which Loop Protect events are counted. The default event window is 180 seconds.

Defaults

None.

Mode

All command modes.

Usage

The Loop Protect Window is a timer value, in seconds, that defines a period during which Loop Protect events are counted. The default value is 180 seconds. If the timer is set to 0, the event counter is not reset until the Loop Protect event threshold is reached. If the threshold is reached, that constitutes a loop protection event.

Example

This example shows how to set the Loop Protect event window to 120 seconds:

```
S Chassis(rw)->set spantree lpwindow 120
```

show spantree lpwindow

Use this command to display the current Loop Protect event window value.

Syntax

show spantree lpwindow

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the current Loop Protect window value:

```
S Chassis(rw)->show spantree lpwindow
LoopProtect event window is set to 120 seconds
```

clear spantree lpwindow

Use this command to reset the Loop Protect event window to the default value of 180 seconds.

Syntax

clear spantree lpwindow

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the Loop Protect event window to the default of 180 seconds:

```
S Chassis(rw)->clear spantree lpwindow
```

set spantree lptrapenable

Use this command to enable or disable Loop Protect event notification.

Syntax

set spantree lptrapenable {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables the sending of Loop Protect traps. Default is disabled.

Defaults

None.

Mode

All command modes.

Usage

Loop Protect traps are sent when a Loop Protect event occurs, that is, when a port goes to listening due to not receiving BPDUs. The trap indicates port, SID and loop protection status.

Example

This example shows how to enable sending of Loop Protect traps:

```
S Chassis(rw)->set spantree lptrapenable enable
```

show spantree lptrapenable

Use this command to display the current status of Loop Protect event notification.

Syntax

show spantree lptrapenable

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the current Loop Protect event notification status:

```
S Chassis(rw)->show spantree lptrapenable
LoopProtect event traps are enabled
```

clear spantree lptrapenable

Use this command to return the Loop Protect event notification state to its default state of disabled.

Syntax

clear spantree lptrapenable

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the Loop Protect event notification state to the default of disabled:

```
S Chassis(rw)->clear spantree lptrapenable
```

set spantree disputedbpduthreshold

Use this command to set the disputed BPDU threshold, which is the number of disputed BPDUs that must be received on a given port/SID until a disputed BPDU trap is sent.

Syntax

set spantree disputedbpduthreshold *value*

Parameters

value	Specifies the number of disputed BPDUs that must be received on a given port/SID to cause a disputed BPDU trap to be sent. A threshold of 0 indicates that traps should not be sent. The default value is 0.

Defaults

None.

Mode

All command modes.

Usage

A disputed BPDU is one in which the flags field indicates a designated role and learning, and the priority vector is worse than that already held by the port. If a disputed BPDU is received the port is forced to the listening state. Refer to the 802.1Q-2005 standard, *IEEE Standard for Local and Metropolitan Area Networks – Virtual Bridged Local Area Networks,* for a full description of the dispute mechanism, which prevents looping in cases of one-way communication.

The disputed BPDU threshold is an integer variable that represents the number of disputed BPDUs that must be received on a given port/SID until a disputed BPDU trap is sent and a syslog message is issued. For example, if the threshold is 10, then a trap is issued when 10, 20, 30, and so on, disputed BPDUs have been received.

If the value is 0, traps are not sent. The trap indicates port, SID and total Disputed BPDU count. The default is 0.

Example

This example shows how to set the disputed BPDU threshold value to 5:

```
S Chassis(rw)->set spantree disputedbpduthreshold 5
```

show spantree disputedbpduthreshold

Use this command to display the current value of the disputed BPDU threshold.

Syntax

show spantree disputedbpduthreshold

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the current disputed BPDU threshold:

```
S Chassis(rw)->show spantree disputedbpduthreshold
Disputed BPDU threshold is set to 0
```

clear spantree disputedbpduthreshold

Use this command to return the disputed BPDU threshold to its default value of 0, meaning that disputed BPDU traps should not be sent.

Syntax

clear spantree disputedbpduthreshold

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the disputed BPDU threshold to the default of 0:

```
S Chassis(rw)->clear spantree disputedbpduthreshold
```

show spantree nonforwardingreason

Use this command to display the reason for placing a port in a non-forwarding state due to an exceptional condition.

Syntax

show spantree nonforwardingreason [**port** *port-string*] [**sid** *sid*]

Parameters

port-string	(Optional) Specifies port(s) for which to display the non-forwarding reason. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
sid *sid*	(Optional) Specifies the specific Spanning Tree(s) for which to display the non-forwarding reason. Valid values are **0** - **4094**. If not specified, SID 0 is assumed.

Defaults

If no *port-string* is specified, non-forwarding reason is displayed for all ports.

If no SID is specified, SID 0 is assumed.

Mode

All command modes.

Usage

Exceptional conditions causing a port to be placed in listening or blocking state include a Loop Protect event, receipt of disputed BPDUs, and loopback detection.

Example

This example shows how to display the non-forwarding reason on ge.1.1:

```
S Chassis(rw)->show spantree nonforwardingreason port ge.1.1

Port ge.1.1 has not been placed in a non-forwarding state on SID 0 due to any
exceptional condition.
```

38

Shortest Path Bridging (SPB) Commands

This chapter describes the Shortest Path Bridging (SPB) set of commands and how to use them. For information about configuring 802.1aq, refer to the "Shortest Path Bridging (SPB) Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show spb	38-1
set spb status	38-2
show spb basevid	38-3
show spb dynamic-ect-alg	38-4
set spb basevid	38-5
clear spb basevid	38-6
show spb port	38-6
set spb port status	38-7
clear spb port	38-8
set spb system	38-8
clear spb system	38-9
show spb neighbors	38-10
set spantree version spt	38-10
clear spantree version	38-11

show spb

Use this command to display SPB configuration information.

Syntax

```
show spb
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to display SPB information for this device:

```
S Chassis(rw)->show spb
Status           : Enabled
System ID        : 001f.459f.00d7
System Name      : 001f.459f.00d7
Area ID          : 00.00.00
Net              : 00.0000.001f.459f.00d7.00
Priority         : 0
SPB VLAN Mode    : Auto
Digest Conv.     : loopFreeBoth
SPVIDs           : 3001-4000
  Total          : 1000
  In Use         : 460
AgreeDigest
  Convention Id  : loopFreeBoth
  Convention Cap : off, loopFreeBoth, loopFreeMcastOnly
  Edge Count     : 36
  Digest         : 00:00:00:11:e9:aa:db:ad:2e:c2:63:4f:ea:0b:37:0b:7b:b2:34:c0
Mcid
  Name           : spb
  Revision       : 0
  Digest         : fa:28:b3:1c:37:11:fe:14:2f:13:9c:95:6c:5d:f7:3e
AuxMcid
  Name           : spb
  Revision       : 0
  Digest         : fa:28:b3:1c:37:11:fe:14:2f:13:9c:95:6c:5d:f7:3e
S Chassis(rw)->
```

set spb status

Use this command to set the SPB administrative status for the system.

Syntax

set spb status {**enable** | **disable**}

Parameters

enable | **disable**	Specifies the SPB administrative status for the system. Defaults to **enable**.

Defaults

SPB defaults to enabled.

Mode

All command modes.

Usage

Use this command to globally enable or disable SPB on the system. SPB is administratively enabled by default but is not operational until the Spanning Tree version is set to SPT using "set spantree version spt" on page 38-10. Spanning Tree defaults to version MSTP.

Examples

This example shows how to administratively disable SPB on the system:

```
S Chassis(rw)->set spb status disable
S Chassis(rw)->
```

show spb basevid

Use this command to display SPB Base-VID configuration.

Syntax

show spb basevid [*baseVid*]

Parameters

baseVid	(Optional) Specifies a specific Base-VID configuration to display. Defaults to all Base-VIDs.

Defaults

All Base-VID configurations display.

Mode

All command modes.

Examples

This example shows how to display:

```
S Chassis(rw)->show spb basevid
                       SPVID
VLAN Algorithm    Actual Cfg  Mode Ingress Remote InDiscard
---- ------------ ------ ---- ---- ------- ------ ---------
50   ieee-1       3553   None spbv yes     yes    0
93   ieee-1       None   None spbv no      yes    0
100  ieee-10      3539   None spbv yes     yes    0
101  ieee-1       3006   None spbv yes     yes    0
102  ieee-2       3900   None spbv yes     yes    0
1001 ieee-2       3834   None spbv yes     yes    0
```

```
1002 ieee-3       3557   None spbv yes     yes    0
1003 ieee-4       3124   None spbv yes     yes    0
1004 ieee-5       3418   None spbv yes     yes    0
1005 ieee-6       3768   None spbv yes     yes    0
1006 ieee-7       3584   None spbv yes     yes    0
1007 ieee-8       3655   None spbv yes     yes    0
S Chassis(rw)->
```

show spb dynamic-ect-alg

Use this command to display the SPB ECT algorithms advertised by the network.

Syntax

show spb dynamic-ect-alg [**basevid** *baseVid*] [**system-id** *system-id*]

Parameters

basevid *baseVid*	(Optional) Displays SPB ECT algorithms advertised by the network associated with the specified Base-VID.
system-id *system-id*	(Optional) Displays SPB ECT algorithms advertised by network associated with the specified SPB system MAC address. Valid formats are *xx-xx-xx-xx-xx-xx*, *xx:xx:xx:xx:xx:xx*, or *xxxx.xxxx.xxxx*.

Defaults

All SPB ECT algorithms advertised by network display.

Mode

All command modes.

Examples

This example shows how to display SPB ECT algorithms advertised by network for Base-VID **50**:

```
S Chassis(rw)->show spb dynamic-ect-alg basevid 50
System-Id      BaseVID Algorithm    Mode Alloc  SPVID Ingress
-------------- ------- ------------ ---- ------ ----- -------
0011.88fe.529a 50      ieee-1       spbv auto   3757  yes
0011.88fe.52aa 50      ieee-1       none auto         no
001f.4562.98ee 50      ieee-1       spbv auto   3809  yes
001f.459b.e1e2 50      ieee-1       none auto         no
001f.459f.00d7 50      ieee-1       spbv auto   3553  yes
20b3.9955.9129 50      ieee-1       spbv auto   3087  yes
20b3.9955.9dff 50      ieee-1       spbv auto   3869  yes
20b3.9957.3f7c 50      ieee-1       none auto         no
20b3.99ad.a490 50      ieee-1       none auto         no
20b3.99ad.a8e5 50      ieee-1       spbv auto   3340  yes
S Chassis(rw)->
```

set spb basevid

Use this command to configure an ECT algorithm and shortest path VID to a Base-VID.

Syntax

set spb basevid *baseVid* **ect-alg ieee** *ect-alg* [**spvid** *spVid*]

Parameters

baseVid	Specifies the Base-VID to configure to the ECT algorithm.
ect-alg ieee *ect-alg*	(Optional) Specifies one of sixteen symmetric ECT algorithms defined in the IEEE 802.1Qaq standard. Valid values are **1** - **16**. Default value is **1**.
spvid *spVid*	(Optional) Specifies the shortest path VID (SPVID) assigned to this Base-VID. Valid values are **1** - **4094**. Defaults to dynamically selected when in auto mode.

Defaults

- The symmetric ECT algorithm defaults to 1.
- The SPVID defaults to 0 (unassigned).

Mode

All command modes.

Usage

It is likely that there will be more than one shortest path between two SPB bridges. Commonly defined Equal Cost Tree (ECT) algorithms are used to select a path among available equal cost paths. The IEEE 802.1Qaq standard defines 16 ECT algorithms.

A single ECT algorithm is assigned to a Base-VID. The combination of Base-VID and configured ECT algorithm is used to make forwarding decisions. If you do not specify the ECT algorithm when entering this command, the ECT algorithm defaults to **1**.

The IS-IS Hello PDU carries the mapping between the Base-VID and the ECT algorithm between SPB adjacencies. Information transmitted in the IS-IS Hello PDU ensures that the adjacent SPB bridges use the same ECT algorithm for a given Base-VID. An SPB adjacency is not formed if the mapping does not agree.

Each ECT is assigned a unique shortest path VID (SPVID) for the Base-VID. The ECT to shortest path VID mapping can be administratively assigned using this command. To administratively assign the SPVID, SPB mode must be set to manual using "set spb system" on page 38-8. VLAN mode defaults to auto. When in auto mode, SPVIDs are dynamically assigned. Regardless of the SPB VLAN mode configured, SPVIDs are reserved in a VLAN pool configured using "set spb system" on page 38-8.

Examples

This example shows how to set the ECT algorithm to **2** for Base-VID **100** and the shortest path VID for this mapping to **1000** (this configuration assumes that VLAN 1000 belongs to the SPB VLAN pool and the SPB VLAN mode is set to **manual**):

```
S Chassis(rw)->set spb basevid 100 ect-alg ieee 2 spvid 1000
S Chassis(rw)->
```

clear spb basevid

Use this command to clear an ECT algorithm and shortest path VID from a Base-VID configuration.

Syntax

clear spb basevid *baseVid* [**ect-alg**] [**spvid**]

Parameters

baseVid	Specifies the Base-VID of the ECT algorithm from the Base-VID configuration to clear. Valid values are **1** - **4094**.
ect-alg	(Optional) Clears the ECT algorithm configuration.
spvid	(Optional) Specifies to only clear the shortest path VID from the specified Base-VID.

Defaults

If **spvid** is not specified, the ECT algorithm from the specified Base-VID configuration is cleared.

Mode

All command modes.

Examples

This example shows how to clear the Base-VID 1 to ECT algorithm configuration:

```
S Chassis(rw)->clear spb basevid 1 ect-alg
S Chassis(rw)->
```

This example shows how to clear the SPVID assignment for the Base-VID 1 to ECT algorithm configuration:

```
S Chassis(rw)->clear spb basevid 1 ect-alg spvid
S Chassis(rw)->
```

show spb port

Use this command to display SPB metrics and status on a per port basis.

Syntax

show spb port [*port-string*] [**-interesting**]

Parameters

port-string	Specifies the port string of the port to display.
-interesting	Displays only SPB ports with an UP status.

Defaults

- If *port-string* is not specified, SPB status for all ports display.
- If **-interesting** is not specified, ports for the specified context display regardless of status.

Mode

All command modes.

Examples

This example shows how to display SPB ports that are currently up:

```
S Chassis(rw)->show spb port -interesting
Port      Metric   Status
--------------------------
ge.1.1    20000    up
tg.1.4    2000     up
S Chassis(rw)->
```

Table 38-1 show spb port Output Display

Output...	What it displays...
Port	Specifies the port for this line of SPB stats.
Metric	Specifies the admin path cost of this link as set in spanning tree using "set spantree adminpathcost" on page 36-11.
Status	Specifies whether the port status as up or down.

set spb port status

Use this command to enable SPB on a port.

Syntax

set spb port *port-string* **status** {**enable** | **disable**}

Parameters

port-string	Specifies the port to SPB enable or disable.
enable | **disable**	Enable or disable SPB on the specified port.

Defaults

SPB is disabled on ports by default.

Mode

All command modes.

Usage

Disabling SPB on a port removes the SPB configuration from that port. You can also use "clear spb port" on page 38-8 to remove SPB configuration from the port.

Examples

This example shows how to enable SPB on ports **ge.1.1** through **ge.1.5**:

```
S Chassis(rw)->set spb port ge.1.1-5 enable
S Chassis(rw)->
```

clear spb port

Use this command to clear SPB configuration on the port.

Syntax

clear spb port *port-string*

Parameters

port-string	Specifies the port to clear for SPB configuration.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to clear SPB configuration on ports **ge.1.1** and **ge.1.2**:

```
S Chassis(rw)->clear spb port ge.1.1-2
S Chassis(rw)->
```

set spb system

Use this command to configure SPB system parameters.

Syntax

set spb system [**area-address** *isis-area*] [**digest-convention** {**off** | **loopfreeboth**}] [**mode-vlan** {**auto** | **manual**}]

Parameters

area-address *isis-area*	(Optional) Specify an IS-IS area address using a format *xx.xx.xx*. Defaults to **00.00.00**.
digest-convention	Configure the SPB agreement digest convention.
off	Disables agreement digest checking in Hellos
loopfreeboth	Blocks unsafe traffic on digest disagreement.
vlan-mode	Configure the VLAN mode.
auto	Specifies that the mapping of Base-VID to SPVID is dynamically handled. SPB VLAN mode defaults to **auto**.
manual	Specifies that the mapping of Base-VID to SPVID is administratively configured.

Defaults

The IS-IS area address defaults to **00.00.00**.

The digest convention defaults to loop protection using **loopfreeboth**.

The SPB VLAN mode defaults to **auto**.

Mode

All command modes.

Usage

You can use this command to optionally set an IS-IS area address for this system.

The digest convention used can be set to off or to block unsafe traffic on digest disagreement.

The SPB VLAN mode determines whether Base-VID to SPVID mapping will be dynamically or manually configured. SPB VLAN mode defaults to dynamic configuration (**auto**). The SPVID is selected from a pool of VLANs configured using "set spantree mstmap" on page 35-13. If manual configuration is selected, use option **spvid** to manually configure the Base-VID to SPVID mapping.

Examples

This example shows how to set an IS-IS area address for this node to 01.01.01:

```
S Chassis(rw)->set spb system area-address 01.01.01
S Chassis(rw)->
```

This example shows how to set the SPB VLAN mode to manual:

```
S Chassis(rw)->set spb system mode-vlan manual
S Chassis(rw)->
```

This example shows how to disable the SPB agreement digest convention for this node:

```
S Chassis(rw)->set spb system digest-convention off
S Chassis(rw)->
```

clear spb system

Use this command to reset or delete SPB system configuration.

Syntax

clear spb system [**area-address**] [**digest-convention**] [**mode-vlan**] [**system-id**]

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage.

This example shows how to reset the SPB VLAN mode to dynamically map the Base-VID to SPVID:

```
S Chassis(rw)->clear spb system mode-vlan
S Chassis(rw)->
```

show spb neighbors

Use this command to display SPB neighbor information.

Syntax

show spb neighbors [**port** *port-string*] [**system-id** *mac-address*] [**-verbose**]

Parameters

port *port-string*	Displays SPB neighbors for the specified port(s).
system-id *mac-address*	Displays SPB neighbor information located on the specified system MAC address.
-verbose	Displays a detailed level of information for this system's SPB neighbors.

Defaults

If no options are specified, information for all SPB neighbors displays.

Mode

All command modes.

Examples

This example shows how to display all SPB neighbors for this system:

```
S Chassis(rw)->show spb neighbors
System-Id      Port    State Name
-----------------------------------------------------------------
20b3.99ad.a4d2 ge.1.1  Up    20-b3-99-ad-a4-d2
0011.88fe.52aa tg.1.4  Up    00-11-88-fe-52-aa
S Chassis(rw)->
```

Table 38-2 provides an explanation of the command output.

Table 38-2 show spb neighbors Output Details

Output...	What it displays...
System-Id	Specifies the neighbor system ID.
Port	Specifies the port connected to this neighbor.
State	Specifies the neighbor state
Name	Specifies the neighbor name.

set spantree version spt

Use this command to set the version of the Spanning Tree protocol to Version 4.

Syntax

set spantree version spt

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

Spanning Tree defaults to MSTP (version 3). The SPT Spanning Tree version 4 sends version 4 BPDUs and is required for SPB to be operational.

Example

This example shows how to globally change the Spanning Tree version from the default of MSTP to SPT:

```
S Chassis(rw)->set spantree version spt
```

clear spantree version

Use this command to reset the Spanning Tree version to MSTP mode.

Syntax

clear spantree version

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the Spanning Tree version to the default version (MSTP):

```
S Chassis(rw)->clear spantree version
```

39

Routing as a Service (RaaS) Commands

This chapter describes the Routing as a Service (RaaS) set of commands and how to use them. For information about configuring RaaS, refer to the "Routing as a Service RaaS" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show raas	39-1
raas	39-2
vrrp fabric-route-mode helper-router	39-3

show raas

Use this command to display RaaS router configuration information.

Syntax

show raas

Parameters

None.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to display RaaS configuration details:

```
S Chassis(rw)->show raas
RaaS is not enabled
--------------------------
Learned Routers
--------------------------

Address        SYSID                Age
----------     -----------------    ----------------------
```

```
10.1.255.1      00-00-0A-01-FF-01   1d03h11m46s
10.1.255.2      00-00-0A-01-FF-02   1d03h11m46s
10.1.255.3      00-00-0A-01-FF-03   1d03h11m46s
```

Table 39-1 provides an explanation of the **show raas** command output.

Table 39-1 show raas Output Display

Output...	What it displays...
Address	Displays the IP address of the learned router.
SYSID	Displays the router system ID.
Age	Displays the length of time the router has been active.

raas

Use this command to configure a main router capable in an RaaS context.

Syntax

raas *router-id*

Parameters

router-id	Specifies an ID unique to this router in an IPv4 quad address format (*x.x.x.x*).

Defaults

None.

Mode

Global router configuration mode.

Usage

An RaaS Main Router is a standard L3 router within the SPB network that is configured for VRRP and is used to forward all packets external to the directly connected Helper Router VLANs. This command configures this router as Main router capable within an SPB network for purposes of Routing as a Service (RaaS).

Examples

This example shows how to configure the SPB main router capability router ID to 1.1.1.1 for this router:

```
S Chassis(rw)->
S Chassis(rw)->configure
S Chassis(rw-config)->raas 1.1.1.1
```

vrrp fabric-route-mode helper-router

Enables this VRRP router as a Helper router in an RaaS context.

Syntax

vrrp fabric-route-mode *vrid* **helper-router**

no vrrp fabric-route-mode *vrid* **helper-router**

Parameters

vrid	Specifies the VRRP instance for this fabric route mode configuration.

Defaults

Fabric route mode is disabled.

Mode

Interface configuration mode.

Usage

The Helper router is enabled under VRRP per VRID per VLAN interface on access SPB switches that ingress to customer VLANs in an RaaS context. Helper router route tables confine routes to connected VLAN interfaces where an interface represents a customer VLAN. The Helper router learns the identity of Main routers by the propagation of type 250 TLV through the SPB network by IS-IS. Helper routers redirect unresolved destination networks to the Main routers.

The Main router responds to ARP requests for any virtual IP address and sends VRRP advertisements to ensure the virtual MAC remains in bridge FDBs within the SPB domain. Helper routers install the VRRP virtual MAC address into the local filter database for packet processing by the forwarding plane.

The “no” form of this command disables the Helper router function on this router.

Example

This example enables fabric route mode on the VRRP backup router on VRID **1**:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 20
S Chassis(rw)-config-intf-vlan.0.20)->vrrp fabric-route-mode 1 helper-router
S Chassis(rw)-config-intf-vlan.0.20)->
```

40

802.1Q VLAN Commands

The commands in this chapter describe how to:

- Create, enable, disable, and name a VLAN.
- Review status and other information related to VLANs.
- Assign ports to a VLAN and filter unwanted frames on one or more ports
- Assign a VLAN to a MIB-II interface in order to view statistics for the VLAN.
- Set VLAN constraints in order to control the filtering database to which VLANs are allowed to belong.
- Set a bridge mode for Layer 2 tunneling of VLANs through a service provider network (provider bridging).

For information about configuring 802.1Q VLANs, refer to the "VLAN Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

Note: The S-Series device can support up to 4094 802.1Q VLANs. The allowable range for VLANs is 2 to 4094. As a default, all ports on the device are assigned to VLAN ID 1, untagged.

For information about...	Refer to page...
Reviewing Existing VLANs	40-1
Creating and Naming Static VLANs	40-3
Assigning Port VLAN IDs (PVIDs) and Ingress Filtering	40-5
Configuring the VLAN Egress List	40-18
Provider Bridging Commands	40-22

Reviewing Existing VLANs

This command allows you to display a list of VLANs currently configured on the device, to determine how one or more VLANs were created, the ports allowed and disallowed to transmit traffic belonging to VLAN(s), and if those ports will transmit the traffic with a VLAN tag included.

For information about...	Refer to page...
show vlan	40-2

show vlan

Use this command to display information related to one or more VLANs.

Syntax

show vlan [**static**] [*vlan-list*]

Parameters

static	(Optional) Displays information related to all configured VLANs regardless of status.
vlan-list	(Optional) Displays information for a specific VLAN or range of VLANs.

Defaults

If no options are specified, all information related to active VLANs will be displayed.

Mode

All command modes.

Usage

Static VLANs are manually created using the **set vlan** command (page 40-3), SNMP MIBs, or the WebView management application. The default VLAN, VLAN 1, is always statically configured and cannot be deleted. Only ports that use a specified VLAN as their default VLAN (PVID) will be displayed.

Example

This example shows how to display information for VLAN 1. In this case, VLAN 1 is named "DEFAULT VLAN" and it is enabled to operate. Ports allowed to transmit frames belonging to VLAN 1 are listed as egress ports. Ports that won't include a VLAN tag in their transmitted frames are listed as untagged ports. There are no forbidden ports (prevented from transmitted frames) on VLAN 1:

```
S Chassis(rw)->show vlan 1
VLAN     : 1           Status     : Enabled
FID      : 1           Name       : DEFAULT VLAN
VLAN Type: Permanent   Last change: 2010-05-26 10:20:17
Egress Ports
host.0.1, ge.1.1-10, ge.2.1-4, ge.3.1-7, lag.0.1-32
 Forbidden Egress Ports
None.
 Untagged Ports
host.0.1, ge.1.1-10, ge.2.1-4, ge.3.1-7, lag.0.1-32
```

Table 40-1 provides an explanation of the command output.

Table 40-1 show vlan Output Details

Output...	What it displays...
VLAN	VLAN ID.
NAME	Name assigned to the VLAN.
Status	Whether it is **enabled** or **disabled**.
VLAN Type	Whether it is **permanent** (static) or **dynamic**.
FID	Filter Database ID of which this VLAN is a member.
Creation Time	Time elapsed since the VLAN was created.
Egress Ports	Ports configured to transmit frames for this VLAN.
Forbidden Egress Ports	Ports prevented from transmitted frames for this VLAN.
Untagged Ports	Ports configured to transmit untagged frames for this VLAN.

Creating and Naming Static VLANs

These commands are used to create a new static VLAN, or to enable or disable existing VLAN(s).

For information about...	Refer to page...
set vlan	40-3
set vlan name	40-4
clear vlan	40-4
clear vlan name	40-5

set vlan

Use this command to create a new static IEEE 802.1Q VLAN, or to enable or disable an existing VLAN.

Syntax

```
set vlan {create | enable | disable} vlan-list
```

Parameters

create | **enable** | **disable**	Creates, enables or disables VLAN(s).
vlan-list	Specifies one or more VLAN IDs to be created, enabled or disabled. VLAN IDs can range from 1 to 4094.

Defaults

None.

Mode

All command modes.

Usage

Each VLAN ID must be unique. If a duplicate VLAN ID is entered, the device assumes that the Administrator intends to modify the existing VLAN.

Enter the VLAN ID using a unique number between 2 and 4094. The VLAN IDs of 0, 1, and 4095 and higher may not be used for user-defined VLANs. See "VLAN Support on Extreme Networks S-Series Switches section of the *Extreme Networks S-Series Configuration Guide* for further VLAN ID 0, 1, and 4095 information.

Once a VLAN is created, you can assign it a name using the **set vlan name** command described in "set vlan name" on page 40-4.

Examples

This example shows how to create VLAN 3:

```
S Chassis(rw)->set vlan create 3
```

This example shows how to disable VLAN 3:

```
S Chassis(rw)->set vlan disable 3
```

set vlan name

Use this command to set or change the ASCII name for a new or existing VLAN.

Syntax

set vlan name *vlan-list vlan-name*

Parameters

vlan-list	Specifies the VLAN ID or a range of VLAN IDs to be named.
vlan-name	Specifies the string used as the name of the VLAN (1 to 32 characters). Diacritical marks are not supported.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the name for VLANs 7-10 to green:

```
S Chassis(rw)->set vlan name 7-10 green
```

clear vlan

Use this command to remove a static VLAN from the list of VLANs recognized by the device.

Syntax

clear vlan *vlan-list*

Parameters

vlan-list	Specifies the VLAN ID of the VLAN(s) to be removed.

Defaults

None.

Mode

All command modes.

Example

This example shows how to remove a static VLAN 9 from the device's VLAN list:

```
S Chassis(rw)->clear vlan 9
```

clear vlan name

Use this command to remove the name of a VLAN from the VLAN list.

Syntax

clear vlan name *vlan-list*

Parameters

vlan-list	Specifies the VLAN ID of the VLAN(s) for which the name will be cleared.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear the name for VLAN 9:

```
S Chassis(rw)->clear vlan name 9
```

Assigning Port VLAN IDs (PVIDs) and Ingress Filtering

These commands are used to assign default VLAN IDs to untagged frames on one or more ports, to configure MIB-II interface mapping to a VLAN, to configure VLAN ingress filtering and constraints, and to set the frame discard mode.

For information about...	Refer to page...
show port vlan	40-6
set port vlan	40-8
clear port vlan	40-9

For information about...	Refer to page...
show vlan interface	40-9
set vlan interface	40-11
clear vlan interface	40-12
show port ingress filter	40-12
set port ingress filter	40-13
show vlan constraint	40-14
set vlan constraint	40-15
clear vlan constraint	40-16
show port discard	40-16
set port discard	40-17
clear port discard	40-17

show port vlan

Use this command to display port VLAN identifier (PVID) information.

Syntax

show port vlan [*port-string*]

Parameters

port-string	(Optional) Displays PVID information for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port -string* is not specified, port VLAN information for all ports will be displayed.

Mode

All command modes.

Usage

PVID determines the VLAN to which all untagged frames received on one or more ports will be classified.

Example

This example shows how to display PVIDs assigned to ports 1 through 6. In this case, untagged frames received on these ports will be classified to VLAN 1:

```
S Chassis(rw)->show port vlan ge.2.1-6
ge.2.1 is set to 1
ge.2.2 is set to 1
ge.2.3 is set to 1
ge.2.4 is set to 1
```

```
ge.2.5 is set to 1
ge.2.6 is set to 1
```

show vlan portinfo

Use this command to display VLAN information for a port or range of ports.

Syntax

show vlan portinfo [**port** *port-string*] [**vlan** *vlan*]

Parameters

port *port-string*	(Optional) Displays VLAN information for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
vlan *vlan*	(Optional) Displays VLAN information for ports on the specified VLAN(s).

Defaults

If the **port** option is not specified, VLAN information for all ports for the VLAN context will display.

If the **vlan** option is not specified, VLAN information for all VLANs for the specified port context will display.

Mode

All command modes.

Examples

This example shows how to display VLAN information for all ports on all VLANs:

```
S Chassis(rw)->show vlan portinfo

            Port  Ingress   VLAN        Egress
Port        VLAN  Filter    Type        VLAN
----------  ----  --------  ----------  ----------
host.0.1    1     false     forwarding
tagged:1,100,200,300,400,500,700,800,900,1000,1111,2500
ge.1.1      1     false     static      untagged:1
ge.1.2      1     false     static      untagged:1
                            forwarding  untagged:1
ge.1.3      1     false     static      untagged:1
ge.1.4      1     false     static      untagged:1
.
.
.
lag.0.59    1     false     static      untagged:1
lag.0.60    1     false     static      untagged:1
lag.0.61    1     false     static      untagged:1
```

```
lag.0.62    1     false     static      untagged:1
S Chassis(rw)->
```

This example shows how to display VLAN information for port ge.1.2 on VLAN 1:

```
S Chassis(rw)->show vlan portinfo port ge.1.2 vlan 1

            Port  Ingress   VLAN        Egress
Port        VLAN  Filter    Type        VLAN
----------  ----  --------  ----------  ----------
ge.1.2      1     false     static      untagged:1
                            forwarding  untagged:1
S Chassis(rw)->
```

set port vlan

Use this command to configure the PVID (port VLAN identifier) for one or more ports.

Syntax

set port vlan *port-string pvid* [**modify-egress** | **no-modify-egress**]

Parameters

port-string	Specifies the port(s) for which to configure a VLAN identifier. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
pvid	Specifies the VLAN ID of the VLAN to which port(s) will be added.
modify-egress | **no-modify-egress**	(Optional) Adds port(s) to VLAN's untagged egress list and removes them from other untagged egress lists, or does not prompt for or make egress list changes

Defaults

If not specified, the egress list will be modified.

Mode

All command modes.

Usage

For information on how to configure protocol-based policy classification to a VLAN, including how to configure a VLAN policy to override PVID, refer to the *Extreme Networks S-Series Configuration Guide*.

The PVID is used to classify untagged frames as they ingress into a given port. It will prompt the user to add the VLAN to the port's egress list as untagged, and remove the default VLAN from the port's egress list. If the user chooses to modify the egress of the VLAN, and the specified VLAN has not already been created, this command will create it.

Example

This example shows how to add ge.1.10 to the port VLAN list of VLAN 4 (PVID 4). Since VLAN 4 is a new VLAN, it is created. Then port ge.1.10 is added to VLAN 4's untagged egress list, and is cleared from the egress list of VLAN 1 (the default VLAN):

```
S Chassis(rw)->set vlan 4 create
S Chassis(rw)->set port vlan ge.1.10 4 modify-egress
S Chassis(rw)->
```

If modify-egress is not used, the following command allows for manually adding ge.1.10 to the VLAN 4 untagged egress list and remove ge.1.10 from the VLAN 1 untagged egress list:

```
S Chassis(rw)->set vlan egress 4 ge.1.10 untagged
S Chassis(rw)->clear vlan egress 1 ge.1.10
```

clear port vlan

Use this command to reset a port's 802.1Q port VLAN ID (PVID) to the host VLAN ID 1.

Syntax

clear port vlan *port-string*

Parameters

port-string	Specifies the port(s) to be reset to the host VLAN ID 1. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset ports 3 and 11 to a VLAN ID of 1 (Host VLAN):

```
S Chassis(rw)->clear port vlan ge.1.3,ge.1.11
```

show vlan interface

Use this command to display one or more VTAP interface MIB-II entries mapped to a VLAN.

Syntax

show vlan interface [*vlan-list*]

Parameters

vlan-list	(Optional) Displays the VTAP interface entry for specified VLAN(s).

Defaults

If *vlan-list* is not specified, VTAP interface entries will be displayed for all VLANs.

Mode

All command modes.

Usage

A VTAP interface provides the data source input of a port mirror or SMON statistics collection. A VLAN will not have a MIB-II ifIndex if a VTAP interface does not exist for it. See "set vlan interface" on page 40-11 for information on creating a VTAP interface.

Example

This example shows how to display the VLAN MIB-II interface entries for this device:

```
S Chassis(rw)->show vlan interface
VLAN MIB-II Interfaces

Max Interfaces     : 16
Current Interfaces : 12


VLAN       Port          Storage Type

-------------------------------------
  1      vtap.0.1        non-volatile
  300    vtap.0.300      non-volatile
  301    vtap.0.301      non-volatile
  302    vtap.0.302      non-volatile
  303    vtap.0.303      non-volatile
  304    vtap.0.304      non-volatile
  305    vtap.0.305      non-volatile
  306    vtap.0.306      non-volatile
  307    vtap.0.307      non-volatile
  308    vtap.0.308      non-volatile
  309    vtap.0.309      non-volatile
  310    vtap.0.310      non-volatile
S Chassis(rw)->
```

Table 40-2 provides an explanation of the command output.

Table 40-2 show vlan interface Output Details

Output...	What it displays...
Max Interfaces	The maximum number of VTAP interfaces supported on this device.
Current Interfaces	The current number of configured VTAP interfaces.

Table 40-2 show vlan interface Output Details (continued)

Output...	What it displays...
VLAN	VLAN ID.
Port	Port-string designation.
Storage Type	Whether the entry is stored as a **volatile** or **non-volatile** entry. Volatile entries are lost when a system is reset. Non-volatile entries are saved in NVRAM and are persistent until cleared.

set vlan interface

Use this command to create, disable or enables a MIB-II interface mapping to a VLAN.

Syntax

set vlan interface *vlan-list* {**create** | **disable** | **enable**} [**volatile**]

Parameters

vlan-list	Specifies the VLAN(s) for which a MIB-II interface entry will be created, disabled or enabled.
create | **disable** | **enable**	Creates, disables or enables an interface entry.
volatile	(Optional) When the **create** keyword is used, stores the entry as a volatile entry. Volatile entries are lost when a system is reset. Non-volatile entries are saved in NVRAM and are persistent until cleared.

Defaults

If **volatile** is not specified, entries will be created as nonvolatile.

Mode

All command modes.

Usage

This command results in the creation of a VTAP port. A VTAP port provides the data source input of a port mirror or SMON statistics collection. VTAP creation is the mechanism for adding a MIB-II interface table entry for a VLAN. The specified VLAN is assigned a MIB-II ifIndex. A VLAN will not have a MIB-II ifIndex if a VTAP port does not exist for it. You must first create a VTAP port before creating a port mirror.

Example

This example shows how to create a non-volatile MIB-II interface entry mapped to VLAN 1:

```
S Chassis(rw)->set vlan interface 1 create
S Chassis(rw)->show vlan interface 1
VLAN MIB-II Interfaces

Max Interfaces     : 16
Current Interfaces : 1
```

```
VLAN       Port          Storage Type

-------------------------------------
  1      vtap.0.1        non-volatile
S Chassis(rw)->
```

clear vlan interface

Use this command to clear the MIB-II interface entry mapped to a VLAN.

Syntax

clear vlan interface *vlan-list*

Parameters

vlan-list	Specifies the VLAN(s) for which an interface entry will be cleared.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear the interface entry mapped to VLAN 1:

```
S Chassis(rw)->clear vlan interface 1
S Chassis(rw)->show vlan interface
VLAN MIB-II Interfaces

Max Interfaces     : 16
Current Interfaces : 0

VLAN       Port          Storage Type

-------------------------------------
There are no VLANs mapped to a MIB-II interface.
S Chassis(rw)->
```

show port ingress filter

Use this command to show all ports that are enabled for port ingress filtering, which limits incoming VLAN ID frames according to a port VLAN egress list.

Syntax

show port ingress-filter [*port-string*]

Parameters

port-string	(Optional) Specifies the port(s) for which to display ingress filtering status. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, ingress filtering status for all ports will be displayed.

Mode

All command modes.

Usage

If the VLAN ID specified in the received frame is not on the port's VLAN egress list, then that frame is dropped and not forwarded.

Example

This example shows how to display the port ingress filter status for ports 10 through 15. In this case, the ports are disabled for ingress filtering:

```
S Chassis(rw)->show port ingress-filter ge.1.10-15
   Port      State
 --------  ---------
  ge.1.10  disabled
  ge.1.11  disabled
  ge.1.12  disabled
  ge.1.13  disabled
  ge.1.14  disabled
  ge.1.15  disabled
```

set port ingress filter

Use this command to discard all frames received with a VLAN ID that don't match the port's VLAN egress list.

Syntax

set port ingress-filter *port-string* {**disable** | **enable**}

Parameters

port-string	Specifies the port(s) on which to enable of disable ingress filtering. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
disable | **enable**	Disables or enables ingress filtering.

Defaults

None.

Mode

All command modes.

Usage

When ingress filtering is enabled on a port, the VLAN IDs of incoming frames are compared to the port's egress list. If the received VLAN ID does not match a VLAN ID on the port's egress list, then the frame is dropped.

Ingress filtering is implemented according to the IEEE 802.1Q standard.

Example

This example shows how to enable port ingress filtering on port 3:

```
S Chassis(rw)->set port ingress-filter ge.1.3 enable
```

show vlan constraint

Use this command to display constraint settings for one or more VLANs. Constraints determine which VLANs belong to which Filter Databases (FIDs).

Syntax

show vlan constraint [*vlan-list*]

Parameters

vlan-list	(Optional) Displays constraint settings for specific VLAN(s).

Defaults

If *vlan-list* is not specified, settings for all VLANs will be displayed.

Mode

All command modes.

Example

This example shows how to display the constraint settings for VLAN 1:

```
S Chassis(rw)->show vlan constraint 1

VLAN ID VLAN SET        VLAN SET TYPE
   1       100              10   Shared
S Chassis(rw)->
```

Table 40-3 provides an explanation of the command output.

Table 40-3 show vlan constraint Output Details

Output...	What it displays...
VLAN ID	Number identifying the VLAN.
VLAN SET	Constraint set ID.
VLAN SET TYPE	Whether or not this constraint is sharing the same filter database as other VLANs in this set, or is using an independent filtering database.

set vlan constraint

Use this command to apply a constraint to a VLAN.

Syntax

set vlan constraint *vlan-list set-num* [**shared** | **independent**]

Parameters

vlan-list	Specifies the VLAN(s) for which to apply the constraint.
set-num	Specifies a constraint set ID. Valid values are: **1** to **65535**.
shared | **independent**	(Optional) Sets the constraint type as sharing the same filter database as other VLANs in this set, or as using an independent filtering database.

Defaults

If not specified, the VLAN constraint will be set to independent.

Mode

All command modes.

Usage

VLAN learning takes place based upon the contents of the VLAN filtering database. There are two types of databases:

- **Independent Virtual Local Area Network (VLAN) Learning (IVL)**: Each VLAN uses its own filtering database. Transparent source address learning performed as a result of incoming VLAN traffic is not made available to any other VLAN for forwarding purposes. This setting is useful for handling devices (such as servers) with NICs that share a common MAC address. One FID is assigned per VLAN. The FID value is the same as the VID it is assigned to. This is the default mode on Extreme Networks switches.
- **Shared Virtual Local Area Network (VLAN) Learning (SVL)**: Two or more VLANs are grouped to share common source address information. This setting is useful for configuring more complex VLAN traffic patterns, without forcing the switch to flood the unicast traffic in each direction. This allows VLANs to share addressing information. It enables ports or switches in different VLANs to communicate with each other (when their individual ports are configured to allow this to occur). One FID is used by two or more VLANs. The FID value defaults to the lowest VID in the filtering database.

See "Appendix F" of the *IEEE Std 802.1Q™2011* standard for a detailed discussion of shared and independent VLAN learning modes and when it is appropriate to use the shared mode.

Example

This example shows how to apply a constraint **1** to VLANs **1**, **2**, and **3** using a shared filtering database:

```
S Chassis(rw)->set vlan constraint 1-3 1 shared
```

clear vlan constraint

Use this command to clear a constraint applied to a VLAN.

Syntax

clear vlan constraint *vlan-list set-num*

Parameters

vlan-list	Specifies the VLAN(s) for which to clear the constraint.
set-num	Specifies the constraint set ID to be cleared.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear constraint 3 from VLAN 1:

```
S Chassis(rw)->clear vlan constraint 1 3
```

show port discard

Use this command to display the frame discard mode for one or more ports.

Syntax

show port discard [*port-string*]

Parameters

port-string	(Optional) Displays the frame discard mode for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, frame discarded mode will be displayed for all ports.

Mode

All command modes.

Usage

Ports can be set to discard frames based on whether or not they contain a VLAN tag. They can also be set to discard both frame types or none of the frames received.

Example

This example shows how to display the frame discard mode for port 7. In this case, the port has been set to discard all tagged frames:

```
S Chassis(rw)->show port discard ge.2.7
 Port         Discard Mode
------------  -------------
 ge.2.7         tagged
```

set port discard

Use this command to set the frame discard mode on one or more ports.

Syntax

set port discard *port-string* {**tagged** | **untagged** | **none** | **both**}

Parameters

port-string	Specifies the port(s) for which to set frame discard mode. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
tagged | **untagged** | **none** | **both**	Sets the port(s) to discard tagged or untagged frames, no frames, or both types of frames.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set port 7 to discard both tagged and untagged frames:

```
S Chassis(rw)->set port discard ge.2.7 both
```

clear port discard

Use this command to reset the frame discard mode to the factory default setting (none).

Syntax

clear port discard *port-string*

Parameters

port-string	Specifies the port(s) for which to reset frame discard mode. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset port 7 to the default discard mode of "none":

```
S Chassis(rw)->clear port discard ge.2.7
```

Configuring the VLAN Egress List

The commands in this section are used to assign or remove ports on the egress list of a particular VLAN. This determines which ports will be eligible to transmit frames for a particular VLAN. For example, ports 1, 5, 9, 8 could be assigned to transmit frames belonging to VLAN 5 (VLAN ID=5).

The port egress type for all ports defaults to tagging transmitted frames, but can be changed to forbidden or untagged. In general, VLANs have no egress (except for VLAN 1) until they are configured by static administration, or through dynamic mechanisms (such as GVRP, policy classification, or Extreme Networks dynamic egress).

Setting a port to forbidden prevents it from participating in the specified VLAN and ensures that any dynamic requests (either through GVRP or dynamic egress) for the port to join the VLAN will be ignored. Setting a port to untagged allows it to transmit frames without a tag header. This setting is usually used to configure a port connected to an end user device.

The default VLAN defaults its egress to untagged for all ports.

For information about...	Refer to page...
show port egress	40-18
set vlan egress	40-19
clear vlan egress	40-20
show vlan dynamicegress	40-21
set vlan dynamicegress	40-21

show port egress

Use this command to display the VLAN membership for one or more ports.

Syntax

show port egress [*port-string*]

Parameters

port-string	(Optional) Displays VLAN membership for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, VLAN membership will be displayed for all ports.

Mode

All command modes.

Example

This example shows you how to show VLAN egress information for ports 1 through 3. In this case, all three ports are allowed to transmit VLAN 1 frames as tagged and VLAN 10 frames as untagged. Both are static VLANs:

```
S Chassis(rw)->show port egress ge.1.1-3
 Port      Vlan           Egress     Registration
Number      Id            Status       Status
-------------------------------------------------------
ge.1.1       1            tagged       static
ge.1.1      10          untagged      static
ge.1.2       1            tagged       static
ge.1.2      10          untagged      static
ge.1.3       1            tagged       static
ge.1.3      10          untagged      static
```

set vlan egress

Use this command to add ports to the VLAN egress list for the device, or to prevent one or more ports from participating in a VLAN. This determines which ports will transmit frames for a particular VLAN.

Syntax

set vlan egress *vlan-list port-string* [**untagged** | **forbidden** | **tagged**]

Parameters

vlan-list	Specifies the VLAN where a port(s) will be added to the egress list.
port-string	Specifies one or more ports to add to the VLAN egress list of the specified *vlan-list*. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
untagged	(Optional) Adds the specified port(s) as untagged which causes the port(s) to transmit frames without an IEEE 802.1Q header tag.
forbidden	(Optional) Adds the specified port(s) as forbidden, which instructs the device to ignore dynamic requests (either through GVRP or dynamic egress) from the port(s) to join the VLAN and disallows egress on that port.

tagged	(Optional) Adds the specified port(s) as tagged, which causes the port(s) to transmit 802.1Q tagged frames.

Defaults

If **untagged, forbidden** or **tagged** is not specified, the port will be added to the VLAN egress list as tagged.

Mode

All command modes.

Examples

This example shows how to add ports 5 through 10 to the egress list of VLAN 7. This means that these ports will transmit VLAN 7 frames as tagged:

```
S Chassis(rw)->set vlan egress 7 ge.1.5-10
```

This example shows how to forbid ports 13 through 15 from joining VLAN 7 and disallow egress on those ports:

```
S Chassis(rw)->set vlan egress 7 ge.1.13-15 forbidden
```

This example shows how to allow port 2 to transmit VLAN 7 frames as untagged:

```
S Chassis(rw)->set vlan egress 7 ge.1.2 untagged
```

clear vlan egress

Use this command to remove ports from a VLAN's egress list.

Syntax

clear vlan egress *vlan-list port-string* [**forbidden**]

Parameters

vlan-list	Specifies the number of the VLAN from which a port(s) will be removed from the egress list.
port-string	Specifies one or more ports to be removed from the VLAN egress list of the specified *vlan-list*. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
forbidden	(Optional) Clears the forbidden setting from the specified port(s) and resets the port(s) as able to egress frames if so configured by either static or dynamic means.

Defaults

If **forbidden** is not specified, tagged and untagged settings will be cleared.

Mode

All command modes.

Examples

This example shows how to remove port 14 from the egress list of VLAN 9:

```
S Chassis(rw)->clear vlan egress 9 ge.3.14
```

This example shows how to remove all ports in slot 2 from the egress list of VLAN 4:

```
S Chassis(rw)->clear vlan egress 4 ge.2.*
```

show vlan dynamicegress

Use this command to display which VLANs are currently enabled for VLAN dynamic egress.

Syntax

show vlan dynamicegress [*vlan-list*]

Parameters

vlan-list	(Optional) Displays dynamic egress status for specific VLAN(s).

Defaults

If *vlan-list* is not specified, status for all VLANs where dynamic egress is enabled will be displayed.

Mode

All command modes.

Example

This example shows how to display which VLANs are enabled for dynamic egress:

```
S Chassis(rw)->show vlan dynamicegress
VLAN 1 is enabled
VLAN 101 is enabled
VLAN 102 is enabled
VLAN 105 is enabled
```

set vlan dynamicegress

Use this command to set the administrative status of one or more VLANs' dynamic egress capability. If VLAN dynamic egress is enabled, the device will add the port receiving a tagged frame to the VLAN egress list of the port according to the frame VLAN ID.

Syntax

set vlan dynamicegress *vlan-list* {**enable** | **disable**}

Parameters

vlan-list	Specifies the number of the VLAN(s) where dynamic egress will be enabled or disabled.
enable | **disable**	Enables or disables dynamic egress.

Defaults

None.

Mode

All command modes.

Example

This example shows how to enable the dynamic egress function on VLAN 7:

```
S Chassis(rw)->set vlan dynamicegress 7 enable
```

Provider Bridging Commands

The commands in this section are used by service providers to set the bridge mode for setting up tunnels through their network to pass through external customer traffic from a provider network ingress port to a provider network egress port. The provider can assign a single VLAN through their network for all customer traffic egressing through a set port, instead of having to create and manage a separate VLAN for each customer VLAN.

The commands specific to this feature set the bridge mode and show the current bridge mode. All other commands for configuring this feature are VLAN commands described elsewhere in this chapter. For a description of the Provider Bridging feature and its configuration, refer to the "VLAN Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
set bridge mode	40-22
show bridge mode	40-23

set bridge mode

Use this command to change the mode of the switch for bridging of customer traffic through a provider network.

Syntax

set bridge mode {**customer-bridge** | **provider-bridge**}

Parameters

customer-bridge	The default mode of bridging and routing external C-VLANs via C-TAGs.
provider-bridge	Provider bridge mode enables tunneling in the provider network by adding S-TAGs to C-VLANs and transporting them as dedicated service VLANs.

Defaults

Customer-bridge mode is the default bridge mode.

Mode

All command modes.

Usage

To clear provider bridge mode, run this command with the customer-bridge option.

Examples

This example shows how to set the bridge mode for configuring a tunnel for customer traffic:

```
S Chassis(rw)->set bridge mode provider-bridge
```

This example shows how to clear bridge mode and return to the default bridge mode:

```
S Chassis(rw)->set bridge mode customer-bridge
```

show bridge mode

Use this command to show the mode of the switch for bridging of customer traffic through a provider network.

Syntax

show bridge mode

Parameters

None.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to display the bridge mode:

```
S Chassis(rw)->show bridge mode
Current bridge operation mode setting: Customer Bridge
```

41

GVRP Commands

The commands in this chapter are used to enable or disable the GARP VLAN Registration Protocol (GVRP), both globally and on an individual port basis, configure the GARP timer values, display the current configuration parameters. By default, GVRP is disabled on all ports, and globally enabled on the device. For information about configuring GVRP, refer to the "VLAN Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show gvrp	41-1
show garp timer	41-2
set gvrp	41-3
clear gvrp	41-4
show gvrp vlan restricted	41-4
set gvrp vlan restricted	41-5
clear gvrp vlan restricted	41-6
set garp timer	41-6
clear garp timer	41-7

show gvrp

Use this command to display GVRP configuration information.

Syntax

show gvrp [*port-string*]

Parameters

port-string	(Optional) Displays GVRP configuration information for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, GVRP configuration information will be displayed for all ports on the device.

Mode

All command modes.

Example

This example shows how to display GVRP status for the device and for port 1 in slot 2:

```
S Chassis(rw)->show gvrp ge.2.1
Global GVRP status is enabled.

Port Number    GVRP status    Last PDU Origin
-----------    -----------    -----------------
ge.2.1         enabled        00-e0-63-97-d4-36
```

Table 41-1 provides an explanation of the command output.

Table 41-1 show gvrp Output Details

Output...	What it displays...
Port Number	Port designation. For a detailed description of possible port-string values, refer to the *Extreme Networks S-Series Configuration Guide*.
GVRP status	Whether GVRP is enabled or disabled on the port.
Last PDU Origin	MAC address of the last GVRP frame received on the port.

show garp timer

Use this command to display GARP timer values for one or more ports.

Syntax

show garp timer [*port-string*]

Parameters

port-string	(Optional) Displays GARP timer information for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, GARP timer information will be displayed for all ports.

Mode

All command modes.

Example

This example shows how to display GARP timer information on ports 1 through 10:

Note: For a functional description of the terms **join**, **leave**, and **leaveall timers**, refer to the standard IEEE 802.1Q documentation, which is not supplied with this device.

```
S Chassis(rw)->show garp timer ge.1.1-10
 Port based GARP Configuration: (Timer units are centiseconds)
 Port Number     Join        Leave     Leaveall
 -----------  ----------  ----------  ----------
 ge.1.1             20          60        1000
 ge.1.2             20          60        1000
 ge.1.3             20          60        1000
 ge.1.4             20          60        1000
 ge.1.5             20          60        1000
 ge.1.6             20          60        1000
 ge.1.7             20          60        1000
 ge.1.8             20          60        1000
 ge.1.9             20          60        1000
 ge.1.10            20          60        1000
```

Table 41-2 provides an explanation of the command output. For details on using the **set garp timer** command to change default timer values, refer to "set garp timer" on page 41-6.

Table 41-2 show garp timer configuration Output Details

Output...	What it displays...
Port Number	Port designation. For a detailed description of possible port-string values, refer to the *Extreme Networks S-Series Configuration Guide*.
Join	Join timer setting.
Leave	Leave timer setting.
Leaveall	Leavall timer setting.

set gvrp

Use this command to enable or disable GVRP globally on the device or on one or more ports.

Syntax

set gvrp {**enable** | **disable**} [*port-string*]

Parameters

enable | **disable**	Enables or disables GVRP on the device. Default: Enabled globally; Disabled at the port level.
port-string	(Optional) Enables or disables GVRP on specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, GVRP will be globally enabled or disabled.

Mode

All command modes.

Examples

This example shows how to enable GVRP globally on the device:

```
S Chassis(rw)->set gvrp enable
```

This example shows how to disable GVRP globally on the device:

```
S Chassis(rw)->set gvrp disable
```

This example shows how to enable GVRP on port 3 in slot 1:

```
S Chassis(rw)->set gvrp enable ge.1.3
```

clear gvrp

Use this command to reset the GVRP status globally or on one or more ports.

Syntax

clear gvrp [*port-string*]

Parameters

port-string	(Optional) Clears GVRP status on specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, GVRP status will be globally cleared.

Mode

All command modes.

Example

This example shows how to clear GVRP status globally on the device:

```
S Chassis(rw)->clear gvrp
```

show gvrp vlan restricted

Use this command to display GVRP VLAN restricted settings information.

Syntax

show gvrp vlan {*vlan-list* | **all**} **restricted**

Parameters

vlan-list	Displays the current GVRP VLAN restricted setting for the specified VLAN(s).
all	Displays the current GVRP VLAN restricted setting for all VLANs on the system.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the GVRP VLAN restricted settings for all VLANs on the system:

```
S Chassis(rw)->show gvrp vlan all restricted
GVRP Restricted Status Enabled on VLAN(s):
none
GVRP Restricted Status Disabled on VLAN(s):
1-4094
S Chassis(rw)->
```

set gvrp vlan restricted

Use this command to disable GVRP processing for specified VLANs.

Syntax

set gvrp vlan *vlan-list* **restricted** {**enable** | **disable**}

Parameters

vlan-list	Specifies a VLAN or range of VLANs the VLAN restricted setting is applied to.
enable | **disable**	Enables or disables the restricted VLAN feature on the specified VLANs. Default: VLAN restricted is disabled globally; GVRP is enabled globally.

Defaults

The VLAN restricted feature defaults to disabled on all VLANs. GVRP processing is enabled on all VLANs by default.

Mode

All command modes.

Usage

When enabling the VLAN restricted feature, GVRP processing is disabled on all specified VLANs regardless of Global or port GVRP settings. Disabling the VLAN restricted setting reverts GVRP behavior back to the current global and per port settings.

Example

This example shows how to disable GVRP processing on VLAN 1 for this system:

```
S Chassis(rw)->set gvrp vlan 1 restricted enable
```

clear gvrp vlan restricted

Use this command to reset the VLAN restrict setting for specified VLAN(s) to the default setting.

Syntax

clear gvrp vlan *vlan-list* **restricted**

Parameters

vlan-list	Specifies a VLAN or range of VLANs for which to reset the VLAN restricted setting to the default setting of disabled.

Defaults

GVRP VLAN behavior defaults to current GVRP global and per port settings.

Mode

All command modes.

Example

This example shows how to clear the VLAN restricted setting on VLAN 1 for this system:

```
S Chassis(rw)->clear gvrp vlan 1 restricted
```

set garp timer

Use this command to adjust the values of the join, leave, and leaveall timers.

Syntax

set garp timer {[**join** *timer-value*] [**leave** *timer-value*] [**leaveall** *timer-value*]} *port-string*

Parameters

join *timer-value*	Sets the GARP join timer in centiseconds (Refer to 802.1Q standard.)
leave *timer-value*	Sets the GARP leave timer in centiseconds (Refer to 802.1Q standard.)
leaveall *timer-value*	Sets the GARP leaveall timer in centiseconds (Refer to 802.1Q standard.)
port-string	Specifies the port(s) on which to configure GARP timer settings. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Usage

The setting of these timers is critical and should only be changed by personnel familiar with the 802.1Q standards documentation, which is not supplied with this device.

Examples

This example shows how to set the GARP join timer value to 100 centiseconds for all ports:

```
S Chassis(rw)->set garp timer join 100 *.*.*
```

This example shows how to set the leave timer value to 300 centiseconds for all ports:

```
S Chassis(rw)->set garp timer leave 300 *.*.*
```

This example shows how to set the leaveall timer value to 20000 centiseconds for all ports:

```
S Chassis(rw)->set garp timer leaveall 20000 *.*.*
```

clear garp timer

Use this command to reset GARP timers back to default values.

Syntax

clear garp timer {[**join**] [**leave**] [**leaveall**]} *port-string*

Parameters

join	(Optional) Resets the join timer to 20 centiseconds.
leave	(Optional) Resets the leave timer to 60 centiseconds.
leaveall	(Optional) Resets the leaveall timer to 1000 centiseconds.
port-string	Specifies the port(s) on which to reset GARP timer(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

At least one optional parameter must be entered.

Mode

All command modes.

Example

This example shows how to reset the GARP leave timer to the default value of 60 centiseconds on port 5 in slot 2:

```
S Chassis(rw)->clear garp timer leave ge.2.5
```

42

MVRP Commands

The commands in this chapter are used to enable or disable the Multiple Vlan Registration Protocol (MVRP) both globally and on an individual port basis, configure the MVRP timer values, and display the current configuration parameters. MVRP is based upon and derives its timers from the Multiple Registration Protocol (MRP). By default, MVRP is disabled on all ports, and globally enabled on the device. For information about configuring MVRP, refer to the "VLAN Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show mrp timer	42-1
set mrp timer	42-2
clear mrp timer	42-3
show mvrp	42-4
set mvrp	42-5
clear mvrp	42-6
show mvrp vlan restricted	42-7
set mvrp vlan restricted	42-7
clear mvrp vlan restricted	42-8

show mrp timer

Use this command to display Multiple Registration Protocol (MRP) timer configuration per port.

Syntax

show mrp timer [*port-string*]

Parameters

port-string	(Optional) Displays MRP timer information for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, MRP configuration information will be displayed for all ports on the device.

Mode

All command modes.

Example

This example shows how to display MRP timer configuration for port 1 in slot 1:

```
S Chassis(rw)->show mrp timer ge.1.1
Port based MRP configuration: (Timer units are centiseconds)
Port Number       Join       Leave      Leaveall    Periodic
-----------    ----------  ----------  ----------  ----------
ge.1.1                 20          60        1000   disabled
```

Table 42-1 provides an explanation of the command output.

Table 42-1 show mrp timer Output Details

Output...	What it displays...
Port Number	Port designation for displayed MRP timer settings.
Join	Specifies the current Join timer setting. Default value is 20 centiseconds (.2 seconds).
Leave	Specifies the current Leave timer setting. Default value is 60 centiseconds (.6 seconds).
Leaveall	Specifies the current LeaveAll timer setting. Default value is 1000 centiseconds (10 seconds).
Periodic	Specifies whether the Periodic timer is enabled or disabled. The value of the Periodic timer is fixed at 1 second.

set mrp timer

Use this command to set the value of Multiple Registration Protocol (MRP) timers on one or more ports.

Syntax

set mrp timer {[**join** *timer-value*] [**leave** *timer-value*] [**leaveall** *timer-value*] [**periodic** {**enable** | **disable**}]} *port-string*

Parameters

join *timer-value*	Specifies the MRP Join timer value as defined in clause 10 of the 802.1Q standard. Valid values are **20** - **4294967295**. The default value is **20** centiseconds (**.2** seconds).
leave *timer-value*	Specifies the MRP Leave timer value as defined in clause 10 of the 802.1Q standard. Valid values are **60** - **4294967295**. The default value is **60** centiseconds (**.6** seconds).
leaveall *timer-value*	Specifies the LeaveAll timer value as defined in clause 10 of the 802.1Q standard. Valid values are **1000** - **4294967295**. The default value is **1000** centiseconds (**10** seconds).

periodic enable | **disable**	Enables or disables the periodic events timer. The periodic timer has a fixed value of **1** second.
port-string	Specifies one or a range of ports the MRP timer settings are applied to. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

The MRP timers default to:

- **join** – 20 centiseconds
- **leave** – 60 centiseconds
- **leaveall** – 1000 centiseconds
- **periodic** – fixed at 1 second and disabled on all ports

Mode

All command modes.

Usage

You must enter at least one timer parameter for this command.

The setting of MRP timers is critical and should only be changed by personnel familiar with the 802.1Q standards documentation. If the default timer values are modified, the following relationships must be maintained:

- The Leave timer should be at least twice the Join timer plus 30 centiseconds.
- The LeaveAll timer should be large relative to the Leave timer.

Setting the LeaveAll timer to a value greater than the Leave timer helps to minimize the volume of rejoining traffic following a LeaveAll message.

MRP timers should be set to the same values on all linked devices.

Examples

This example shows how to set the MRP leave timer to 1 second on ports 1 through 24 for slot 1:

```
S Chassis(rw)->set mrp timer leave 100 ge.1.1-24
```

This example shows how to enable the MRP periodic timer on ports 1 through 24 for slot 1:

```
S Chassis(rw)->set mrp timer periodic enable ge.1.24
```

clear mrp timer

Use this command to reset the value of MRP timers to default values on one or more ports.

Syntax

clear mrp timer {[**join**] [**leave**] [**leaveall**] [**periodic**]} *port-string*

Parameters

join	Resets the interval between the sending of MVRP protocol data units to the default value of 20 centiseconds (.2 seconds).

leave	Resets the number of centiseconds a VLAN will remain in the Leave state before being unregistered to the default value of 60 centiseconds (.6 seconds).
leaveall	Resets the interval between sending LeaveAll messages to the default value of 1000 centiseconds (10 seconds).
periodic	Resets the periodic events timer state to the default value of disabled.
port-string	Specifies one or a range of ports the MRP timer clear settings are applied to. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

The MRP timers default to:

- **join** – 20 centiseconds
- **leave** – 60 centiseconds
- **leaveall** – 1000 centiseconds
- **periodic** – fixed at 1 second and disabled on all ports

Mode

All command modes.

Usage

You must enter at least one timer parameter for this command.

Example

This example shows how to reset the MRP leave timer to the default value of .6 seconds on port ge.1.2:

```
S Chassis(rw)->clear mrp timer leave ge.1.2
```

show mvrp

Use this command to display MVRP state and statistics for one or more ports.

Syntax

show mvrp [*port-string*]

Parameters

port-string	(Optional) Displays MVRP information for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, MVRP information will be displayed for all ports.

Mode

All command modes.

Example

This example shows how to display MVRP information on ports 1 through 3 for slot 1:

```
S Chassis(rw)->show mvrp ge.1.1-3
Global MVRP state is enabled

Port Number    MVRP state     Last PDU Origin      Failed Registrations
-----------    -----------    -----------------    --------------------
ge.1.1         disabled       00-00-00-00-00-00    0
ge.1.2         disabled       00-00-00-00-00-00    0
ge.1.3         disabled       00-00-00-00-00-00    0
```

Table 42-2 provides an explanation of the command output.

Table 42-2 show garp timer configuration Output Details

Output...	What it displays...
Port Number	Specifies the port designation for this MVRP information entry. For a detailed description of possible port-string values, refer to the *Extreme Networks S-Series Configuration Guide*.
MVRP state	Specifies whether MVRP is enabled or disabled on the port.
Last PDU Origin	Specifies the source MAC address of the last PDU received on the port.
Failed Registrations	Specifies the number of times MVRP registration has failed on the port.

set mvrp

Use this command to enable or disable MVRP globally on the device or on one or more ports.

Syntax

set mvrp {**enable** | **disable**} [*port-string*]

Parameters

enable | **disable**	Enables or disables MVRP on the device or specified port(s). Default: Enabled globally; Disabled at the port level.
port-string	(Optional) Enables or disables MVRP on specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

By default MVRP is globally enabled and disabled on all ports.

If *port-string* is not specified, MVRP will be globally enabled or disabled.

Mode

All command modes.

Usage

Global MVRP status determines the flood behavior for MVRP PDUs on the chassis. MVRP and GVRP can not be enabled on the same port. You must first ensure that GVRP is disabled on a port before attempting to enable MVRP. GVRP is disabled by default at the port level.

Examples

This example shows how to enable MVRP globally on the device:

```
S Chassis(rw)->set mvrp enable
```

This example shows how to disable MVRP globally on the device:

```
S Chassis(rw)->set mvrp disable
```

This example shows how to enable MVRP on all ports:

```
S Chassis(rw)->set mvrp enable *.*.*
```

clear mvrp

Use this command to reset MVRP to the default setting globally on the device or on one or more ports.

Syntax

clear mvrp [*port-string*]

Parameters

port-string	(Optional) Resets MVRP to the default value on specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, MVRP will be globally enabled. If a *port-string* is specified, MVRP will be disabled on the specified ports.

Mode

All command modes.

Examples

This example shows how to reset the global MVRP setting to the default value of enabled on the device:

```
S Chassis(rw)->clear mvrp
```

This example shows how to reset the MVRP setting to the default value of disabled on all ports:

```
S Chassis(rw)->clear mvrp *.*.*
```

show mvrp vlan restricted

Use this command to display the MVRP restricted VLAN status for one or more VLANs.

Syntax

show mvrp vlan {*vlan-list* | **all**} **restricted**

Parameters

vlan-list | **all**	Displays MVRP restricted VLAN status for specific or all VLANs. Valid VLAN values are **1** - **4094**.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to display MVRP restricted VLAN status on VLANs 100, 200, and 300:

```
S Chassis(rw)->show mvrp vlan 100,200,300 restricted
MVRP Restricted Status Disabled on VLAN(s):
100,200,300
```

This example shows how to display MVRP restricted VLAN status on all VLANs:

```
S Chassis(rw)->show mvrp vlan all restricted
MVRP Restricted Status Enabled on VLAN(s):
none
MVRP Restricted Status Disabled on VLAN(s):
1-4094
```

set mvrp vlan restricted

Use this command to enable or disable MVRP restricted VLAN on specified VLANs.

Syntax

set mvrp vlan *vlan-list* **restricted** {**enable** | **disable**}

Parameters

vlan-list	Specifies one or a range of VLANs to restrict MVRP on.
enable | **disable**	Enable or disable VLAN restriction on the specified VLANs: • Enable – Restricts (disables) MVRP on specified VLANs • Disable – Disables VLAN restriction (enables MVRP) on the specified VLANs Default: VLAN restriction is disabled on all VLANs.

Defaults

By default MVRP VLAN restriction is disabled on all VLANs.

Mode

All command modes.

Example

This example shows how to enable MVRP restricted VLAN on VLANS 100, 200, and 300:

```
S Chassis(rw)->set mvrp vlan 100,200,300 restricted enable
```

clear mvrp vlan restricted

Use this command to reset MVRP VLAN restriction to the default setting for the specified VLANs.

Syntax

clear mvrp vlan {*vlan-list* | **all**} **restricted**

Parameters

vlan-list | **all**	Resets the MVRP VLAN restricted setting for one, a range, or all VLANs to the default setting of disabled.

Defaults

MVRP VLAN restriction is disabled on all VLANs.

Mode

All command modes.

Example

This example shows how to reset MVRP VLAN restriction to enabled on VLANS 100, 200, and 300:

```
S Chassis(rw)->clear mvrp vlan 100,200,300 restricted
```

43

Policy Profile Commands

This chapter describes the policy profile and rule command sets and how to use them. The chapter is organized into two sections:

- Commands associated with the creation and management of policy roles
- Commands associated with classification rules that set traffic classification and policy behaviors for the roles they are assigned to.

For information about configuring policy, refer to the "Policy Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

Note: It is recommended that you use Extreme Networks S-Series as an alternative to CLI for configuring policy classification on the Extreme Networks S-Series devices.

For information about...	Refer to page...
Policy Profile Commands	43-1
Classification Rule Commands	43-16

Policy Profile Commands

A policy profile is a container that holds all aspects of policy configuration for a given policy role. The policy role defined in the profile is an abstracted basis for applying policy to a part of your network, such as sales, engineering, service or geographical location. Commands in this section provide for:

- Configuration of the policy profile
- Setting of dynamically assigned policy profile options
- Assigning the action the device will apply to an invalid or unknown policy
- Setting a VLAN to policy mapping
- Allowing the application of rules to a profile that overwrite the current user priority and other VLAN tag TCI field information.

For information about...	Refer to page...
show policy profile	43-2
set policy profile	43-4
clear policy profile	43-6
show policy dynamic	43-9

For information about...	Refer to page...
set policy dynamic	43-10
clear policy dynamic	43-11
show policy invalid	43-11
set policy invalid action	43-12
clear policy invalid action	43-12
set policy maptable	43-13
show policy maptable	43-14
clear policy maptable	43-15
show port tcioverwrite	43-15
set port tcioverwrite	43-16

Note: Extreme Networks S-Series devices also support policy-based routing, which forwards or drops packets at Layer 3 according to matching access lists (ACLs) in route maps configured on routing interfaces. For details, refer to the *Extreme Networks S-Series Configuration Guide*. For route map command details see Chapter 85, **Route-Map Manager Commands**.

show policy profile

Use this command to display policy profile information.

Syntax

show policy profile {**all** | *profile-index* [*consecutive-pids*] [**-verbose**]}

Parameters

all | *profile-index*	Displays policy information for all profile indexes or a specific profile index.
consecutive-pids	(Optional) Displays information for specified consecutive profile indexes.
-verbose	(Optional) Displays detailed information.

Defaults

If optional parameters are not specified, summary information will be displayed for the specified index or all indexes.

Mode

All command modes.

Example

This example shows how to display policy information for policy profile 11:

```
S Chassis(rw)->show policy profile 11
Profile Index           :11
Profile Name            :MacAuth1
Row Status              :active
```

```
Port VID Status         :enabled
Port VID Override       :11
CoS Status              :disabled
CoS                     :0
Mirror                  :
Syslog on use           :disabled
Trap on use             :disabled
Disable ingress port    :disabled
Replace TCI Status      :disabled
Tagged Egress VLAN List :11
Forbidden VLAN List     :none
Untagged VLAN List      :none
Replace TCI Status      :enabled
Admin Profile Usage     :none
Oper Profile Usage      :ge.2.1-2
Dynamic Profile Usage   :ge.2.1-2
```

Table 43-1 provides an explanation of the command output.

Table 43-1 show policy profile Output Details

Output...	What it displays...
Profile Index	Number of the policy profile.
Profile Name	User-supplied name assigned to this policy profile.
Row Status	Whether or not the policy profile is enabled (**active**) or disabled.
Port VID Status	Whether or not PVID override is **enabled** or **disabled** for this policy profile. If all the classification rules associated with this profile are missed, then this parameter, if specified, determines default behavior.
Port VID Override	The PVID to assign to packets, if PVID override is enabled.
CoS Status	Whether or not Class of Service override is **enabled** or **disabled** for this profile. If all the classification rules associated with this profile are missed, then this parameter, if specified, determines default behavior.
CoS	The CoS priority value to assign to packets, if CoS override is enabled.
Mirror	Specifies the mirror destination index to this profile.
Syslog on use	Specifies whether Syslog on use is enabled or disabled.
Trap on use	Specifies whether trap on use is enabled or disabled
Disable ingress port	Specifies whether disable ingress port is enabled or disabled.
Tagged Egress VLAN List	VLAN(s) that ports to which the policy profile is assigned can use for tagged egress.
Forbidden VLAN List	VLAN(s) forbidden to ports to which the policy profile is assigned.
Untagged VLAN List	VLAN(s) that ports to which the policy profile is assigned can use for untagged egress.
Replace TCI status	Whether or not the TCI overwrite function is enabled or disabled for this profile.

Table 43-1 show policy profile Output Details (continued)

Output...	What it displays...
Admin Profile Usage	Ports administratively assigned to use this policy profile.
Oper Profile Usage	Ports currently assigned to use this policy profile.
Dynamic Profile Usage	Port dynamically assigned to use this policy profile.

set policy profile

Use this command to create a policy profile entry.

Syntax

```
set policy profile profile-index [name name] [pvid-status {enable | disable}]
[pvid pvid] [cos-status {enable | disable}] [cos cos] [egress-vlans egress-vlans]
[forbidden-vlans forbidden-vlans] [untagged-vlans untagged-vlans] [append]
[clear] [tci-overwrite {enable | disable}] [precedence precedence-list]
[mirror-destination mirror-index] | [clear-mirror] | [prohibit-mirror][syslog
{enable | disable}] [trap {enable | disable}] [disable-port {enable | disable}]
[fst class-index] [web-redirect redirect-index]
```

Parameters

profile-index	Specifies an index number for the policy profile. Valid values are **1** - **1023**.
name *name*	(Optional) Specifies a name for the policy profile. This is a string from 1 to 64 characters.
pvid-status enable | **disable**	(Optional) Enables or disables PVID override for this policy profile. If all the classification rules associated with this profile are missed, then this parameter, if specified, determines default behavior.
pvid *pvid*	(Optional) Specifies the PVID to assign to packets, if PVID override is enabled and invoked as the default behavior.
cos-status enable | **disable**	(Optional) Enables or disables Class of Service override for this policy profile. If all the classification rules associated with this profile are missed, then this parameter, if specified, determines default behavior.
cos *cos*	(Optional) Specifies a COS value to assign to packets, if CoS override is enabled and invoked as the default behavior. Valid values are 0 to 255.
egress-vlans *egress-vlans*	(Optional) Specifies that the port to which this policy profile is applied should be added to the egress list of the VLANs defined by *egress-vlans*. Packets will be formatted as tagged.
forbidden-vlans *forbidden-vlans*	(Optional) Specifies that the port to which this policy profile is applied should be added as forbidden to the egress list of the VLANs defined by *forbidden-vlans*. Packets from this port will not be allowed to participate in the listed VLANs.
untagged-vlans *untagged-vlans*	(Optional) Specifies that the port to which this policy profile is applied should be added to the egress list of the VLANs defined by *untagged-vlans*. Packets will be formatted as untagged.

append	(Optional) Appends this policy profile setting to settings previously specified for this policy profile by the **egress-vlans**, **forbidden-vlans**, or **untagged-vlans** parameters. If **append** is not used, previous VLAN settings are replaced.
clear	(Optional) Clears this policy profile setting from settings previously specified for this policy profile by the **egress-vlans**, **forbidden-vlans**, or **untagged-vlans** parameters.
tci-overwrite enable | **disable**	(Optional) Enables or disables TCI (tag control information) overwrite for this profile. When enabled, rules configured for this profile are allowed to overwrite user priority and other classification information in the VLAN tag's TCI field.
precedence *precedence-list*	(Optional) Assigns a rule precedence to this profile. Lower values will be given higher precedence.
mirror-destination *mirror-index*	(Optional) Applies the specified mirror destination index to this profile. Valid values: 1 - 255.
clear-mirror	(Optional) Clears mirroring on this profile.
prohibit-mirror	(Optional) Prohibits mirroring on this profile.
syslog enable | **disable**	(Optional) Enables or disables syslog on profile use.
trap enable | **disable**	(Optional) Enables or disables traps on profile use.
disable-port enable | **disable**	(Optional) Enables or disables the disabling of ingress ports on profile use.
fst *class-index*	(Optional) Specifies a flow limit class to associate with this profile.
web-redirect *redirect-index*	(Optional) Specifies a web-redirection index used by captive portal redirection to associate with this profile. 0 = No index set. Default = 0.

Defaults

- If optional parameters are not specified, none will be applied.
- If disable-port enable is not specified, disable-port is disabled.
- If syslog enable is not specified, syslog is disabled.
- If trap enable is not specified, traps are disabled.
- *redirect-index* defaults to 0.
- If an FST class is not specified, flowlimiting is not applied to this profile.
- If web-redirect is not specified, The web-redirect class indexes remain unchanged.

Mode

All command modes.

Example

This example shows how to create a policy profile 1 named "netadmin" with PVID override enabled for PVID 10, and Class-of-Service override enabled for CoS 5. This profile can use VLAN 10 for untagged egress:

```
S Chassis(rw)->set policy profile 1 name netadmin pvid-status enable pvid 10
cos-status enable cos 5 untagged-vlans 10
```

clear policy profile

Use this command to delete a policy profile entry.

Syntax

clear policy profile *profile-index*

Parameters

profile-index	Specifies the index number of the policy profile entry to be deleted. Valid values are **1** to **1023**.

Defaults

None.

Mode

All command modes.

Example

This example shows how to delete policy profile 8:

```
S Chassis(rw)->clear policy profile 8
```

show policy captive-portal

Use this command to display the status of dynamically assigned policy profile options.

Syntax

show captive-portal [**listening**] [**web-redirect** [*class-index*]]

Parameters

listening	(Optional) Displays the configured Captive Portal Redirection listening ports for this device.
web-redirect *class-index*	

Defaults

If no option is specified, both listening configuration and web-direct configuration for all web-direct classes display.

If class-index is not specified, web-direct configuration for all web-direct classes display.

Mode

All command modes.

Example

This example shows how to display the Captive Portal Redirection listening configuration:

```
S Chassis(rw)->show policy captive-portal listening
Captive Portal Listening Ports: 80   8080
```

This example shows how to display the web-redirect class index **1** configuration:

```
S Chassis(rw)->show policy captive-portal web-redirect 1
Web-redirect Index: 1
      Server Index: 1
        Server Status:  Enabled
        Server URL:     http://10.52.3.101:80/static/index.jsp

      Server Index: 2
        Server Status:  Enabled
        Server URL:     http://10.52.3.102:80/static/index.jsp
```

set policy captive-portal listening

Use this command to configure the ports on which policy will listen for client traffic subject to HTTP redirection.

Syntax

set policy captive-portal listening *port-list*

Parameters

port-list	Specifies up to three ports delineated by a comma on which the captive portal feature will listen for traffic subject to HTTP redirection.

Defaults

None.

Mode

All command modes.

Usage

The captive portal policy feature uses HTTP redirection to force a client's web browser to be redirected to a particular administrative web page. The ports on which captive portal listens for client traffic subject to HTTP redirection are configured using this command. Specify up to three listening ports in the port list. Each port is delineated by a comma.

Example

This example configures captive portal listening on ports 80 and 8080:

```
S Chassis(rw)->set policy captive-portal listening 80,8080
S Chassis(rw)->
```

clear policy captive-portal listening

Use this command to remove ports on which policy will listen for client traffic subject to HTTP redirection.

Syntax

clear policy captive-portal listening *port-list*

Parameters

port-list	Specifies up to three ports delineated by a comma to remove from the captive portal listening port list.

Defaults

None.

Mode

All command modes.

Example

This example removes port 80 from the captive portal listening port list:

```
S Chassis(rw)->clear policy captive-portal listening 80
S Chassis(rw)->
```

set policy captive-portal web-redirect

Use this command to configure and enable or disable a web-redirect server configuration.

Syntax

set policy captive-portal web-redirect *redirect-index* **server** *server-id* **http://***ipaddress*:*port*/path {**enable** | **disable**}

Parameters

redirect-index	Specifies the web-redirect index value associated with the policy profile.
server *server-id*	Specifies the server associated with this web-redirect configuration.
http://*ipaddress*:*port*/*path*	Specifies the absolute server address associated with this web-redirect configuration.
enable | disable	Enables or disables the web-redirect configuration.

Defaults

None.

Mode

All command modes.

Usage

The captive portal policy feature uses HTTP redirection to force a client's web browser to be redirected to a particular administrative web page. This command provides for the association of the server on which the redirected web page resides with a web-redirect index. The web-redirect index is associated with a given policy profile using the web-redirect option when configuring the policy profile (See "set policy profile" on page 43-4). The absolute server address must begin with http://, specify an IPv4 address and TCP port delineated by a colon, followed by a path that must have at least a single backslash (/).

Example

This example enables WEB index **1** to redirect a client's web browser to IP address **11.11.11.1** and port of **1234** on server **1**:

```
S Chassis(rw)->set policy captive-portal web-redirect 2 server 1 url http
://10.52.3.103:80/ status enable
S Chassis(rw)->
```

clear policy captive-portal web-redirect

Use this command to delete a web-redirect configuration.

Syntax

clear policy captive-portal web-redirect *redirect-index* **server** *server-index*

Parameters

redirect-index	Specifies the web-redirect index value for the web-redirect configuration to clear.
server-index	Specifies the web-redirect server to clear for this web-redirect index

Defaults

None.

Mode

All command modes.

Example

This example deletes web-redirect index 1 server 1 configuration:

```
S Chassis(rw)->clear policy captive-portal web-redirect 1 server 1
S Chassis(rw)->
```

show policy dynamic

Use this command to display the status of dynamically assigned policy profile options.

Syntax

show policy dynamic {[**override**] [**syslog-default**] [**trap-default**]}

Parameters

override	Shows the status of which current profile admin or dynamic assignment rules are overriding the other.
syslog-default	Shows the status of automatically sending Syslog messages when a dynamic rule is applied.
trap-default	Shows the status of automatically sending SNMP trap messages when a dynamic rule is applied.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the status of Syslog message sending when a dynamic rule is applied:

```
S Chassis(rw)->show policy dynamic syslog-default
Syslog-default is ENABLED
```

set policy dynamic

Use this command to set the status of dynamically assigned policy profile options.

Syntax

set policy dynamic {[**syslog-default** {**enable** | **disable**}] [**trap-default** {**enable** | **disable**}]}

Parameters

syslog-default enable | disable	Enables or disables the sending of Syslog messages when a dynamic rule is applied.
trap-default enable | disable	Enables or disables the sending of SNMP trap messages when a dynamic rule is applied.

Defaults

None.

Mode

All command modes.

Usage

Dynamic policy profiles are assigned by authentication protocols as traffic enters the device. The authentication server returns a policy profile ID to the edge device as part of the authentication process. This ID is then used by the device to place the port (and its user) into a predefined policy profile, consisting of a set of rules and limitations to be applied to the port.

Example

This example shows how to disable the sending of Syslog messages when a dynamic rule is applied:

```
S Chassis(rw)->set policy dynamic syslog-default disable
```

clear policy dynamic

Use this command to reset the status of dynamically assigned policy profiles back to defaults.

Syntax

```
clear policy dynamic {[syslog-default] [trap-default]}
```

Parameters

syslog-default	Resets the status of the sending of Syslog messages when a dynamic rule is applied to enabled.
trap-default	Resets the status of the sending of SNMP trap messages when a dynamic rule is applied to enabled.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the sending of Syslog messages when a dynamic rule is applied to enabled:

```
S Chassis(rw)->clear policy dynamic syslog-default
```

show policy invalid

Displays information about the action the device will apply on an invalid or unknown policy.

Syntax

```
show policy invalid {action | count | all}
```

Parameters

action	Displays the action the device should take if asked to apply an invalid or unknown policy. The action is set by “set policy invalid action” on page 43-12.
count	Displays the number of times the device has detected an invalid/unknown policy.
all	Displays both action and count information.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display invalid policy action and count information:

```
S Chassis(rw)->show policy invalid all
Current action on invalid/unknown profile is: Forward packets
Number of invalid/unknown profiles detected: 4
```

set policy invalid action

Use this command to assign the action the device will apply to an invalid or unknown policy.

Syntax

set policy invalid action {**default-policy** | **drop** | **forward**}

Parameters

default-policy	Instructs the device to ignore the result and search for the next policy assignment rule. If all rules are missed, the default policy is applied.
drop	Instructs the device to block traffic.
forward	Instructs the device to forward traffic as if no policy has been assigned via 802.1d/Q rules.

Defaults

None.

Mode

All command modes.

Example

This example shows how to assign a drop action to invalid policies:

```
S Chassis(rw)->set policy invalid action drop
```

clear policy invalid action

Use this command to reset the action the device will apply to an invalid or unknown policy to the default action.

Syntax

clear policy invalid action

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

The default action instructs the device to ignore the invalid or unknown policy and search for the next policy assignment rule. If all rules are missed, the default policy is applied.

Example

This example shows how to reset the invalid policy action:

```
S Chassis(rw)->clear policy invalid action
```

set policy maptable

Use this command to add entries to the mapping table and to set the map table response state for the switch.

Syntax

set policy maptable {*vlan-list profile-index* | **response** {**tunnel** | **policy** | **both**}}

Parameters

vlan-list	VLAN ID or range of IDs. Valid values: **1** to **4094**.
profile-index	Policy ID. Valid Values **1** to **1023**.
response tunnel | **policy** | **both**	Indicates which attributes to use from RADIUS response. **tunnel** - Apply the vlan-tunnel attribute **policy** - Apply the filter-id attribute (default response) **both** - Apply both attributes

Defaults

None.

Mode

All command modes.

Usage

The **policy** response is the default response for the **set policy maptable** command.

Example

This example adds an entry to the map table that maps VLAN 3 to policy profile 8:

```
S Chassis(rw)->set policy maptable 3 8
```

This example sets the switch to use both tunnel and policy attributes in the RADIUS response for the Policy Profile mappings:

```
S Chassis(rw)->set policy maptable response both
```

show policy maptable

Use this command to display the VLAN ID - Policy Profile mappings table for all or the specified VLANs.

Syntax

show policy maptable [*vlan-list*]

Parameters

vlan-list	(Optional) VLAN ID or range of IDs (1 to 4094)

Defaults

If a vlan-list is not specified, maptable entries for all VLANs are displayed.

Mode

All command modes, Read.

Examples

This example displays the policy map table status and also the contents of the map table for all VLANs.

```
S Chassis(rw)->show policy maptable

Policy map response:  policy
Policy map last change: 0 days 3:19:02.77
Policy Mappings:
VLAN ID   Policy Profile
1         22  (Engineering User)
2         23  (Sales User)
4094      400 (Guest)
S Chassis(rw)->
```

This example displays the policy map table status and also the contents of the map table for VLAN 2:

```
S Chassis(rw)->show policy maptable 2

Policy map response     :  policy
Policy map last change  :  0 days 3:21:02.77
```

```
VLAN ID        Policy Profile
2              23 (Sales User)

S Chassis(rw)->
```

clear policy maptable

Use this command to clear a VLAN to policy mapping table entry or to reset the maptable response to the default value of policy mode.

Syntax

clear policy maptable {*vlan-list* | **response**}

Parameters

vlan-list	Specifies the VLAN ID or range of IDs (1 to 4094) to clear.
response	Specifies that the response should be reset to the default value of **policy**.

Defaults

None.

Mode

All command modes.

Examples

This example resets the policy mappings table response to the default value of **policy**.

```
S Chassis(rw)->clear policy maptable response
```

This example deletes the policy mappings table for VLAN 1 and VLAN 2.

```
S Chassis(rw)->clear policy maptable 1-2
```

show port tcioverwrite

Use this command to display the status of the port Tag Control Information (TCI) overwrite function on one or more ports.

Syntax

show port tcioverwrite [*port-string*]

Parameters

port-string	(Optional) Displays TCI overwrite status for specific port(s).

Defaults

If *port-string* is not specified, TCI overwrite status will be displayed for all ports.

Mode

All command modes.

Usage

When enabled, using "set port tcioverwrite" on page 43-16, TCI overwrite allows policy rules to overwrite all tagged (TCI) frames ingressing on those ports. The **show port tcioverwrite** command displays the TCI overwrite status for each port or the specified port on the device.

Example

This example shows how to display TCI overwrite status for port ge.1.3:

```
S Chassis(rw)->show port tcioverwrite ge.1.3
TCI overwrite for port ge.1.3 is disabled
```

set port tcioverwrite

Use this command to enable or disable the TCI overwrite function on one or more ports.

Syntax

set port tcioverwrite *port-string* {**enable** | **disable**}

Parameters

port-string	Specifies port(s) on which to enable or disable the TCI overwrite function.
enable | **disable**	Enables or disables the TCI overwrite function.

Defaults

None.

Mode

All command modes.

Usage

When enabled, this allows policy rules to overwrite user priority and other classification information in the VLAN tag's TCI field. The **set port tcioverwrite** command, when enabled, also overwrites ingressing frames tagged to a port VLAN and policy assignment, if a policy has not already been assigned.

Example

This example shows how to enable TCI overwrite on port ge.1.3:

```
S Chassis(rw)->set port tcioverwrite ge.1.3 enable
```

Classification Rule Commands

Classification rules associate specific traffic classifications or policy behaviors with the policy role. Classification rules associate a traffic classification with a policy role by assigning the traffic classification to an administrative profile. Classification rules also assign policy rules that define desired policy behaviors for the specified traffic classification type.

Classification and rule management commands in this section provide for:

- Configuration of policy rules and admin profiles

- Collection of classification rule statistics through policy accounting
- Assigning of administrative rules to a port
- Applying traffic rules to the admin profile for one or more
- Clearing of rule usage information if operational status “up” is detected on any port
- Configuration of Syslog policy settings

For information about...	Refer to page...
show policy rule	43-17
show policy capability	43-21
set policy rule	43-23
clear policy rule	43-27
clear policy all-rules	43-29
show policy accounting	43-29
set policy accounting	43-30
clear policy accounting	43-30
set policy port	43-31
show policy allowed-type	43-31
set policy allowed-type	43-33
clear policy allowed-type	43-35
show policy dropped-notify	43-36
show policy disabled-ports	43-36
clear policy disabled-ports	43-37
clear policy usage-list	43-37
show policy autoclear	43-39
set policy autoclear	43-40
clear policy autoclear	43-40
clear policy port-hit	43-41
show policy syslog	43-42
set policy syslog	43-42
clear policy syslog	43-44

show policy rule

Use this command to display policy classification and admin rule information.

Syntax

show policy rule [**attribute**] | [**all**] | [**admin-profile**] | [*profile-index*] [**port-hit**] {**application** | **ether** | **icmptype** | **ip6dest** | **ip6source** | **ipdestsocket** | **ipfrag** | **ipproto** | **ipsourcesocket** | **iptos** | **ipttl** | | **ipxclass** | **ipxdest** | **ipxsource** | **ipxdestsocket** | **ipxsourcesocket** | **ipxtype** | **llcDsapSsap** | **macdest** |

macsource | **port** | **tci** | **tcpdestport** | **tcpdestportIP** | **tcpsourceport** | **tcpsourceportIP** | **udpdestportIP** | **udpsourceport** | **udpsourceportIP** | **vlantag**} [*data*] [**mask** *mask*] [**port-string** *port-string*] [**rule-status** {**active** | **not-in-service** | **not-ready**}] [**storage-type** {**non-volatile** | **volatile**}] [**vlan** *vlan*] | [**drop** | **forward**] [**dynamic-pid** *dynamic-pid*] [**cos** *cos*] [**admin-pid** *admin-pid*] [**syslog** {**enable** | **disable** | **prohibit**}] [-verbose] [**trap** {**enable** | **disable** | **prohibit**}] [**disable-port** {**enable** | **disable** | **prohibit**}] [**usage-list**] [**display-if-used** *port-list*] [**tci-overwrite** {**enable** | **disable** | **prohibit**}] [**mirror-destination** *mirror-index*] | [**clear-mirror**] | [**prohibit-mirror**] [**-verbose**] [**-wide**]

Parameters

attribute	Displays the attributes of the specified rules.
all | **admin-profile** | *profile-index*	Displays **all** admin and classification rules, rules for the admin profile, or for a specific *profile-index* number. Valid index values are **1** - **1023**.
port-hit	Displays ports for which a policy rule-hit has occurred.
application	Displays based upon queries or responses from applications Link Local Multicast Name Resolution (LLMNR), Simple Service Discovery Protocol (SSDP), or Multicast Domain Name System - Self Discovery (mDNS-SD).
ether	Displays Ethernet type II rules.
icmptype	Displays ICMP type rules.
ip6dest	Displays IPv6 destination address rules.
ip6source	Displays IPv6 source address rules.
ipdestsocket	Displays IP destination address rules with optional post-fixed port.
ipfrag	Displays IP fragmentation rules.
ipproto	Displays IP protocol field in IP packet rules.
ipsourcesocket	Displays IP source address rules with optional post-fixed port.
iptos	Displays Type of Service rules.
ipttl	Displays IP time-to-live (TTL) rules.
ipxclass	Displays IPX transmission control rules.
ipxdest	Displays destination IPX address rules.
ipxsource	Displays source IPX address rules.
ipxdestsocket	Displays destination IPX socket rules.
ipxsourcesocket	Displays source IPX socket rules.
ipxtype	Displays IPX packet type rules.
llcDsapSsap	Displays 802.3 DSAP/SSAP rules.
macdest	Displays MAC destination address rules.
macsource	Displays MAC source address rules.
port	Displays port related rules.
tci	Displays Tag Control Information rules.
tcpdestport	Displays TCP destination port rules.
tcpdestportip	Displays TCP destination port with optional IP address rules.
tcpsourceport	Displays TCP source port rules.

tcpsourceportip	Displays TCP source port with optional IP address rules.
udpdestport	Displays UDP destination port rules.
udpsourceport	Displays
udpsourceportip	Displays UDP source port with optional IP address rules.
vlantag	Displays VLAN tag rules.
data	(Not required for **ipfrag** classification.) Displays rules for a predefined classifier. This value is dependent on the classification type entered. Refer to Table 43-3 on page 43-26 for valid values for each classification type.
mask *mask*	(Optional) Displays rules for a specific data mask. Refer to Table 43-3 on page 43-26 for valid values for each classification type and data value.
port-string *port-string*	(Optional) Displays rules related to a specific ingress port.
rule-status active | **not-in-service** | **not-ready**	(Optional) Displays rules related to a specific rules status.
storage-type non-volatile | **volatile**	(Optional) Displays rules configured for either non-volatile or volatile storage.
vlan vlan	(Optional) Displays rules for a specific VLAN ID.
drop | **forward**	Displays rules based on whether matching packets specified by the **vlan** parameter will be dropped or forwarded.
dynamic-pid *dynamic-pid*	Displays rules associated with a specific dynamic policy profile index ID.
cos *cos*	(Optional) Displays rules for a Class-of-Service value.
admin-pid admin-pid	Displays rules associated with a specific administrative policy profile index ID.
syslog enable | **disable**	(Optional) Displays rules that have Syslog enabled or disabled.
trap enable | **disable**	(Optional) Displays rules that have SNMP traps enabled or disabled.
disable-port enable | **disable**	(Optional) Displays rules that have the disable port feature enabled or disabled.
usage-list *usage-list*	(Optional) Displays all rule usage for the specified port.
display-if-used *port-list*	(Optional) Displays only rule(s) used for the specified port.
tci-overwrite enable | **disable** | **prohibit**	(Optional) Displays TCI overwrite rules.
mirror-destination *mirror-index*	(Optional) Displays rules for the specified mirror destination index.
clear-mirror	(Optional) Displays clear mirror rules.
prohibit-mirror	(Optinal) Displays prohibit mirror rules.
-verbose	(Optional) Displays detailed information.
-wide	(Optional) Display is greater than 80 characters in width.

Defaults

- If *port-string*, **cos** and **storage-type** are not specified, all rules related to other specifications will be displayed.
- If -**verbose** is not specified, summary information will be displayed.
- If **-wide** is not specified, an 80 character display width is used.

Mode

All command modes.

Examples

This example shows how to display policy classification information for **macsource** rules:

```
S Chassis(rw)->show policy rule macsource
Admn|Rule Type   |Rule Data            |Msk|PortStr   |RS|ST|STDO|dPID|aPID|Mir|U|Qua|
admn|MACSource   |00-00-11-00-00-11    | 48|ge.2.2    | A| V|    |fwrd|    |   |?|   |
admn|MACSource   |00-00-12-00-00-12    | 48|ge.2.4    | A| V|    |fwrd|    |   |?|   |
admn|MACSource   |00-00-21-00-00-21    | 48|ge.2.46   | A| V|    |fwrd|    |   |?|   |
admn|MACSource   |00-00-22-00-00-22    | 48|ge.2.48   | A| V|    |fwrd|    |   |?|   |
admn|MACSource   |00-01-F4-DA-04-92    | 48|ge.2.1    | A| V|    |fwrd|    |   |?|   |
admn|MACSource   |00-11-22-33-44-55    | 48|ge.2.10   | A| V|    |fwrd|    |   |?|   |
admn|MACSource   |00-11-88-15-EF-13    | 48|ge.2.1    | A| V|    |fwrd|    |   |?|   |
admn|MACSource   |00-11-88-BD-A9-22    | 48|ge.2.1    | A| V|    |fwrd|    |   |?|   |
admn|MACSource   |00-11-88-FE-52-74    | 48|ge.2.1    | A| V|    |fwrd|    |   |?|   |
```

This example shows how to display admin rule information for the policy profile with rule type UDP source port:

```
S Chassis(rw)->show policy rule udpsourceport
PID |Rule Type   |Rule Data            |Msk|PortStr   |RS|ST|STDO|VLAN|CoS |Mir|U|Qua|
4   |UDPSrcPort  |67                   | 16|All       | A|NV|    |    |    |   |?|1  |
4   |UDPSrcPort  |161                  | 16|All       | A|NV|    |drop|    |   |?|   |
4   |UDPSrcPort  |162                  | 16|All       | A|NV|    |drop|    |   |?|   |
10  |UDPSrcPort  |67                   | 16|All       | A|NV|    |drop|    |   |?|1  |
10  |UDPSrcPort  |69                   | 16|All       | A|NV|    |drop|    |   |?|   |
10  |UDPSrcPort  |520                  | 16|All       | A|NV|    |drop|   7|   |?|   |
10  |UDPSrcPort  |13119                | 16|All       | A|NV|Y   |drop|    |   |?|1  |
```

Table 43-2 provides an explanation of the command output.

Table 43-2 show policy rule Output Details

Output...	What it displays...
PID	Profile profile index number, indicating a classification rule is displayed. Assigned to this classification rule with the **set policy profile** command (“set policy profile” on page 43-4).
Admin	Indicates an admin rule is displayed.
Rule Type	Whether the rule protocol-based or port-based. Refer to Table 43-3 on page 43-26 for valid classification types.
Rule Data	Rule data value. Refer to Table 43-3 on page 43-26 for valid values for each classification type.

Table 43-2 show policy rule Output Details (continued)

Output...	What it displays...
Msk	Rule data mask. Refer to Table 43-3 on page 43-26 for valid values for each classification data value.
PortStr	Ingress port(s) to which this rule applies.
RS	Whether or not the status of this rule is active (A), not in service or not ready.
ST	Whether or not this rule's storage type is non-volatile (NV) or volatile (V).
S	Whether or not Syslog is enabled (Y) or disabled for this rule.
T	Whether or not SNMP traps are enabled (Y) or disabled for this rule.
D	Whether or not the port disable feature is enabled (Y) or disabled for this rule.
Vlan	VLAN ID to which this rule applies and whether or not matching packets will be dropped or forwarded.
CoS	Class of Service value to which this rule applies.
Mir	Whether or not a destination mirror is applied to this policy
U	Whether or not this rule has been used.
dPID	Whether or not this is a dynamic profile ID.
aPID	Whether or not this is an administrative profile index ID.
Qua	The quarantine policy profile index if a quarantine policy profile is applied to the rule.

show policy capability

Use this command to display all policy classification capabilities supported by your Extreme Networks S-Series device.

Syntax

show policy capability

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

The output of this command shows a table listing classifiable traffic attributes and the type of actions, by rule type, that can be executed relative to each attribute. Above the table is a list of all the actions possible on this device.

The left-most column of the table lists all possible classifiable traffic attributes. The next two columns from the left indicate how policy profiles may be assigned, either administratively or dynamically. The next four columns from the left indicate the actions that may be performed. The last three columns indicate auditing options.

An x in an action column for a traffic attribute row indicates that your system has the capability to perform that action for traffic classified by that attribute.

Example

This example shows how to display your Extreme Networks S-Series device's policy classification capabilities. Refer to "set policy rule" on page 43-23 for a description of the parameters displayed:

```
S Chassis(rw)->show policy capability

The following supports related to policy are supported in this device:
----------------------------------------------------------------------

VLAN Forwarding         Priority               Permit
Deny                    Precedence Reordering  TCI Overwrite
Rules Table             Rule-Use Accounting    Rule-Use Notification
CoS Table               Longest Prefix Rules   Port Disable Action
Auto Clear On Link      Auto Clear Interval    Auto Clear On Profile
RFC 3580 Map            Policy Enable          Mirror Action
Egress Policy           Flow Setup Thresholding Quarantine Assignment


=================================================================================
|                          | D |   |   |   | F |   |   | D | T |   | Q |
|                          | Y |   |   |   | O | S |   | I | C | M | U |
|                          | N | A |   |   | R | Y |   | S | I | I | A |
|                          | A | D | V |   | D | W | S | T | A | O | R | R |
|                          | M | M | L | C | R | A | L | R | B | V | R | A |
|                          | I | I | A | O | O | R | O | A | L | E | O | N |
| SUPPORTED RULE TYPES     | C | N | N | S | P | D | G | P | E | R | R | T |
=================================================================================
|MAC source address        | X | X | X | X | X | X | X | X | X | X | X | X |
|MAC destination address   | X | X | X | X | X | X | X | X | X | X | X | X |
|IPX source address        | X | X | X | X | X | X | X | X | X | X | X | X |
|IPX destination address   | X | X | X | X | X | X | X | X | X | X | X | X |
|IPX source socket         | X | X | X | X | X | X | X | X | X | X | X | X |
|IPX destination socket    | X | X | X | X | X | X | X | X | X | X | X | X |
|IPX transmission control  | X | X | X | X | X | X | X | X | X | X | X | X |
|IPX type field            | X | X | X | X | X | X | X | X | X | X | X | X |
|IPv6 source address       | X | X | X | X | X | X | X | X | X | X | X | X |
|IPv6 destination address  | X | X | X | X | X | X | X | X | X | X | X | X |
|IPv6 flow label           | X | X | X | X | X | X | X | X | X | X | X | X |
|IP source address         | X | X | X | X | X | X | X | X | X | X | X | X |
```

```
|IP destination address   | X | X | X | X | X | X | X | X | X | X | X |
|IP fragmentation         | X | X | X | X | X | X | X | X | X | X | X |
|UDP port source          | X | X | X | X | X | X | X | X | X | X | X |
|UDP port destination     | X | X | X | X | X | X | X | X | X | X | X |
|TCP port source          | X | X | X | X | X | X | X | X | X | X | X |
|TCP port destination     | X | X | X | X | X | X | X | X | X | X | X |
|ICMP packet type         | X | X | X | X | X | X | X | X | X | X | X |
|TTL                      | X | X | X | X | X | X | X | X | X | X | X |
|IP type of service       | X | X | X | X | X | X | X | X | X | X | X |
|IP proto                 | X | X | X | X | X | X | X | X | X | X | X |
|Ether II packet type     | X | X | X | X | X | X | X | X | X | X | X |
|LLC DSAP/SSAP/CTRL       | X | X | X | X | X | X | X | X | X | X | X |
|VLAN tag                 | X | X | X | X | X | X | X | X | X | X | X |
|Replace TCI              | X | X | X | X | X | X | X | X | X | X | X |
|Port string              | X | X | X | X | X | X | X | X | X | X | X |
================================================================================
```

set policy rule

Use this command to assign incoming untagged frames to a specific policy profile and to VLAN or Class-of-Service classification rules.

Syntax

set policy rule {**admin-profile** | *profile-index*} {**application** | **ether** | **icmptype** | **ip6dest | ip6source** | **ipfrag** | **ipproto** | **ipdestsocket** | **ipsourcesocket** | **iptos** | **ipxclass** | **ipxdest** | **ipxsource** | **ipxdestsocket** | **ipxsourcesocket** | **ipxtype** | **llcDsapSsap** | **macdest** | **macsource** | **tci** | **port** | **tcpdestportip** | **tcpsourceportip** | **udpdestportip** | **udpsourceportip** | **vlantag**} *data* [**mask** *mask*] [**port-string** *port-string*] [**storage-type** {**non-volatile** | **volatile**}] [**vlan** *vlan*] | [**drop** | **forward**] [**admin-pid** *admin-pid*] [**cos** *cos*] [**syslog** {**enable** | **disable** | **prohibit**}][**trap** {**enable** | **disable** | **prohibit**}] [**disable-port** {**enable** | **disable** | **prohibit**}] [**tci-overwrite** {**enable** | **disable** | **prohibit**}] [**quarantine-profile** *quarantine-profile*] [**clear-quarantine-profile**] [**prohibit-quarantine-profile**] [**mirror-destination** mirror-index] | [**clear-mirror**] | [**prohibit-mirror**]

Parameters

admin-profile | *profile-index*	Specifies that this is an administrative rule or associates this classification rule with a policy profile index configured with the **set policy profile** command ("set policy profile" on page 43-4). Valid *profile-index* values are **1**- **1023**. **Note:** Admin profiles can be assigned to a specific ingress port by specifying **port-string** and **admin-pid** values as described below.
application	Classifies based upon queries or responses/announcements from applications Link Local Multicast Name Resolution (LLMNR), Simple Service Discovery Protocol (SSDP) , or Multicast Domain Name System - Self Discovery (mDNS-SD). The data field can be entered using keywords: • **llmnr** {**query** | **response**} • **ssdp** {**query** | **announce**} • **mdns-sd** {**query** | **response**}
ether	Classifies based on type field in Ethernet II packet.
i**cmptype**	Classifies based on ICMP type.
ip6dest	Classifies based on the IPv6 destination address with optional post-fixed port. Valid values are aaaa::bbbb[-ab (0..65535)]; mask 1-144).
ip6source	Classifies based on the IPv6 source address with optional post-fixed port. Valid values are aaaa::bbbb[-ab (0..65535)]; mask 1-144.
ipdest	Classifies based on destination IP address.
ipdestsocket	Classifies based on destination IP address with optional post-fixed port.
ipfrag	Classifies based on IP fragmentation value.
ipproto	Classifies based on protocol field in IP packet.
ipsource	Classifies based on source IP address.
ipsourcesocket	Classifies based on source IP address with optional post-fixed port.
iptos	Classifies based on Type of Service field in IP packet.
ipxclass	Classifies based on transmission control in IPX.
ipxdest	Classifies based on destination IPX address.
ipxsource	Classifies based on source IPX address.
ipxdestsocket	Classifies based on destination IPX socket.
ipxsourcesocket	Classifies based on source IPX socket.
ipxtype	Classifies based on IPX packet type.
llcDsapSsap	Classifies based on DSAP/SSAP pair in 802.3 type packet.
macdest	Classifies based on MAC destination address.
macsource	Classifies based on MAC source address.
tci	Classifies based on Tag Control Information.
port	Classifies based on data ingressing on the specified port-string.
tcpdestportip	Classifies based on TCP destination port with optional post-fix IP address.
tcpsourceportip	Classifies based on TCP source port optional post-fix IP address.

udpdestportip	Classifies based on UDP destination port optional post-fix IP address.
udpsourceportip	Classifies based on UDP source port optional post-fix IP address.
vlantag	Classifies based on VLAN tag.
data	(Not required for **ipfrag** classification.) Specifies the code for a predefined classifier. This value is dependent on the classification type entered. Refer to Table 43-3 on page 43-26 for valid values for each classification type.
mask *mask*	(Optional) Specifies the number of significant bits to match, dependent on the *data* value entered. Refer to Table 43-3 on page 43-26 for valid values for each classification type and data value.
port-string *port-string*	(Optional) Displays rule based on the port number on which this rule is applied. If the port parameter is specified, the specified port strings must be the same.
storage-type non-volatile | **volatile**	(Optional) Adds or removes this entry from non-volatile storage.
vlan vlan	(Optional) Classifies to a VLAN ID.
drop | **forward**	(Optional) Specifies that packets within this classification will be dropped or forwarded.
admin-pid admin-pid	(Optional) If **admin-profile** is specified, associates this rule with a policy profile index ID. Valid values are **1** - **1023**.
cos *cos*	(Optional) Specifies that this rule will classify to a Class-of-Service ID. Valid values are **0** - **255**, and can be configured using the **set cos settings** command as described in "set cos settings" on page 45-21. A value of -1 indicates that no CoS forwarding behavior modification is desired.
syslog enable | **disable** | **prohibit**	(Optional) Enables or disables sending of Syslog messages on first rule use. Prohibit - Prohibits lower precedence rules from sending syslog messages.
trap enable | **disable** | **prohibit**	(Optional) Enables or disables sending SNMP trap messages on first rule use. Prohibit - Prohibits lower precedence rules from sending trap messages.
disable-port enable | **disable** | **prohibit**	(Optional) Enables or disables the ability to disable the ingress port on first rule use. Prohibit - Prohibits lower precedence rules from disabling the ingress port.
tci-overwrite enable | **disable** | **prohibit**	(Optional) Enables or disables tci-overwrite, or prohibits lower precedence rules from overwriting the TCI.
quarantine-profile *quarantine-profile*	(Optional) Set the quarantine profile index for this rule. Valid values are 1 - 1024.
clear-quarantine-profile	(Optional) Clear the quarantine profile on this rule.
prohibit-quarantine-profile	(Optional) Prohibit quarantine on this rule.
mirror-destination *mirror-destination-index*	(Optional) Applies the specified mirror-destination to this rule.
clear-mirror	(Optional) Clears mirroring for this rule.
prohibit-mirror	(Optional) Prohibits mirroring for this rule.

Defaults

- If *mask* is not specified, all data bits will be considered relevant.
- If *port-string* is not specified, rule will be scoped to all ports.

Mode

All command modes.

Usage

Classification rules are automatically enabled when created.

Examples

This example shows how to use Table 43-3 on page 43-26 to create (and enable) a classification rule to associate with policy number 1. This rule will filter Ethernet II Type 1526 frames to VLAN 7:

```
S Chassis(rw)->set policy rule 1 ether 1526 vlan 7
```

This example shows how to use Table 43-3 on page 43-26 to create (and enable) a classification rule to associate with policy profile number 5. This rule specifies that UDP frames from source port 45 will be filtered to VLAN 7:

```
S Chassis(rw)->set policy rule 5 udpportsourceip 45 vlan 7
```

This example shows how to configure classification rule 2 as an administrative profile and assign it to ingress port ge.1.1:

```
S Chassis(rw)->set policy rule admin-profile port ge.1.1 port-string ge.1.1
admin-pid 2
```

This example shows how to classify all Ethernet II Type 1526 frames to administrative policy profile 2:

```
S Chassis(rw)->set policy rule admin-profile ether 1526 admin-pid 2
```

Table 43-3 provides the **set policy rule** *data* values that can be entered for a particular classification type, and the *mask* bits that can be entered for each classifier associated with that parameter.

Table 43-3 Valid Values for Policy Classification Rules

Classification Rule Parameter	*data* value	*mask* bits
application	{**llmnr**| **ssdp** | **mdns-sd**} {**query** | **response**}	Not applicable.
ether	Type field in Ethernet II packet: **1536** - **65535**	**1**- **16**
icmptype	ICMP Type: **a.b**	**1**- **16**
Destination or Source IP Address: **ipdestsocket** **ipsourcesocket**	IP Address in dotted decimal format: **000.000.000.000** and (Optional) post-fixed port: **0** - **65535**	**1** - **48**
ipfrag	Not applicable.	Not applicable.
ipproto	Protocol field in IP packet: **0** - **255**	**1**- **8**
iptos	Type of Service field in IP packet: **0** - **255**	**1**- **8**
ipttl	Time-to-live (TTL) in IP packet: **0** - **255**	**1** - **8**

Table 43-3 Valid Values for Policy Classification Rules (continued)

Classification Rule Parameter	*data* value	*mask* bits
ipxclass	Transmission control (Class of Service) field in IPX: **0** - **255**	**1**- **8**
Destination or Source IPX Network: **ipxdest** **ipxsource**	IPX Address: **0** - **0xffffffff**	**1** - **32**
Destination or Source IPX Socket: **ipxdestsocket** **ipxsourcesocket**	IPX Socket Number: **0 - 65535**	**1** - **16**
ipxtype	IPX packet type field: **0** - **255**	**1** - **8**
llcDsapSsap	DSAP/SSAP/CTRL field in llc: **a-b-c-ab**	**1** - **40**
Destination or Source MAC: **macdest** **macsource**	MAC Address: **00-00-00-00-00-00**	**1** - **48**
port	Port string: Eg. **ge.1.1**	**1** - **16**
tci	Tag Control Information: **0 - 65535** or **0xFFFF**	**1** - **16**
Destination or Source TCP port: **tcpdestportip** **tcpsourceportip**	TCP Port Number with optional post-fix IP address: **ab[:c.d.e.f] 0-65535:1.1.1.1;** or **0-0xFFFF:1.1.1.1**	**1** - **48**
Destination or Source UDP port: **udpsourceportip** **udpdestportip**	UDP Port Number with optional post-fix IP address: **ab[:c.d.e.f] 0-65535:1.1.1.1;** or **0-0xFFFF:1.1.1.1**	**1** - **48**
vlantag	VLAN tag: **1**- **4094**	**1** -**12**

clear policy rule

Use this command to delete one or all policy classification rule entries.

Syntax

clear policy rule {**admin-profile** | *profile-index*} **all-pid-entries** | **application** | **ether** | **icmptype** | **ip6dest** | **ip6source** | **ipfrag** | **ipproto** | **ipdestsocket** | **ipsourcesocket** | **iptos** | **ipttl** | **ipxclass** | **ipxdest** | **ipxsource** | **ipxdestsocket** | **ipxsourcesocket** | **ipxtype** | **llcDsapSsap** | **macdest** | **macsource** | **tci** | **port** | **tcpdestportip** | **tcpsourceportip** | **udpdestportip** | **udpsourceportip** | **vlantag**] [**all-traffic-entries** | *data*][**mask** *mask*] [**port-string** *port-string*]

Parameters

admin-profile | *profile-index*	Deletes an administrative profile rule, or deletes rule(s) associated with a specific profile number. Valid *profile-index* values are **1** - **1023**.
all-pid-entries	Deletes all rules associated with the specified policy profile index ID.
application	Deletes associated application policy.
ether	Deletes associated Ethernet II classification rule.

icmptype	Deletes associated ICMP classification rule.
ipdest	Deletes associated IP destination classification rule.
ipsource	Deletes associated IP source classification rule.
ipfrag	Deletes associated IP fragmentation classification rule.
ipproto	Deletes associated IP protocol classification rule.
ipdestsocket	Deletes associated IP destination with optional post-fixed port classification rule.
ipsourcesocket	Deletes associated IP source with optional post-fixed port classification rule.
iptos	Deletes associated IP Type of Service classification rule.
ipttl	Deletes associated IP Time-to-Live (TTL) classification rule.
ipxclass	Deletes associated IPX transmission control classification rule.
ipxdest	Deletes associated IPX destination address classification rule.
ipxsource	Deletes associated IPX source address classification rule.
ipxdestsocket	Deletes associated IPX destination socket classification rule.
ipxsourcesocket	Deletes associated IPX source socket classification rule.
ipxtype	Deletes associated IPX packet type classification rule.
llcDsapSsap	Deletes associated DSAP/SSAP classification rule.
macdest	Deletes associated MAC destination address classification rule.
macsource	Deletes associated MAC source address classification rule.
tci	Deletes associated Tag Control Information classification rule.
port	Deletes associated port-string classification rule.
tcpdestport	Deletes associated TCP destination port classification rule.
tcpdestportip	Deletes associated TCP destination port classification rule with optional post-fix IP address.
tcpsourceportip	Deletes associated TCP source port classification rule with optional post-fix IP address.
udpdestportip	Deletes associated UDP destination port classification rule with optional post-fix IP address.
udpsourceportip	Deletes associated UDP source port classification rule with optional post-fix IP address.
vlantag	Deletes associated VLAN tag classification rule.
all-traffic-entries | *data*	(Optional) Deletes all entries associated with this traffic rule or a specific data value entry. Refer to Table 43-3 on page 43-26 for valid values for each classification type.
mask *mask*	(Optional) Deletes associated data mask. Refer to Table 43-3 on page 43-26 for valid values for each classification type and data value.
port-string *port-string*	(Optional) Deletes specified rule entries for the specified ingress port.

Defaults

When applicable, *data*, *mask*, and *port-string* must be specified for individual rules to be cleared.

Mode

All command modes.

Example

This example shows how to delete all classification rule entries associated with policy profile 1 from all ports:

```
S Chassis(rw)->clear policy rule 1 all-pid-entries
```

clear policy all-rules

Use this command to remove all admin and classification rules.

Syntax

clear policy all-rules

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to remove all administrative and classification rules:

```
S Chassis(rw)->clear policy all-rules
```

show policy accounting

Use this command to display the status of policy accounting.

Syntax

show policy accounting

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the status of policy accounting:

```
S Chassis(rw)->show policy accounting
Accounting Enable control status is ENABLED
```

set policy accounting

Use this command to enable or disable policy accounting, which controls the collection of classification rule statistics. This function is enabled by default.

Syntax

set policy accounting {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables the policy accounting function.

Defaults

None.

Mode

All command modes.

Usage

Use the **port-hit** option of the show policy rule command on page 43-17 to display classification rule hits that are collected when policy accounting is enabled.

Example

This example shows how to disable policy accounting:

```
S Chassis(rw)->set policy accounting disable
```

clear policy accounting

Use this command to restore policy accounting to its default state of enabled.

Syntax

clear policy accounting

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to re-enable policy accounting:

```
S Chassis(rw)->clear policy accounting
```

set policy port

Use this command to assign an administrative rule to a port.

Syntax

set policy port *port-name admin-id*

Parameters

port-name	Specifies the port(s) on which to set assign an administrative rule.
admin-id	Specify a policy profile index number with a valid range of 1 - 1023.

Defaults

None.

Mode

All command modes.

Example

This example shows how to assign an administrative rule with an index of 20 to port ge.1.3:

```
S Chassis(rw)->set policy port ge.1.3 20
```

show policy allowed-type

Use this command to display a list of currently supported traffic rules applied to the administrative profile for one or more ports.

Syntax

show policy allowed-type *port-string* [**-verbose**]

Parameters

port-string	Specifies port(s) for which to display traffic rules.
-verbose	(Optional) Displays detailed information.

Defaults

If **-verbose** is not specified, summary information will be displayed.

Mode

All command modes.

Usage

The **show policy allowed-type** command output displays traffic rule types in attribute ID order (1 - 31) from left to right. Traffic rule type precedence defaults to the attribute ID order. See the "Traffic Classification Based Policy Capabilities" table in the "Policy Configuration" chapter of the *Extreme Networks S-Series Configuration Guide* for a listing and description of each traffic classification type. Traffic rule type precedence can be changed using the **precedence** option of the set policy profile command on page 43-4. The current precedence attribute ID order can be displayed using the show policy profile command on page 43-2.

The **show policy allowed-type** command specifies two categories of traffic rule type: supported and allowed. Supported indicates whether the specified port supports the traffic rule type. Allowed is an administrative function. By default, all supported traffic rule types are allowed on the port. Traffic rule types for a port can be disallowed using "set policy allowed-type" on page 43-33.

Example

This example:

- Disallows traffic rule index **7** (IPX CoS) on port **ge.3.1** using the **set policy allowed-type** command
- Displays the allowed traffic rule types for port **ge.3.1** (index **7** is now supported but no longer allowed)
- Allows traffic rule type index **7** on port **ge.3.1**
- Displays the allowed traffic types for port **ge.3.1** (index **7** is now both supported and allowed)

```
S Chassis(rw)->set policy allowed-type ge.3.1 traffic-rule 7 clear
S Chassis(rw)->show policy allowed-type ge.3.1

                SUPPORTED AND ALLOWED TRAFFIC RULE TYPES

 o Means Traffic Rule Type is supported on this bridge port
 * Means Traffic Rule Type is supported and allowed on this bridge port

================================================================================
|              |   TRAFFIC  RULE  TYPES                                      |E|
|              |---+-----------+-----+-----+---+---+-+-----+-+---+---+--+|g|
|              |   |           |     |     |   |   | |     | |   |   | | |r|
|              |MAC|   IPX     |IPv6 | IP  |UDP|TCP| | IP  | |   |   |A| |e|
|              |   |           |     |     |   |   | |     |I|   |   |P| |s|
|              |   |    S D    |     |     |   |   | |     |C|E  |   |P| |s|
|              |   |    S S   T|    F|    F|   |   |I|    T|M|N  |V  |L|P| |
|              |S D|S D O O C Y|S D L|S D R|S D|S D|C|T T Y|P|E L|L T|I|O|E|
|              |R S|R S C C O P|R S O|R S A|R S|R S|M|T O P|v|T L|A C|C|R|n|
|              |C T|C T K K S E|C T W|C T G|C T|C T|P|L S E|6|2 C|N I|.|T|a|
|              |---+-----------+-----+-----+---+---+-+-----+-+---+---+-+-|b|
|              |   |           |  1 1|1 1 1|1 1|1 1|1|2 2 2|2|2 2|2 2|2|3|l|
|     Port     |1 2|3 4 5 6 7 8|9 0 1|2 3 4|5 6|7 8|9|0 1 2|3|5 6|7 8|9|1|e|
================================================================================
| ge.3.1       |* *|* * * * o *|* * *|* * *|* *|* *|*|* * *|*|* *|* *|*|*| |
```

```
S Chassis(rw)->set policy allowed-type ge.3.1 traffic-rule 7 append
S Chassis(rw)->>show policy allowed-type ge.3.1

                SUPPORTED AND ALLOWED TRAFFIC RULE TYPES

 o Means Traffic Rule Type is supported on this bridge port
 * Means Traffic Rule Type is supported and allowed on this bridge port

================================================================================
|               |   TRAFFIC  RULE  TYPES                                      |E|
|               |---+-----------+-----+-----+---+---+-+-----+-+---+---+--+|g|
|               |   |           |     |     |   |   | |     | |   |   | | |r|
|               |MAC|   IPX     |IPv6 | IP  |UDP|TCP| | IP  | |   |   |A| |e|
|               |   |           |     |     |   |   | |     |I|   |   |P| |s|
|               |   |    S D    |     |     |   |   | |     |C|E  |   |P| |s|
|               |   |    S S   T|    F|    F|   |   |I|    T|M|N  |V  |L|P| |
|               |S D|S D O O C Y|S D L|S D R|S D|S D|C|T T Y|P|E L|L T|I|O|E|
|               |R S|R S C C O P|R S O|R S A|R S|R S|M|T O P|v|T L|A C|C|R|n|
|               |C T|C T K K S E|C T W|C T G|C T|C T|P|L S E|6|2 C|N I|.|T|a|
|               |---+-----------+-----+-----+---+---+-+-----+-+---+---+-+-|b|
|               |   |           |  1 1|1 1 1|1 1|1 1|1|2 2 2|2|2 2|2 2|2|3|l|
|     Port      |1 2|3 4 5 6 7 8|9 0 1|2 3 4|5 6|7 8|9|0 1 2|3|5 6|7 8|9|1|e|
================================================================================
| ge.1.1        |* *|* * * * * *|* * *|* * *|* *|* *|*|* * *|*|* *|* *|*|*|*| |S
Chassis(rw)->
```

set policy allowed-type

Use this command to assign a list of traffic rules that can be applied to the admin profile for one or more ports.

Syntax

set policy allowed-type *port-string* **traffic-rule** *rule-list* [**append** | **clear**]

Parameters

port-string	Specifies port(s) on which to apply traffic rules.
traffic-rule *rule-list*	Specifies traffic rules to be allowed. This is a numeric value displayed in the **show policy allowed-type** output ("show policy allowed-type" on page 43-31). Entering "none" means that no traffic rules will be allowed on this port.
append | **clear**	(Optional) Appends traffic rule(s) to the port(s) current rules, or clears specified rules.

Defaults

If **append** or **clear** is not specified, rule(s) will be appended to the port's current list.

Mode

All command modes.

Usage

Each port supports a set of traffic rule types. Supported traffic rule types for a given port can also be administratively allowed or disallowed. The **set policy allowed-type** command allows you to either disallow (clear) or allow traffic rule types for the specified port(s). When allowing traffic rule types, all traffic types not specified are cleared unless the **append** option is specified. The **append** option allows the specified traffic types, leaving all unspecified traffic types unchanged.

Clearing allowed traffic types using the **set policy allowed-type clear** command, disallows only the specified traffic types, leaving all unspecified traffic types unchanged.

The **show policy allowed-type** command output displays supported traffic rule types and whether a traffic type is allowed for the specified port

Examples

This example:

- Only allows traffic rule types 1 and 2 (source and destination MAC address classification) to be applied to the admin profile for port ge.3.5
- Displays the new traffic rule allowed types setting

```
S Chassis(rw)->set policy allowed-type ge.3.5 traffic-rule 1-2
S Chassis(rw)->show policy allowed-type ge.3.5
              SUPPORTED AND ALLOWED TRAFFIC RULE TYPES
 o Means Traffic Rule Type is supported on this bridge port
 * Means Traffic Rule Type is supported and allowed on this bridge port
=========================================================================
|              |   TRAFFIC  RULE  TYPES                                  |
+--------------+---+-----------+-----+-----+---+---+-+-----+---+---+-+-+
|              |   |           |     |     |   |   | |     |   |   | | |
|              |MAC|   IPX     |IPv6 | IP  |UDP|TCP| | IP  |   |   | | |
|              |   |           |     |     |   |   | |     |   |   | | |
|              |   |    S D    |     |     |   |   | |     |E  |   | | |
|              |   |    S S   T|    F|    F|   |   |I|    T|N  |V  |P|
|              |S D|S D O O C Y|S D L|S D R|S D|S D|C|T T Y|E L|L T|O|
|              |R S|R S C C O P|R S O|C S A|R S|R S|M|T O P|T L|A C|R|
|              |C T|C T K K S E|C T W|R T G|C T|C T|P|L S E|2 C|N I|T|
|              |---+-----------+-----+-----+---+---+-+-----+---+---+-+-+
|              |   |           |  1 1|1 1 1|1 1|1 1|1|2 2 2|2 2|2 2|3|
|     Port     |1 2|3 4 5 6 7 8|9 0 1|2 3 4|5 6|7 8|9|0 1 2|5 6|7 8|1|
=========================================================================
| ge.3.5       |* *|o o o o o o|     |o o o|o o|o o|o|  o o|o o|o o|o|
```

This example:

- Clears only rule type 27 (VLAN classification) from the allowed rule type list on port ge.3.5. All other rule type configuration on the port is unchanged for the specified port.
- Displays the new traffic rule allowed types setting.

```
S Chassis(rw)->set policy allowed-type ge.3.5 traffic-rule 27 clear
S Chassis(rw)->show policy allowed-type ge.3.5
              SUPPORTED AND ALLOWED TRAFFIC RULE TYPES
 o Means Traffic Rule Type is supported on this bridge port
 * Means Traffic Rule Type is supported and allowed on this bridge port
=========================================================================
|              |   TRAFFIC  RULE  TYPES                                  |
+--------------+---+-----------+-----+-----+---+---+-+-----+---+---+-+
|              |   |           |     |     |   |   | |     |   |   | |
|              |MAC|   IPX     |IPv6 | IP  |UDP|TCP| | IP  |   |   | |
|              |   |           |     |     |   |   | |     |   |   | |
|              |   |    S D    |     |     |   |   | |     |E  |   | |
|              |   |    S S   T|    F|    F|   |   |I|    T|N  |V  |P|
|              |S D|S D O O C Y|S D L|S D R|S D|S D|C|T T Y|E L|L T|O|
|              |R S|R S C C O P|R S O|C S A|R S|R S|M|T O P|T L|A C|R|
|              |C T|C T K K S E|C T W|R T G|C T|C T|P|L S E|2 C|N I|T|
|              |---+-----------+-----+-----+---+---+-+-----+---+---+-+
|              |   |           |  1 1|1 1 1|1 1|1 1|1|2 2 2|2 2|2 2|3|
|     Port     |1 2|3 4 5 6 7 8|9 0 1|2 3 4|5 6|7 8|9|0 1 2|5 6|7 8|1|
=========================================================================
| ge.3.5 |* *|* * * * * *|     |* * *|* *|* *|*|  * *|* *|o *|*|
```

clear policy allowed-type

Use this command to clear the list of traffic rules currently assigned to the admin profile for one or more ports. This will reassign the default setting, which is all rules are allowed.

Syntax

clear policy allowed-type *port-string*

Parameters

port-string	Specifies port(s) on which to clear traffic rules.

Defaults

None.

Mode

All command modes.

Usage

This command will reassign the default setting, which is all rules are allowed.

Example

This example shows how to clear the allowed rule list from port ge.1.5:

```
S Chassis(rw)->clear policy allowed-type ge.1.5
```

show policy dropped-notify

Use this command to display a count of the number of times the device has dropped Syslog and/or trap notifications of rule usage on ports.

Syntax

show policy dropped-notify

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to show dropped notify information:

```
S Chassis(rw)->show policy dropped-notify
Dropped notifications: 0
```

show policy disabled-ports

Use this command to display ingress ports disabled by the first use of an associated rule.

Syntax

show policy disabled-ports

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

This command is only in effect if the port disable function has been enabled using the **set policy rule** command as described in "set policy rule" on page 43-23. The **disabled-port** option of the **set policy rule** command provides for disabling a port on first use of the policy rule. There is also a **prohibit** setting for the **disabled-port** option that prohibits lower precedence rules from disabling the ingress port when a rule usage occurs. The current traffic rule precedence can be displayed using "show policy profile" on page 43-2.

Example

This example shows how to display information about ports disabled by the first use of a policy rule. In this case, no ports have been disabled:

```
S Chassis(rw)->show policy disabled-ports
Disabled-ports      :ge.1.2;ge.5.10
S Chassis(rw)->
```

clear policy disabled-ports

Use this command to clear ports from the disabled state that have been disabled due to the first use of a policy rule on those ports.

Syntax

clear policy disabled-ports {**all** | *port-string*}

Parameters

all | *port-string*	Clears all ports or specific port(s) from the disabled state.

Defaults

None.

Mode

All command modes.

Usage

This command is only in effect if the port disable function has been enabled using the **set policy rule** command as described in "set policy rule" on page 43-23. To become active again, disabled ports must also be removed from the policy usage list as described in "clear policy usage-list" on page 43-37.

Example

This example shows how to clear all disabled ports from the disabled state:

```
S Chassis(rw)->clear policy disabled-ports all
```

clear policy usage-list

Use this command to clear usage statistics for ports disabled by first rule usage.

Syntax

clear policy usage-list [**all**] | [**admin-profile**] | *profile-index* {**application** | **ether** | **icmptype** | **ipproto** | **ipdestsocket** | **ipfrag** | **ipsource** | **ipsourcesocket** | **iptos** | **ipxclass** | **ipxdest** | **ipxsource** | **ipxdestsocket** | **ipxsourcesocket** | **ipxtype** | **llcDsapSsap** | **macdest** | **macsource** | **port** | **tci** | **tcpdestport** | **tcpsourceport** | **udpdestport** | **udpsourceport** | **vlantag**} [*data*] [**mask** *mask*] [**port-string** *port-string*] [**port-list** *port-list*]

Parameters

all | **admin-profile** | *profile-index*	Clears all usage statistics, those associated with an administrative profile rule, or those associated with a specific profile rule. Valid *profile-index* values are **1** - **1023**.
application	Clears application rule usage statistics.
ether	Clears Ethernet II rule usage statistics.
icmptype	Clears ICMP rule usage list statistics.
ipproto	Clears IP protocol rule usage statistics.
ipdestsocket	Clears IP destination socket rule usage statistics.
ipfrag	Clears IP fragmentation rule usage statistics.
ipsource	Clears source address rule usage statistics.
ipsourcesocket	Clears source socket rule usage statistics.
iptos	Clears IP Type of Service rule usage statistics.
ipxclass	Clears IPX transmission control rule usage statistics.
ipxdest	Clears IPX destination address rule usage statistics.
ipxsource	Clears IPX source address rule usage statistics.
ipxdestsocket	Clears IPX destination socket rule usage statistics.
ipxsourcesocket	Clears IPX source socket rule usage statistics.
ipxtype	Clears IPX packet type rule usage statistics.
llcDsapSsap	Clears DSAP/SSAP rule usage statistics.
macdest	Clears MAC destination address rule usage statistics.
macsource	Clears MAC source address rule usage statistics.
port	Clears Port rule usage statistics.
tci	Clears Tag Control Information rule usage statistics.
tcpdestport	Clears TCP destination port rule usage statistics.
tcpsourceport	Clears TCP source port rule usage statistics.
udpdestport	Clears UDP destination port rule usage statistics.
udpsourceport	Clears UDP source port rule usage statistics.
vlantag	Clears VLAN tag rule usage statistics.
data	(Optional) Specifies an associated data value entry. Refer to Table 43-3 on page 43-26 for valid values for each classification type.
mask *mask*	(Optional) Specifies an associated data mask. Refer to Table 43-3 on page 43-26 for valid values for each classification type and data value.
port-string *port-string*	(Optional) Specifies rule usage port scope.
port-list *port-string*	(Optional) Specifies disabled port(s) to remove from usage list.

Defaults

- When applicable, *data*, *mask* and *port-string* must be specified for individual rules to be cleared.
- If not specified, all ports will be removed from usage lists.

Mode

All command modes.

Usage

To become active again, disabled ports must also be removed from the policy disabled-ports list as described in “clear policy disabled-ports” on page 43-37.

Example

This example shows how to clear rule usage statistics pertaining to all ports and all classification rules:

```
S Chassis(rw)->clear policy usage-list all
```

show policy autoclear

Use this command to display the status of the policy auto clear function.

Syntax

show policy autoclear {**all** | **link** | **interval** | **profile** | **ports**}

Parameters

all	Displays all auto clear status information.
link	Displays rule usage when a link’s operating status of up is detected.
interval	Displays the interval in minutes at which the device will automatically clear rule usage statistics.
profile	Displays profiles for which rule usage has been cleared when an assigned profile has been activated.
ports	Displays port(s) on which rule usage statistics will be automatically cleared by one of the auto clear actions (link/interval/profile).

Defaults

None.

Mode

All command modes.

Example

This example shows how to display all auto clear status information. In this case, the auto clear function has not been configured:

```
S Chassis(rw)->show policy autoclear all
AutoClear interval is 0 minute(s)
AutoClear on link status is DISABLED
AutoClear on profile status is DISABLED
AutoClear port-list: none
```

set policy autoclear

Use this command to enable or disable the policy rule auto clear function.

Syntax

```
set policy autoclear {[enable | disable] [interval interval] [profile {enable | disable}] [ports port-list [append | clear]]}
```

Parameters

enable | **disable**	Enables or disables autoclear when link (operstatus up) is detected. The default setting is **disable**.
interval *interval*	Specifies the interval in minutes at which the device will automatically clear rule usage statistics. Valid values are **0** - **65535**. Default value is **0**.
profile enable | **disable**	Specifies that rule usage is cleared (**enable**), or not cleared (**disable**), when the profile is activated, if the rule is assigned to that profile. The default setting is **disable**.
ports *port-list*	Specifies port(s) on which rule usage statistics will be automatically cleared by the autoclear actions.
append | **clear**	Appends this port list to the designated port list on which rule usage statistics will be automatically cleared, or removes this port list.

Defaults

None.

Mode

All command modes.

Usage

When enabled, this command clears rule usage information, if operational status “up” is detected on any port.

Use the **show policy rule port-hit** or **show policy rule usage-list** commands to display statistics affected by this command.

Example

This example shows how to clear the rule usage list on all ports for a rule assigned to a profile when the profile is activated:

```
S Chassis(rw)->set policy autoclear profile enable ports ge.*.*
```

clear policy autoclear

Use this command to clear policy rule auto clear settings.

Syntax

```
clear policy autoclear {all | link [interval | profile | ports]}
```

Parameters

all	Clears all auto clear settings .
link	Clears rule usage when a link's operating status of up is detected.
interval	(Optional) Resets the interval setting to the default value of **0** minutes.
profile	(Optional) Resets the profile setting to the default value of **disable**.
ports	(Optional) Clears the assigned port-list.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear all policy auto clear settings:

```
S Chassis(rw)->clear policy autoclear all
```

clear policy port-hit

Use this command to clear rule port hit indications on one or more ports.

Syntax

clear policy port-hit {**all** | **port-list** *port-list*}

Parameters

all | **port-list** *port-list*	Clears port hit indications on all ports or on one or more specified ports.

Defaults

None.

Mode

All command modes.

Usage

Policy rule port-hits are displayed using the **show policy rule port-hit** command.

Example

This example shows how to clear rule port hit indications on all ports:

```
S Chassis(rw)->clear policy port-hit all
```

show policy syslog

Use this command to show the message formatting settings. Messages can be enabled or disabled for both machine-readable and extended-format.

Syntax

```
show policy syslog [machine-readable] [extended-format]
```

Parameters

machine-readable	(Optional) Displays the control for device formatting of rule usage messages. When enabled, the format is machine readable. When disabled, the format is human readable.
extended-format	(Optional) Displays the control for the extended syslog message format. When enabled, additional rule usage information is included in the message format. When disabled, the original rule usage information is included in the message format.

Defaults

If no option is specified, both settings are displayed.

Mode

All command modes.

Example

This example shows how to display the device formatting of rule usage messages:

```
S Chassis(rw)->show policy syslog
Syslog machine-readable: disabled
Syslog extended-format : disabled
```

set policy syslog

Use this command to enable and extended format syslog policy settings.

Syntax

```
set policy syslog [machine-readable {enable | disable}] [extended-format {enable
| disable}]
```

Parameters

machine-readable enable | disable	(Optional) Sets the formatting of rule usage messages. The format is either machine-readable or human-readable. **enable** - Formats the rule usage messages so that they might be processed by a machine (scripting backend, etc.). **disable** - Formats the rule usage messages so that they are human readable.
extended-format enable | disable	(Optional) Sets the control for the extended syslog message format. **enable** - Includes additional information in the rule usage syslog messages. **disable** - Uses the original rule usage syslog message format.

Defaults

If machine-readable enable is not specified, syslog formatting is set to human-readable. If extended-format enable is not specified, syslog standard format is set.

Mode

All command modes.

Usage

The data included in the extended format is VLAN, COS assigned, and the following fields found in the packet:

- DEST MAC
- SRC MAC
- TAG(8100:tci)
- Ether Type
- SIP(ip)
- DIP(ip)
- Protocol
- TOS/DSCP
- Fragmentation indication
- Destination PORT
- Source PORT

Example

This example shows how to set the device formatting of rule usage messages as machine-readable:

```
S Chassis(rw)->set policy syslog machine-readable enable
```

clear policy syslog

Use this command to clear policy syslog and extended-format syslog message settings to the default state.

Syntax

```
clear policy syslog [machine-readable] [extended-format]
```

Parameters

machine-readable	(Optional) Clears the machine-readable formatting of rule usage messages to its default, which is human-readable (disabled).
extended-format	(Optional) Clears the additional information in the rule usage syslog messages to its default, which is the original rule usage syslog message format (disabled).

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear the machine-readable formatting of rule usage messages to the default setting of human-readable:

```
S Chassis(rw)->clear policy syslog machine-readable
```

44

System Logging Commands

The commands in this chapter are used to display and configure system logging, including Syslog server settings, logging severity levels for various applications, Syslog default settings, and the logging buffer. For information about configuring Syslog, refer to the "System Logging Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show logging all	44-1
show logging server	44-4
set logging server	44-5
clear logging server	44-6
show logging default	44-7
set logging default	44-7
clear logging default	44-8
show logging application	44-9
set logging application	44-11
clear logging application	44-14
show logging local	44-14
set logging local	44-15
clear logging local	44-16
set logging here	44-16
clear logging here	44-17
show logging buffer	44-17

show logging all

Use this command to display all configuration information for system logging.

Syntax

```
show logging all
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display all system logging information:

```
S Chassis(rw)->show logging all

        Application   Current Severity Level Server List
-----------------------------------------------------------
  88    RtrAcl                          6      1-8,console,file
  89    CLI                             6      1-8,console,file
  90    SNMP                            6      1-8,console,file
  91    Webview                         6      1-8,console,file
  93    System                          6      1-8,console,file
  95    RtrFe                           6      1-8,console,file
  96    Trace                           6      1-8,console,file
 105    RtrLSNat                        6      1-8,console,file
 111    FlowLimt                        6      1-8,console,file
 112    UPN                             6      1-8,console,file
 117    AAA                             6      1-8,console,file
 118    Router                          6      1-8,console,file
 140    AddrNtfy                        6      1-8,console,file
 141    OSPF                            6      1-8,console,file
 142    VRRP                            6      1-8,console,file
 145    RtrArpProc                      6      1-8,console,file
 147    LACP                            6      1-8,console,file
 148    RtrNat                          6      1-8,console,file
 151    RtrTwcb                         6      1-8,console,file
 154    DbgIpPkt                        6      1-8,console,file
 158    HostDoS                         6      1-8,console,file
 180    RtrMcast                        6      1-8,console,file
 183    PIM                             6      1-8,console,file
 184    DVMRP                           6      1-8,console,file
 185    BGP                             6      1-8,console,file
 196    LinkFlap                        6      1-8,console,file
 199    Spoof                           6      1-8,console,file
 207    IPmcast                         6      1-8,console,file
 209    Spantree                        6      1-8,console,file
 211    trackobj                        6      1-8,console,file
 213    LinkTrap                        6      1-8,console,file
 214    CDP                             6      1-8,console,file
```

```
 215    LLDP                                6      1-8,console,file
 216    CiscoDP                             6      1-8,console,file
 218    OAM                                 6      1-8,console,file
 222    Security                            7      console,sfile
 225    RMON                                6      1-8,console,file
 231    IPsec                               6      1-8,console,file

1(emergencies)  2(alerts)       3(critical)
4(errors)       5(warnings)     6(notifications)
7(information)  8(debugging)


 Server Index: 1
   IP Address: 2001:4000::a00:27ff:fee7:3cd6
   Facility: local4
   Severity: debugging(8)
   Description: default
   Port: 514
   Status: enabled


Defaults:          local4 debugging(8)                          514


Syslog Console Logging disabled

Syslog File Logging enabled

Syslog Secure File Logging enabled
S Chassis(rw)->
```

Table 44-1 provides an explanation of the command output.

Table 44-1 show logging all Output Details

Output...	What it displays...
Application	A mnemonic abbreviation of the textual description for applications being logged.
Current Severity Level	Severity level (**1** - **8**) at which the server is logging messages for the listed application. For details on setting this value using the **set logging application** command, refer to “set logging application” on page 44-11.
Server List	Servers the application is being logged to, as well as console and file type: file = standard logging file; sfile = secure file.
Server Index	Index number of the server for the information that follows.
IP Address	Syslog server’s IP address. For details on setting this using the **set logging server** command, refer to “set logging server” on page 44-5.

Table 44-1 show logging all Output Details (continued)

Output...	What it displays...
Facility	Syslog facility that will be encoded in messages sent to this server. Valid values are: **local0** to **local7**.
Severity	Severity level at which the server is logging messages.
Description	Text string description of this facility/server.
Port	UDP port the client uses to send to the server.
Status	Whether or not this Syslog configuration is currently enabled or disabled.
Defaults	Default facility name, severity level and UDP port designation (as described below.) For details on setting this value using the **set logging defaults** command, refer to “set logging default” on page 44-7.
Syslog Console Logging	Current state for Syslog console logging.
Syslog File Logging	Current state for Syslog file logging.
Syslog Secure File Logging	Current state for Syslog secure file logging.

show logging server

Use this command to display the Syslog configuration for a particular server.

Syntax

show logging server [*index*]

Parameters

index	(Optional) Displays Syslog information pertaining to a specific server table entry. Valid values are **1**-**8**.

Defaults

If *index* is not specified, all Syslog server information will be displayed.

Mode

All command modes.

Example

This example shows how to display Syslog server configuration information. For an explanation of the command output, refer back to Table 44-1.

```
S Chassis(rw)->show logging server

 Server Index: 1
   IP Address: 2001:4000::a00:27ff:fee7:3cd6
   Facility: local4
   Severity: debugging(8)
   Description: default
```

```
   Port: 514
   Status: enabled
S Chassis(rw)->
```

Table 44-2 provides an explanation of the command output.

Table 44-2 show logging server Output Details

Output...	What it displays...
Server Index	Index number of the server for the information that follows.
IP Address	Syslog server's IP address. For details on setting this using the **set logging server** command, refer to "set logging server" on page 44-5.
Facility	Syslog facility that will be encoded in messages sent to this server. Valid values are: **local0** to **local7**.
Severity	Severity level at which the server is logging messages.
Description	Text string description of this facility/server.
Port	UDP port the client uses to send to the server.
Status	Whether or not this Syslog configuration is currently enabled or disabled.

set logging server

Use this command to configure a Syslog server.

Syntax

set logging server *index* [**ip-addr** *ip-addr*] [**facility** *facility*] [**severity** *severity*] [**descr** *descr*] [**port** *port*] [**state** {**enable** | **disable**}]

Parameters

index	Specifies the server table index number for this server. Valid values are **1** - **8**.
ip-addr *ip-addr*	(Optional) Specifies the Syslog message server's IPv4 or IPv6 address.
facility *facility*	(Optional) Specifies the server's facility name. Valid values are: **local0** to **local7.**
severity *severity*	(Optional) Specifies the severity level at which the server will log messages. Valid values and corresponding levels are: 1 - emergencies (system is unusable) 2 - alerts (immediate action required) 3 - critical conditions 4 - error conditions 5 - warning conditions 6 - notifications (significant conditions) 7 - informational messages 8 - debugging messages
descr *descr*	(Optional) Specifies a textual string description of this facility/server.

port *port*	(Optional) Specifies the default UDP port the client uses to send to the server.
state enable | **disable**	(Optional) Enables or disables this facility/server configuration.

Defaults

- If **ip-addr** is not specified, an entry in the Syslog server table will be created with the specified *index* number and a message will display indicating that no IP address has been assigned.
- If not specified, **facility**, severity and port will be set to defaults configured with the **set logging default** command ("set logging default" on page 44-7).
- If port is not specified, the UDP port defaults to 514 unless changed using "set logging default" on page 44-7.
- If **descr** is not specified, no description is configured.
- If **state** is not specified, the server will not be enabled or disabled.

Mode

All command modes.

Usage

If C2 security mode is enabled, You can not create, modify, or clear a server logging configuration while in Read-Write user mode.

Example

This command shows how to enable a Syslog server configuration for index 1, IP address 134.141.89.113, facility local4, severity level 3 on port 514:

```
S Chassis(rw)->set logging server 1 ip-addr 134.141.89.113 facility local4
severity 3 port 514 state enable
```

clear logging server

Use this command to remove a server from the Syslog server table.

Syntax

clear logging server *index*

Parameters

index	Specifies the server table index number for the server to be removed. Valid values are **1** - **8**.

Defaults

None.

Mode

All command modes.

Usage

If C2 security mode is enabled, You can not clear a server logging configuration while in Read-Write user mode.

Example

This command shows how to remove the Syslog server with index 1 from the server table:

```
S Chassis(rw)->clear logging server 1
```

show logging default

Use this command to display the Syslog server default values.

Syntax

show logging default

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This command shows how to display the Syslog server default values. For an explanation of the command output, refer back to Table 44-1.

```
S Chassis(rw)->show logging defaults
                   Facility Severity                          Port
Defaults:          local4 debugging(8)                         514
```

set logging default

Use this command to set logging default values.

Syntax

set logging default {[**facility** *facility*] [**severity** *severity*] [**port** *port*]}

Parameters

facility *facility*	Specifies the default facility name. Valid values are: **local0** to **local7.**

severity *severity*	Specifies the default logging severity level. Valid values and corresponding levels are: 1 - emergencies (system is unusable) 2 - alerts (immediate action required) 3 - critical conditions 4 - error conditions 5 - warning conditions 6 - notifications (significant conditions) 7 - informational messages 8 - debugging messages
port *port*	Specifies the default UDP port the client uses to send to the server.

Defaults

None.

Mode

All command modes.

Usage

If C2 security mode is enabled, You can not create, modify, or clear a default logging configuration while in Read-Write user mode.

Example

This example shows how to set the Syslog default facility name to local2 and the severity level to 4 (error logging):

```
S Chassis(rw)->set logging default facility local2 severity 4
```

clear logging default

Use this command to reset logging default values.

Syntax

```
clear logging default {[facility] [severity] [port]}
```

Parameters

facility	(Optional) Resets the default facility name to **local4.**
severity	(Optional) Resets the default logging severity level to **6** (notifications of significant conditions).
port	(Optional) Resets the default UDP port the client uses to send to the server to **514**.

Defaults

- At least one optional parameter must be entered.
- All three optional keywords must be entered to reset all logging values to defaults.

Mode

All command modes.

Usage

If C2 security mode is enabled, You can not clear a local logging configuration while in Read-Write user mode.

Example

This example shows how to reset the Syslog default severity level to 6:

```
S Chassis(rw)->clear logging default severity
```

show logging application

Use this command to display the severity level of Syslog messages for one or all applications configured for logging on your system.

Syntax

show logging application [*mnemonic* | **all**]

Parameters

mnemonic | **all**	(Optional) Displays severity level for one or all applications configured for logging.

Defaults

If not specified, information for all applications will be displayed.

Mode

All command modes.

Usage

Mnemonics will vary depending on the number and types of applications running on your system. To display a complete list, use the **show logging application** command as described in "show logging application" on page 44-9. Sample values and their corresponding applications are listed in Table 44-4.

Mnemonic values are case sensitive and must be typed as they appear in Table 44-4.

Example

This example shows how to display system logging information pertaining to the all supported applications.

```
S Chassis(su)->show logging application

        Application   Current Severity Level Server List
-----------------------------------------------------------
  88    RtrAcl                          6      1-8,console,file
  89    CLI                             6      1-8,console,file
  90    SNMP                            6      1-8,console,file
  91    Webview                         6      1-8,console,file
  93    System                          6      1-8,console,file
  95    RtrFe                           6      1-8,console,file
  96    Trace                           6      1-8,console,file
 105    RtrLSNat                        6      1-8,console,file
 111    FlowLimt                        6      1-8,console,file
 112    UPN                             6      1-8,console,file
 117    AAA                             6      1-8,console,file
 118    Router                          6      1-8,console,file
 140    AddrNtfy                        6      1-8,console,file
 141    OSPF                            6      1-8,console,file
 142    VRRP                            6      1-8,console,file
 145    RtrArpProc                      6      1-8,console,file
 147    LACP                            6      1-8,console,file
 148    RtrNat                          6      1-8,console,file
 151    RtrTwcb                         6      1-8,console,file
 154    DbgIpPkt                        6      1-8,console,file
 158    HostDoS                         6      1-8,console,file
 180    RtrMcast                        6      1-8,console,file
 183    PIM                             6      1-8,console,file
 184    DVMRP                           6      1-8,console,file
 185    BGP                             6      1-8,console,file
 196    LinkFlap                        6      1-8,console,file
 199    Spoof                           6      1-8,console,file
 207    IPmcast                         6      1-8,console,file
 209    Spantree                        6      1-8,console,file
 211    trackobj                        6      1-8,console,file
 213    LinkTrap                        6      1-8,console,file
 214    CDP                             6      1-8,console,file
 215    LLDP                            6      1-8,console,file
 216    CiscoDP                         6      1-8,console,file
 218    OAM                             6      1-8,console,file
 222    Security                        7      console,sfile
 225    RMON                            6      1-8,console,file
```

```
 226     CFM                                 6       1-8,console,file
 231     IPsec                               6       1-8,console,file

1(emergencies)  2(alerts)       3(critical)
4(errors)       5(warnings)     6(notifications)
7(information)  8(debugging)
```

This example shows how to display system logging information pertaining to the SNMP application.

```
S Chassis(rw)->show logging application snmp ?
  <cr>
S8 Chassis(su)->show logging application snmp

        Application   Current Severity Level Server List
-------------------------------------------------------------
  90    SNMP                                6       1-8,console,file

1(emergencies)  2(alerts)       3(critical)
4(errors)       5(warnings)     6(notifications)
7(information)  8(debugging)
```

Table 44-3 provides an explanation of the command output.

Table 44-3 show logging application Output Details

Output...	What it displays...
Application	A mnemonic abbreviation of the textual description for applications being logged.
Current Severity Level	Severity level at which the server is logging messages for the listed application. This range (from 1 to 8) and its associated severity list is shown in the CLI output. For a description of these entries, which are set using the **set logging application** command, refer to “set logging application” on page 44-11.
Server List	Servers the application is being logged to, as well as console and file type: file = standard logging file; sfile = secure file.

set logging application

Use this command to set the severity level of log messages and the server(s) to which messages will be sent for one or all applications.

Syntax

set logging application {[*mnemonic* | **all**]} [**level** *level*] [**servers** *servers*]

Parameters

mnemonic	Specifies a case sensitive mnemonic abbreviation of an application to be logged. This parameter will vary depending on the number and types of applications running on your system. To display a complete list, use the **show logging application** command as described in "show logging application" on page 44-9. Sample values and their corresponding applications are listed in Table 44-4.
all	Sets the logging severity level for all applications.
level *level*	(Optional) Specifies the severity level at which the server will log messages for applications. Valid values and corresponding levels are: 1. emergencies (system is unusable) 2. alerts (immediate action required) 3. critical conditions 4. error conditions 5. warning conditions 6. notifications (significant conditions) 7. informational messages 8. debugging messages
servers *servers*	(Optional) Specifies the index number(s) of the Syslog server(s) to which messages will be sent. Valid values are **1** - **8** and are set using the command "set logging server" on page 44-5.

Defaults

- If **level** is not specified, none will be applied.
- If **server** is not specified, messages will be sent to all Syslog servers.

Mode

All command modes.

Usage

The security application must be set to a level of 7 and logged to the security file (sfile). See below for an example security application CLI input.

If C2 security mode is enabled, You can not create, modify, or clear a logging application configuration while in Read-Write user mode.

Use "set logging local" on page 44-15 to enable logging to the console, standard logging file, or security logging file.

Mnemonic values are case sensitive and must be typed as they appear in Table 44-4.

Table 44-4 Sample Mnemonic Values for Logging Applications

Mnemonic	Application
AAA	Authentication, Authorization, & Accounting
AddrNtfy	Address Add and Move Notification
BGP	Border Gateway Protocol
CDP	Enterasys Discovery Protocol

Table 44-4 Sample Mnemonic Values for Logging Applications

Mnemonic	Application
CiscoDP	Cisco Discovery Protocol
CLI	Command Line Interface
DbgIpPkt	Debug IP Packet
DVMRP	Distance Vector Multicast Routing Protocol
FlowLimit	Flow Limiting
HostDos	Host DoS
IPmcast	IP Multicast
IPsec	Internet Protocol Security
LACP	Link Aggregation Control Protocol
LinkFlap	Link Flap
Linktrap	Link SNMP Trap
LLDP	Link Layer Discovery Protocol
OAM	Ethernet Operations, Administration, and Maintenance
OSPF	Open Shortest Path First Routing Protocol
PIM	Protocol Independent Multicast
RMON	Remote Monitoring
Router	Router
RtrAcl	Router Access Control List
RtrArpProc	Router Arp Process
RtrFE	Router Forwarding Engine
RtrLSNat	Router Load Sharing Network Address Translation
RtrMcast	Router Multicast
RtrNat	Router Network Address Translation
RtrTwcb	Router Transparent Web Cache Balancing
Security	Security
SNMP	Simple Network Management Protocol
Spantree	Spanning Tree Protocol
Spoof	CheckSpoof
System	Non-Application items such as general blade/chassis/configurations, etc.
Trace	Router Tracing
Trackobj	Track Object Manager
UPN	User Personalized Networking
VRRP	Virtual Router Redundancy Protocol
Webview	Webview Device Management

Examples

This example shows how to set the severity level for SSH (Secure Shell) to 4 so that error conditions will be logged for that application and sent to Syslog server 1:

```
S Chassis(rw)->set logging application SSH level 4 server 1
```

This example shows how to set the security application to send security logging with a severity level of 7 to server 1, the console, and the security logging file:

```
S Chassis(rw)->set logging application security servers 1,console,sfile level 7
```

clear logging application

Use this command to reset the logging severity level for one or all applications to the default value of 6 (notifications of significant conditions).

Syntax

clear logging application {*mnemonic* | **all**}

Parameters

mnemonic | **all**	(Optional) Resets the severity level for a specific application or for all applications. Valid mnemonic values and their corresponding applications are listed in Table 44-4.

Defaults

None.

Mode

All command modes.

Usage

If C2 security mode is enabled, You can not clear a logging application configuration while in Read-Write user mode.

Example

This example shows how to reset the logging severity level for SSH:

```
S Chassis(rw)->clear logging application SSH
```

show logging local

Use this command to display the state of message logging to the console and a persistent file.

Syntax

show logging local

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the state of message logging. In this case, logging to the console is enabled and logging to a persistent file is disabled.

```
S Chassis(rw)->show logging local
Syslog Console Logging disabled
Syslog File Logging enabled
Syslog Secure File Logging enabled
S Chassis(rw)->
```

set logging local

Use this command to configure log messages to the console and a persistent file.

Syntax

set logging local console {**enable** | **disable**} **file** {**enable** | **disable**} **sfile** {**enable** | **disable**}

Parameters

console enable | **disable**	Enables or disables logging to the console. Local console is enabled by default
file enable | **disable**	Enables or disables logging to a persistent file. Logging to a persistent file is disabled by default.
sfile enable | **disable**	Enables or disables logging to a persistent security file. Logging to a persistent security file is disabled by default.

Defaults

None.

Mode

All command modes.

Usage

If C2 security mode is enabled, You can not create, modify, or clear a local logging configuration while in Read-Write user mode.

Example

This command shows how to enable logging to the console and disable logging to standard and security persistent files:

```
S Chassis(rw)->set logging local console enable file disable sfile disable
```

clear logging local

Use this command to reset the console and persistent store logging for the local session to the default value.

Syntax

```
clear logging local
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

If C2 security mode is enabled, You can not clear a local logging configuration while in Read-Write user mode.

Example

This example shows how to clear local logging:

```
S Chassis(rw)->clear logging local
```

set logging here

Use this command to enable or disable the current CLI session as a Syslog destination.

Syntax

```
set logging here {enable | disable}
```

Parameters

enable | **disable**	Enables or disables display of logging messages for the current CLI session.

Defaults

None.

Mode

All command modes.

Usage

The effect of this command will be temporary if the current CLI session is using Telnet or SSH, but persistent on the console.

If C2 security mode is enabled, You can not create, modify, or clear a logging here configuration while in Read-Write user mode.

Example

This command shows how to enable the display of logging messages to the current CLI session:

```
S Chassis(rw)->set logging here enable
```

clear logging here

Use this command to clear the logging state for the current CLI session.

Syntax

clear logging here

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

If C2 security mode is enabled, You can not clear a logging here configuration while in Read-Write user mode.

Example

This command shows how to clear the logging state for the current CLI session:

```
S Chassis(rw)->clear logging here
```

show logging buffer

Use this command to display the last 256 messages logged on all blades.

Syntax

show logging buffer

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

If C2 security mode is enabled, the **show logging buffer** command can not be accessed while in Read-Write or Read-Only user modes.

Example

This example shows a portion of the information displayed with the **show logging buffer** command

```
S Chassis(rw)->show logging buffer
<165>Sep  4 07:43:09 10.42.71.13 CLI[5]User:rw logged in from 10.2.1.122 (telnet)
<165>Sep  4 07:43:24 10.42.71.13 CLI[5]User: debug failed login from 10.4.1.100
(telnet)
```

45

Policy Class of Service (CoS) Commands

This chapter describes the policy Class of Service (CoS) set of commands and how to use them. For information about configuring Quality of Service (QoS), refer to the "Quality of Service (QoS) Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

Note: It is recommended that you use Extreme Networks S-Series as an alternative to CLI for configuring policy-based CoS on the Extreme Networks S-Series devices.

For information about...	Refer to page...
show cos state	45-2
set cos state	45-2
show cos port-type	45-3
show cos unit	45-4
show cos port-config	45-6
set cos port-config irl	45-7
clear cos port-config irl	45-7
set cos port-config txq	45-8
clear cos port-config txq	45-10
set cos port-config flood-ctrl	45-10
clear cos port-config flood-ctrl	45-11
show cos port-resource	45-12
set cos port-resource irl	45-12
clear cos port-resource irl	45-13
set cos port-resource txq	45-14
clear cos port-resource txq	45-15
set cos port-resource flood-ctrl	45-16
clear cos port-resource flood-ctrl	45-17
show cos reference	45-18
set cos reference irl	45-19
clear cos reference irl	45-19
set cos reference txq	45-20

For information about...	Refer to page...
clear cos reference txq	45-20
show cos settings	45-21
set cos settings	45-21
clear cos settings	45-23
show cos violation	45-23
clear cos violation	45-24
clear cos all-entries	45-25

show cos state

Use this command to display the Class of Service enable state.

Syntax

show cos state

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to show the Class of Service enable state:

```
S Chassis(rw)->show cos state
Class-of-Service application is enabled
```

set cos state

Use this command to enable or disable Class of Service.

Syntax

set cos state {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables Class of Service. Class of Service is disable by default.

Defaults

None.

Mode

All command modes.

Example

This example shows how to enable Class of Service:

```
S Chassis(rw)->set cos state enable
```

show cos port-type

Use this command to display Class of Service port type configurations.

Syntax

show cos port-type [**irl** | **txq** | **flood-ctrl**] [*index-list*]

Parameters

irl | **txq** | **flood-ctrl**	(Optional) Displays inbound rate limiting, transmit queue, outbound rate limiting, or flood control information.
index-list	(Optional) Displays the specified port-type index-list. Valid values are **0** - **1**. Default: All port-types.

Defaults

If not specified, all rate limiting information for all port types will be displayed.

Mode

All command modes.

Example

This example shows how to display transmit queue Class of Service port type 0 information:

```
S Chassis(rw)->show cos port-type txq 0

Number of resources:              Supported rate types:
 txq = transmit queue(s)           perc  = percentage
 irl = inbound rate limiter(s)     pps   = packets per second
 orl = outbound rate limiter(s)    Kbps  = kilobits per second
 fld = flood rate limiter(s)       Mbps  = megabits per second
                                   Gbps  = gigabits per second
                                   Tbps  = terabits per second

                    Number of
                    slices /
       Port type    Number of  Supported  Eligible           Unselected
Index  description  queues     rate type  ports              ports
-----  -----------  ---------  ---------  -----------------  -----------------
0      S-Series      100/11    perc       ge.4.1-48;         None
       11Q                     Kbps       ge.6.1-48;
```

```
Mbps        ge.8.1-48;
Gbps        ge.8.101-112
```

Table 45-1 provides an explanation of the command output.

Table 45-1 show cos port-type Output Details

Output...	What it displays...
Index	Port type index.
Number of slices / Number of queues	The total number of slices of transmit resources that can be divided among port queues, and the total number of queues available.
Number of limiters	Maximum number of inbound rate limiters configurable for each port type.
Supported rate types	Unit of measure supported by the port type.
Eligible ports	Which device ports meet this port type criteria.
Unselected ports	Which ports have not been assigned user-defined port configuration settings,

show cos unit

Use this command to display Class of Service units of measure information, including rate type, minimum and maximum limits of the port groups, and their respective granularity.

Syntax

show cos unit [**irl** | **txq** | **flood-ctrl**] [**port-type** *index*]

Parameters

irl | **txq** | **flood-ctrl**	(Optional) Displays inbound rate limiting, transmit queue,, or flood control information.
port-type *index*	(Optional) Displays information for a specific port type. Valid values are **0** - 1. Default: All port-types.

Defaults

If not specified, all rate limiting information for all port types and CoS units of measure will be displayed.

Mode

All command modes.

Example

This example shows how to show all CoS unit of measure information:

```
S Chassis(rw)->show cos unit

Type:                           Unit:
 txq = transmit queue            perc  = percentage
 irl = inbound rate limiting     pps   = packets per second
 orl = outbound rate limiting    Kbps  = Kilobits per second
```

```
 fld = flood rate limiting        Mbps  = Megabits per second
                                  Gbps  = Gigabits per second
                                  Tbps  = Terabits per second

Port Type  Type  Unit  Maximum Rate  Minimum Rate  Granularity
---------  ----  ----  ------------  ------------  -----------
0          txq   Gbps  10            1             1
0          txq   Mbps  10000         1             1
0          txq   Kbps  10000000      64            1
0          txq   perc  100           1             1
1          txq   Gbps  10            1             1
1          txq   Mbps  10000         1             1
1          txq   Kbps  10000000      64            1
1          txq   perc  100           1             1

Port Type  Type  Unit  Maximum Rate  Minimum Rate  Granularity
---------  ----  ----  ------------  ------------  -----------
0          irl   Gbps  10            1             1
0          irl   Mbps  10000         1             1
0          irl   Kbps  10000000      8             1
0          irl   pps   10000         1             1
0          irl   perc  100           1             1
1          irl   Gbps  10            1             1
1          irl   Mbps  10000         1             1
1          irl   Kbps  10000000      8             1
1          irl   pps   10000         1             1
1          irl   perc  100           1             1

Port Type  Type  Unit  Maximum Rate  Minimum Rate  Granularity
---------  ----  ----  ------------  ------------  -----------
0          orl   Gbps  10            1             1
0          orl   Mbps  10000         1             1
0          orl   Kbps  10000000      8             1
0          orl   pps   10000         1             1
0          orl   perc  100           1             1
1          orl   Gbps  10            1             1
1          orl   Mbps  10000         1             1
1          orl   Kbps  10000000      8             1
1          orl   pps   10000         1             1
1          orl   perc  100           1             1

Port Type  Type  Unit  Maximum Rate  Minimum Rate  Granularity
---------  ----  ----  ------------  ------------  -----------
0          fld   Gbps  1             1             1
0          fld   Mbps  1000          1             1
```

```
0          fld   Kbps  100000        8             1
0          fld   pps   10000         1             1
0          fld   perc  100           1             1
```

show cos port-config

Use this command to display Class of Service port group configurations.

Syntax

show cos port-config [**irl** | **txq** | **flood-ctrl**] [*group-type-index*]

Parameters

irl | **txq** | **orl** | **flood-ctrl**	(Optional) Displays inbound rate limiting, transmit queue, or flood control information.
group-type-index	(Optional) Displays information for a specific port group-type index. Valid entries are in the form of **group.type**. Group can be 0 - 11, with 0 designating the default group, and 1 - 11 reserved for user-defined groups. Port type can be 0 - 1.

Defaults

If not specified, all rate limiting information for all port types will be displayed.

Mode

All command modes.

Example

This example shows how to show the transmit queue Class of Service port group 0.0 configuration information:

```
S Chassis(rw)->show cos port-config txq 0.0

 * Percentage/queue (if any) are approximations based on
   [(slices/queue) / total number of slices]

Transmit Queue Port Configuration Entries
--------------------------------------------------------------------------
Port Group Name  :S-Series 11Q
Port Group       :0
Port Type        :0
Assigned Ports   :none
Arbiter Mode     :Low Latency Queue
Slices/queue     :Q [0]: LLQ  Q [1]:   0  Q [2]:   0  Q [3]:   0
                 :Q [4]:   0  Q [5]:   0  Q [6]:   0  Q [7]:   0
                 :Q [8]: 100  Q [9]: LLQ  Q [10]: LLQ
Percentage/queue :Q [0]: LLQ  Q [1]:   0% Q [2]:   0% Q [3]:   0%
                 :Q [4]:   0% Q [5]:   0% Q [6]:   0% Q [7]:   0%
                 :Q [8]: 100% Q [9]: LLQ  Q [10]: LLQ
```

```
--------------------------------------------------------------------------
```

set cos port-config irl

Use this command to set the Class of Service inbound rate limiting port group configuration.

Syntax

set cos port-config irl *group-type-index* [**name** *name*] [**ports** *port-list*] [**append** | **clear**]

Parameters

group-type-index	(Optional) Displays information for a specific port group-type index. Valid entries are in the form of **group.type**. Group can be 0 - 11, with 0 designating the default group, and 1 - 11 reserved for user-defined groups. Port type can be 0 - 1.
name *name*	(Optional) Specifies a name for this configuration.
ports *port-list*	(Optional) Applies this configuration to one or more ports in the port group.
append | **clear**	(Optional) Appends or clears port designations from a previously configured port group.

Defaults

- If a **name** is not specified, no name is assigned to the configuration.
- If the **ports** option is not specified, this configuration will be applied to all ports in the port group.
- If **append** or **clear** are not specified, port(s) will be appended to the specified port grouping.

Mode

All command modes.

Example

This example shows how to create a CoS inbound rate limiting port group entry named **testirl** with a port group ID of **1** and a port type ID of **1**:

```
S Chassis(rw)->set cos port-config irl 1.1 name testirl
```

clear cos port-config irl

Use this command to clear a non-default Class of Service inbound rate limiting port group configuration.

Syntax

clear cos port-config irl {**all** | *group-type-index*} {[**entry**] | [**name**] | [**ports**]}

Parameters

all | *group-type-index*	Clears all inbound rate limiting non-default configurations, or those for a specific user-defined port group index. Valid port group-type index entries are in the form of **group.type**. Group can be 0 - 11, with 0 designating the default group, and 1 - 11 reserved for user-defined groups. Port type can be 0 - 1.
entry | **name** | **ports**	Deletes a specific entry or name, or clears the ports assigned to this inbound rate limiting configuration.

Defaults

None.

Mode

All command modes.

Example

This example shows how to delete the CoS inbound rate limiting port group entry **1.1**:

```
S Chassis(rw)->clear cos port-config irl 1.1 entry
```

set cos port-config txq

Use this command to set the Class of Service transmit queue port group configuration.

Syntax

set cos port-config txq *group-type-index* [**name** *name*] [**ports** *port-list*] [**append** | **clear**] [**arb-slice** *slice-list*] [**arb-percentage** *percentage-list*] [**enhanced-groups** *group-id*] [**enhanced-percentage** *bandwidth*]

Parameters

group-type-index	(Optional) Displays information for a specific port group-type index. Valid entries are in the form of **group.type**. Group can be 0 - 11, with 0 designating the default group, and 1 - 11 reserved for user-defined groups. Port type can be 0 - 1.
name *name*	(Optional) Specifies a name for this configuration.
ports *port-list*	(Optional) Applies this configuration to one or more ports in the port group.
append | **clear**	(Optional) Appends or clears port designations from a previously configured port group.
arb-slice *slice-list*	(Optional) The number of slices of transmit resources allocated to each queue of a port. Input is in the format of x0,x1,x2,...,xn.
arb-percentage *percentage-list*	(Optional) The percentage of slices of transmit resources allocated to each queue of a port. Input is in the format of x0,x1,x2,...,xn.
enhanced-groups *group-id*	(Optional) The enhanced transmission selection groups assigned to port transmit queues.
enhanced-percentage *bandwidth*	(Optional) The amount of bandwidth assigned to the enhanced transmission selection queue group

Defaults

- If a **name** is not specified, no name will be applied.
- If not specified, this configuration will be applied to all ports in the port group.
- If **append** or **clear** are not specified, port(s) will be appended to the specified port grouping.
- If **arb-slice** or **arb-percentage** values are not specified, default allocations will be applied.
- If **enhanced-groups** is specified, the group ID or 0 must be specified.
- If **enhanced-percentage** is specified, a bandwidth percentage must be specified for each enhanced group or 0 is no enhanced group is configured using the **enhanced-groups** option

Mode

All command modes.

Usage

Enhanced Transmission Selection (ETS) queuing provides for the designation of two or more traffic class queues (0 - 7) to be allocated for bandwidth that will not be serviced until all non-ETS queues are empty.

Use the **enhanced-groups** option to specify the group ID of the ETS queue. Each queue is specified, delineated by a comma (,), with either a group ID or 0 for a non-ETS queue. The S-Series supports the configuration of up to eight ETS groups.

Use the **enhanced-percentage** option to specify the percentage of bandwidth to be applied to the ETS group (traffic class). Aggregate ETS bandwidth must total 100%. A value is specified for each traffic class 0 - 7 delineated by a comma (,) as either a bandwidth percentage for any traffic class configured for ETS queuing or 0 for non-ETS traffic classes.

See the Data Center Bridging chapter of the *Extreme Networks S-Series Configuration Guide* for ETS configuration details.

Examples

This example shows how to create a CoS transmit queue port group entry named **testTxq** with a port group ID of **2** and a port type ID of **0**:

```
S Chassis(rw)->set cos port-config txq 2.0 name "testTxq"
```

This example assigns ETS groups to an 11 queue device, followed by allocation of ETS bandwidth to the assigned groups. Using the **enhanced-groups** option, ETS group to queue assignment is:

- Group **2** to queues **0**, **1**, and **2**
- Group **4** to queues **3** and **4**

Using the **enhanced-percentage** option the assigned ETS bandwidth allocation is:

- **30** percent to group **2**
- **70** percent to group **4**

```
S Chassis(rw)->set cos port-config txq 2.1 name testTxq enhanced-groups
2,2,2,4,4,0,0,0,0,0,0,0 enhanced-percentage 0,30,0,70,0,0,0,0
```

clear cos port-config txq

Use this command to clear one or all non-default Class of Service transmit queue port group configurations.

Syntax

clear cos port-config txq {**all** | *group-type-index*} {**entry** | **name** | **ports arb-slice** | **arb-percentage** | **enhanced-groups** | **enhanced-percentage**}

Parameters

all | *group-type-index*	Clears all transmit queue port config entries or a specific entry. Valid port group-type entries are in the form of **group.type**. Group can be 0 - 11, with 0 designating the default group, and 1 - 11 reserved for user-defined groups. Port type can be 0 - 1.
entry	Clears all non-default transmit queue entries.
name	Clears the name associated with this transmit queue entry.
ports	Clears the port(s) assigned to this port group.
arb-slice	Clears the number of slices setting.
arb-percentage	Clears the percentage of slices setting.
enhanced-groups	Clears the enhanced group for this index.
enhanced-percentage	Clears the enhanced bandwidth percentage for this index.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear all non-default CoS transmit queue port group entries:

```
S Chassis(rw)->clear cos port-config txq all
```

set cos port-config flood-ctrl

Use this command to set the Class of Service flood control port group configuration.

Syntax

set cos port-config flood-ctrl *group-type-index* [**name** *name*] [**ports** *port-list*] [**append** | **clear**]

Parameters

group-type-index	Specifies a port group-type index. Valid entries are in the form of **group.type**. Group can be 0 - 11, with 0 designating the default group, and 1 - 11 reserved for user-defined groups. Port type can be 0 - 1.
name *name*	(Optional) Specifies a name for this configuration.

ports *port-list*	(Optional) Applies this configuration to one or more ports in the port group.
append | **clear**	(Optional) Appends or clears port designations from a previously configured port group.

Defaults

- If a **name** is not specified, no name will be applied.
- If a port is not specified, this configuration will be applied to all ports in the port group.
- If **append** or **clear** is not specified, port designations are appended.

Mode

All command modes.

Usage

CoS-based flood control prevents configured ports from being disrupted by a traffic storm by rate limiting specific types of packets through those ports. When flood control is enabled on a port, incoming traffic is monitored over one second intervals. During an interval, the incoming traffic rate for each configured traffic type (unicast, broadcast, multicast) is compared with the configured traffic flood control rate, specified in packets per second. If, during a one second interval, the incoming traffic of a configured type reaches the traffic flood control rate configured on the port, CoS-based flood control drops the traffic until the interval ends. Packets are then allowed to flow again until the limit is again reached.

Example

This example shows how to create a CoS flood control port group entry named **flood1** with a port group ID of **2** and a port type ID of **1**:

```
S Chassis(rw)->set cos port-config flood-ctrl 2.1 name flood1
```

clear cos port-config flood-ctrl

Use this command to clear one or all non-default Class of Service flood control port group configurations.

Syntax

clear cos port-config flood-ctrl {**all** | *group-type-index*} **entry**

Parameters

all | *group-type-index*	Clears all flood control port config entries or a specific entry. Valid port group-type entries are in the form of **group.type**. Group can be 0 - 11, with 0 designating the default group, and 1 - 11 reserved for user-defined groups. Port type can be 0 - 1.
entry	Clears all non-default flood control entries.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear all non-default CoS flood control port group entries:

```
S Chassis(rw)->clear cos port-config flood-ctrl all
```

show cos port-resource

Use this command to display Class of Service port resource configuration information.

Syntax

show cos port-resource [**irl** | **txq** | **flood-ctrl**] *group-type-index* [*resource*] [**violators**]

Parameters

irl | **txq** | **flood-ctrl**	(Optional) Displays inbound rate limiting, transmit queue, or flood control information.
group-type-index	(Optional) Displays information for a specific port group-type index. Valid entries are in the form of **group.type**. Group can be 0 - 11, with 0 designating the default group, and 1 - 11 reserved for user-defined groups. Port type can be 0 - 1.
resource	(Optional) Displays rate limiters, transmit queues, or flood-ctrl resources associated with this entry as a single or range of resources.
violators	(Optional) Displays ports that have violated inbound rate limiters.

Defaults

If no options are specified, all rate limiting information for all port types will be displayed.

Mode

All command modes.

Example

This example shows how to show all inbound rate limiting port resource configuration information for port group **0.1**:

```
S Chassis(rw)->show cos port-resource irl 0.1
```

set cos port-resource irl

Use this command to configure a Class of Service inbound rate limiting port resource entry.

Syntax

set cos port-resource irl *group-type-index irl-range* {[**unit** {**percentage** | **pps** | **kbps** | **mbps** | **gbps**}] [**rate** *rate*] [**type** {**drop**}] [**syslog** {**disable** | **enable**}] [**trap** {**disable** | **enable**}] [**disable-port** {**disable** | **enable**}]}

Parameters

group-type-index	Specifies a port group-type index. Valid entries are in the form of **group.type**. Group can be 0 - 11, with 0 designating the default group, and 1 - 11 reserved for user-defined groups. Port type can be 0 - 1.
irl-range	Specifies a single or a range of inbound rate limiter ID(s) to be associated with this entry.
unit percentage | **pps** | **kbps** | **mbps** | **gbps**	Specifies the unit of measure as percentage of total bandwidth, or packets per second kilobits, megabits, or gigabits per second.
rate *rate*	(Optional) Data rate in units for this inbound rate limiter.
type drop	(Optional) Specifies that frames exceeding this limiter will be dropped.
syslog disable | **enable**	(Optional) Enables or disables the generation of a Syslog message when this limiter is exceeded.
trap disable | **enable**	(Optional) Enables or disables the sending of an SNMP trap message when this limiter is exceeded.
disable-port disable | **enable**	(Optional) Enables or disables the disabling of the violating port when this limiter is exceeded.

Defaults

- If a **rate** is not specified, port defaults will be applied.
- If not specified, frames will not be dropped.
- If not specified, Syslog and port disabling will not be configured.

Mode

All command modes.

Example

This example shows how to configure Class of Service port resource IRL entry **0** for port group **0.0** assigning an inbound rate limit of **512** kilobits per second. This entry will trigger a Syslog and an SNMP trap message if this rate is exceeded:

```
S Chassis(rw)->set cos port-resource irl 0.0 0 unit kbps 512 syslog enable trap
enable
```

clear cos port-resource irl

Use this command to clear one or all Class of Service inbound rate limiting port resource configurations.

Syntax

clear cos port-resource irl {**all** | *group-type-index resource*} [**unit**] [**rate**] [**type**] [**syslog**] [**trap**] [**disable-port**] [**violators** *port-list*]

Parameters

all | *group-type-index*	Clears all inbound rate limiting port resource entries or a specific entry. Valid group-type entries are in the form of **group.type**. Group can be 0 - 11, with 0 designating the default group, and 1 - 11 reserved for user-defined groups. Port type can be 0 - 1.
resource	Specifies a single or range of resource entries to be cleared.
unit	(Optional) Clears the unit of measure setting.
rate	(Optional) Clears the data rate setting.
type	(Optional) Clears the type of action setting.
syslog	(Optional) Clears the Syslog setting.
trap	(Optional) Clears the SNMP trap setting.
disable-port	(Optional) Clears the disable port setting.
violators *port-list*	(Optional) Clears the limit violation setting.

Defaults

If no options are specified, all non-default settings will be cleared for the associated rate limiter.

Mode

All command modes.

Example

This example shows how to clear all inbound rate limiting settings associated with port group **0.1**, resource entry 0:

```
S Chassis(rw)->clear cos port-resource irl 0.1 0
```

set cos port-resource txq

Use this command to configure a Class of Service transmit queue port resource entry.

Syntax

set cos port-resource txq *group-type-index transmit-queue* {[**unit** {**percentage** | **kbps** | **mbps** | **gbps**}] [**rate** *rate*] [**algorithm tail-drop**]}

Parameters

group-type-index	Specifies a transmit queue port group-type index for this entry. Valid entries are in the form of **group.type**. Group can be 0 - 11, with 0 designating the default group, and 1 - 11 reserved for user-defined groups. Port type can be 0 - 1.
transmit-queue	Specifies a single or range of transmit queues to be associated with this entry. Valid values are type 0: 0-10; type 1: 0 - 14.
unit percentage | **kbps** | **mbps** | **gbps**	Specifies the unit of measure as percentage of total bandwidth, or kilobits, megabits, or gigabits per second.
rate *rate*	(Optional) Specifies a data rate in units for this transmit queue.
algorithm tail-drop	(Optional) Sets the algorithm by which transmit frames are discarded from the tail of the queue.

Defaults

- If a **rate** is not specified, port defaults will be applied.
- If not specified, no algorithm will be assigned.

Mode

All command modes.

Example

This example shows how to configure a Class of Service port resource entry for port group **0.1** assigning **50** percent of the total available inbound bandwidth to transmit queue **7**:

```
S Chassis(rw)->set cos port-resource txq 0.1 7 unit percentage 50
```

clear cos port-resource txq

Use this command to clear one or all Class of Service transmit queue port resource entry.

Syntax

clear cos port-resource txq {**all** | *group-type-index resource*} [**unit**] [**rate**] [**algorithm**]

Parameters

all | *group-type-index*	Clears all transmit queue port resource entries or a specific entry. Valid group-type entries are in the form of **group.type**. Group can be 0 - 11, with 0 designating the default group, and 1 - 11 reserved for user-defined groups. Port type can be 0 - 1.
resource	Specifies a single or range resource entries to be cleared.
unit	(Optional) Clears unit of measure settings.
rate	(Optional) Clears rate settings.
algorithm	(Optional) Clears the taildrop algorithm setting.

Defaults

If no options are specified, all associated non-default settings will be cleared.

Mode

All command modes.

Example

This example shows how to clear all port resource settings associated with Class of Service transmit queue **1** in port group **0.1**:

```
S Chassis(rw)->clear cos port-resource txq 0.1 1
```

set cos port-resource flood-ctrl

Use this command to configure a Class of Service flood-ctrl resource entry.

Syntax

set cos port-resource flood-ctrl *group-type-index traffic-type* {[**unit** {**percentage** | **pps** | **kbps** | **mbps** | **gbps**}] [**rate** *rate*]] [**syslog** {**disable** | **enable**}] [**trap** {**disable** | **enable**}] [**disable-port** {**disable** | **enable**}]}

Parameters

group-type-index	Specifies an outbound rate limiting port group-type index for this entry. Valid entries are in the form of **group.type**. Group can be 0 - 11, with 0 designating the default group, and 1 - 11 reserved for user-defined groups. Port type can be 0 - 1.
traffic-type	Specifies the traffic type to be limited: • **unknown-unicast** - Specifies that unknown-unicast traffic will be limited • **multicast** - Specifies that multicast traffic will be limited • **broadcast** - Specifies that broadcast traffic will be limited
unit percentage | **pps** | **kbps** | **mbps** | **gbps**	Specifies the unit of measure as percentage of total bandwidth, or packets per second kilobits, megabits, or gigabits per second.
rate *rate*	(Optional) Data rate in units for this outbound rate limiter.
syslog disable | **enable**	(Optional) Enables or disables the generation of a Syslog message when this limiter is exceeded.
trap disable | **enable**	(Optional) Enables or disables the sending of an SNMP trap message when this limiter is exceeded.
disable-port disable | **enable**	(Optional) Enables or disables the disabling of the violating port when this limiter is exceeded.

Defaults

- If a **rate** is not specified, port defaults will be applied.
- If not specified, Syslog, trap, and port disabling are set to disabled.

Mode

All command modes.

Usage

CoS-based flood control prevents configured ports from being disrupted by a traffic storm by rate limiting specific types of packets through those ports. When flood control is enabled on a port, incoming traffic is monitored over one second intervals. During an interval, the incoming traffic rate for each configured traffic type (unicast, broadcast, multicast) is compared with the configured traffic flood control rate, specified in packets per second. If, during a one second interval, the incoming traffic of a configured type reaches the traffic flood control rate configured on the port, CoS-based flood control drops the traffic until the interval ends. Packets are then allowed to flow again until the limit is again reached.

Example

This example shows how to configure Class of Service port resource flood control of multicast traffic for port group **0.1** assigning an outbound rate limit of **512** kilobits per second. This entry will trigger a Syslog and an SNMP trap message if this rate is exceeded:

```
S Chassis(rw)->set cos port-resource flood-ctrl 0.1 multicast unit kbps 512 syslog
enable trap enable
```

clear cos port-resource flood-ctrl

Use this command to clear one or all Class of Service flood control port resource configurations.

Syntax

clear cos port-resource flood-ctrl all | *group-type-index resource* [**unit**] [**rate**] [**type**] [**syslog**] [**trap**] [**disable-port**] [**violators** *port-list*]

Parameters

all | *group-type-index*	Clears all outbound rate limiting port resource entries or a specific entry. Valid entries are in the form of **group.type**. Group can be 0 - 11, with 0 designating the default group, and 1 - 11 reserved for user-defined groups. Port type can be 0 - 1.
resource	Specifies a resource entry to be cleared.
unit	(Optional) Clears the unit of measure setting.
rate	(Optional) Clears the data rate setting.
type	(Optional) Clears the type of action setting.
syslog	(Optional) Clears the Syslog setting.
trap	(Optional) Clears the SNMP trap setting.
disable-port	(Optional) Clears the disable port setting.
violators *port-list*	(Optional) Clears the limit violation setting.

Defaults

If no options are specified, all non-default settings will be cleared for the associated flood control settings.

Mode

All command modes.

Example

This example shows how to clear all flood control settings associated with port group **0.1** and resource entry **0**:

```
S Chassis(rw)->clear cos port-resource flood-ctrl 0.1 0
```

show cos reference

Use this command to display Class of Service port reference information.

Syntax

show cos reference [**irl** | **txq**] *group-type-index* [*reference*]]

Parameters

irl | **txq**	(Optional) Displays inbound rate limiting or transmit queue rate limiting reference information.
group-type-index	(Optional) Displays information for a specific *port group.type* entry. Valid entries are in the form of **group.type**. Group can be 0 - 11, with 0 designating the default group, and 1 - 11 reserved for user-defined groups. Port type can be 0 - 1.
reference	(Optional) Displays information for a specific reference entry.

Defaults

If no options are specified, all reference information for all port types will be displayed.

Mode

All command modes.

Example

This example shows how to show all transmit queue reference configuration information for port group **0.0**:

```
S Chassis(rw)->show cos reference txq 0.0

Group Index Reference Type    Queue
----------- --------- ---- ------------
0.0         0         txq  0
0.0         1         txq  1
0.0         2         txq  2
0.0         3         txq  3
0.0         4         txq  4
0.0         5         txq  5
0.0         6         txq  6
0.0         7         txq  7
0.0         8         txq  8
0.0         9         txq  9
0.0         10        txq  10
0.0         11        txq  11
0.0         12        txq  12
0.0         13        txq  13
0.0         14        txq  14
0.0         15        txq  15
```

set cos reference irl

Use this command to set a Class of Service inbound rate limiting reference configuration.

Syntax

set cos reference irl *group-type-index reference* **rate-limit** *number*

Parameters

group-type-index	Specifies an inbound rate limiting port group-type index for this entry. Valid entries are in the form of **group.type**. Group can be 0 - 11, with 0 designating the default group, and 1 - 11 reserved for user-defined groups. Port type can be 0 - 1.
reference	Specifies a reference number to be associated with this entry.
rate-limit *number*	Specifies a rate limiter resource ID to bind to this entry.

Defaults

None.

Mode

All command modes.

Example

This example shows how to configure inbound rate limiting reference entry **0** for port group **0.1** referencing resources defined by IRL entry **0**:

```
S Chassis(rw)->set cos reference irl 0.1 0 rate-limit 0
```

clear cos reference irl

Use this command to clear one or all Class of Service inbound rate limiting reference configurations.

Syntax

clear cos reference irl {**all** | *group-type-index reference*}

Parameters

all | *group-type-index*	Clears all non-default inbound rate limiting reference entries or a specific entry. Valid group-type entries are in the form of **group.type**. Group can be 0 - 11, with 0 designating the default group, and 1 - 11 reserved for user-defined groups. Port type can be 0 - 1.
reference	Specifies a reference number of the entry to be cleared.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear all Class of Service inbound rate limiting reference entries:

```
S Chassis(rw)->clear cos reference irl all
```

set cos reference txq

Use this command to set a Class of Service transmit queue reference configuration.

Syntax

set cos reference txq *group-type-index reference* **queue** *number*

Parameters

group-type-index	Specifies a transmit queue port group-type index for this entry. Valid entries are in the form of **group.type**. Group can be 0 - 11, with 0 designating the default group, and 1 - 11 reserved for user-defined groups. Port type can be 0 - 1.
reference	Specifies a reference number to be associated with this entry.
queue *number*	Specifies a transmit queue resource ID to bind to this entry.

Defaults

None.

Mode

All command modes.

Example

This example shows how to configure transmit queue reference resource entry **0** for port group **0.1** referencing resources defined by TXQ entry **0**:

```
S Chassis(rw)->set cos reference txq 0.1 0 queue 0
```

clear cos reference txq

Use this command to clear one or all non-default Class of Service transmit queue reference configurations.

Syntax

clear cos reference txq {**all** | *group-type-index reference*}

Parameters

all | *group-type-index*	Clears all non-default transmit queue reference entries or a specific entry. Valid group-type entries are in the form of **group.type**. Group can be 0 - 11, with 0 designating the default group, and 1 - 11 reserved for user-defined groups. Port type can be 0 - 1.
reference	Specifies a reference number of the entry to be cleared.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear all Class of Service transmit queue reference entries:

```
S Chassis(rw)->clear cos reference txq all
```

show cos settings

Use this command to display Class of Service parameters.

Syntax

show cos settings [*cos*]

Parameters

cos	(Optional) Specifies a Class of Service entry to display.

Defaults

If no CoS entry is specified, all CoS entries will be displayed.

Mode

All command modes.

Example

This example shows how to display the CoS settings for CoS entry **0**:

```
S Chassis(rw)->show cos settings 0

 * Means attribute has not been configured

CoS Index  Priority    ToS      TxQ    IRL    ORL    Drop Prec Flood-Ctrl
---------  ----------  -------  -----  -----  -----  --------- ----------
0          0           *        0      *      *      *         Disabled
```

set cos settings

Use this command to configure a Class of Service entry.

Syntax

set cos settings *cos-list* [**priority** *priority*] [**tos-value** *tos-value*] [**txq-reference** *txq-reference*] [**irl-reference** *irl-reference*] [**orl-reference** *orl-reference*] [**drop-precedence** *drop-precedence*] [**flood-ctrl** *flood-ctrl*]

Parameters

cos-list	Specifies a Class of Service entry. Valid values are 0 - 255.
priority *priority*	(Optional) Specifies a CoS priority value. Valid values are **0** - **7**, with 0 being the lowest priority.
tos-value *tos-value*	(Optional) Specifies a Type of Service value with mask in the format of 0 - 255:0 - 255 or 0 - 0xFF:0 - 0xFF.
txq-reference *txq-reference*	(Optional) Specifies the transmit queue associated with this entry. Valid values are 0 - 15.
irl-reference *irl-reference*	(Optional) Specifies the inbound rate limiter associated with this entry. Valid values are 0 - 31.
orl-reference *orl-reference*	(Optional) Specifies the outbound rate limiter associated with this entry. Valid values are 0 - 3 for port type 0 and 0 - 15 for port type 1.
flood-ctrl *flood-ctrl*	(Optional) Specifies the flood rate limiter associated with this entry. Valid values are 0 - 2.
drop-precedence *drop-precedence*	(Optional) Specifies a drop precedence for this entry. Valid values are 0 - 2.

Defaults

If no optional parameters are specified for an already existing CoS, none will be applied. If a new CoS entry is configured with no optional parameters specified, txq-reference is set to **0** and flood-ctrl is set to **disabled**; no other options are applied.

Mode

All command modes.

Usage

By default only CoS entries 0 - 7 are configured. Additional CoS entries may be created by entering a value between 8 - 255 inclusive. If no additional options are specified, the new CoS entry is configured with TxQ set to **0** and flood control set to enabled.

Drop-precedence is a CoS settings option. CoS settings are assigned to a policy rule. In a Flex-Edge context, drop precedence is limited to rules that apply to a single port and specify a traffic classification of either port or macsource. For any packets matching the policy rule, you can assign one of three drop-precedence priority levels:

- Favored - A drop-precedence value of **0** provides a better chance of being passed on for packet processing than traffic categorized as best-effort.
- Best-Effort - A drop-precedence value of **1** provides a best-effort level of priority within the Flex-Edge priority scheme.
- Unfavored - A drop-precedence value of **2** provides a somewhat worse chance of being passed on for packet processing than traffic categorized as best-effort. This is the lowest possible priority setting within the Flex-Edge mechanism.

Example

This example shows how to create CoS entry **10** with a priority value of **3** and bind it to transmit queue reference ID **5**:

```
S Chassis(rw)->set cos settings 10 priority 3 txq-reference 5
```

clear cos settings

Use this command to clear Class of Service entry settings.

Syntax

```
clear cos settings cos-list {[all] | [priority] [tos-value] [txq-reference]
[irl-reference] [flood-ctrl flood-ctrl]}
```

Parameters

cos-list	Specifies a Class of Service entry to clear.
all	(Optional) Clears all settings associated with this entry.
priority	(Optional) Clears the priority value associated with this entry.
tos-value	(Optional) Clears the Type of Service value associated with this entry.
txq-reference	(Optional) Clears the transmit queue reference associated with this entry.
irl-reference	(Optional) Clears the inbound rate limiting reference associated with this entry.
flood-ctrl	(Optional) Clears the flood rate limiter associated with this entry.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear the priority and transmit queue reference values for CoS entry **2**:

```
S Chassis(rw)->clear cos settings 2 priority txq-reference
```

show cos violation

Use this command to display Class of Service violation statistics.

Syntax

```
show cos violation [irl | flood-ctrl] [disabled-ports] | [violation-index]
```

Parameters

irl | **flood-ctrl**	(Optional) Displays inbound rate limiting or flood control violation statistics.
disabled-ports	(Optional) Displays the port(s) that are disabled because of violating an inbound rate limiter.
violation-index	(Optional) Displays information for a specific violation index. Valid entries are in the form of *port-list*:*irl-list*, or ***.*.*:** for all entries.

Defaults

If no options are specified, all violation information will be displayed.

Mode

All command modes.

Example

This example shows how to show any CoS flood control violations:

```
S Chassis(rw)->show cos violation flood-ctrl

             Rate-Limiter        Rate-Limiter  Rate-Limiter
Port         Index         Type  Status        Counter
-----------  ------------  ----  ------------  --------------------
ge.1.1       UnknownUcast  fld   not-violated  0
ge.1.1       Multicast     fld   not-violated  0
ge.1.1       Broadcast     fld   not-violated  0
ge.1.2       UnknownUcast  fld   not-violated  0
ge.1.2       Multicast     fld   not-violated  0
ge.1.2       Broadcast     fld   not-violated  0
ge.1.3       UnknownUcast  fld   not-violated  0
.
.
.
ge.1.60      UnknownUcast  fld   not-violated  0
ge.1.60      Multicast     fld   not-violated  0
ge.1.60      Broadcast     fld   not-violated  0
```

clear cos violation

Use this command to clear Class of Service violation statistics.

Syntax

clear cos violation {**irl** | **flood-ctrl**} {**all** | **disabled-ports** *port-list* | *violation-index*} {**both** | **status** | **counter**}

Parameters

irl | **flood-ctrl**	Specifies the type of limiter statistics to clear: • **irl** – inbound rate limiter • **flood-ctrl** – flood control
all	Clears all limiting violation entries for the specified limiter.
disabled-ports *port-list*	Clears the list of ports that are disabled because of violating the specified rate limiter.
violation-index	Clears the entry for a specific violation index.
both | **status** | **counter**	Clears the violation status, the violation counter, or both.

Defaults

If no options are specified, all information for all types of CoS violations will be cleared.

Mode

All command modes.

Example

This example shows how to clear both status and counters from all CoS inbound rate limiting violation entries:

```
S Chassis(rw)->clear cos violation irl all both
```

clear cos all-entries

Use this command to clears all Class of Service entries except priority settings 0 - 7.

Syntax

clear cos all-entries

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear all Class of Service entries except priority settings 0 - 7 which are changed to default values:

```
S Chassis(rw)->clear cos all-entries
```

46

Network Monitoring Commands

This chapter describes Network Monitoring commands and how to use them. For information about configuring network monitoring, refer to the "Network Monitoring Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show netstat	46-1
show users	46-3
tell	46-4
disconnect	46-5

show netstat

Use this command to display statistics for the switch's active network connections.

Syntax

```
show netstat [icmp | ip | stats | tcp | udp]
```

Parameters

icmp	(Optional) Shows Internet Control Message Protocol (ICMP) statistics.
ip	(Optional) Shows Internet Protocol (IP) statistics.
stats	(Optional) Shows all statistics for TCP, UDP, IP, and ICMP.
tcp	(Optional) Shows Transmission Control Protocol (TCP) statistics.
udp	(Optional) Shows User Datagram Protocol (UDP) statistics.

Defaults

If no parameters are specified, all switch network connections display.

Mode

All command modes.

Usage

The display of routes configured on the host stack have been moved to the **host** option of command "show ip route" on page 56-1.

Example

This example shows how to display statistics for all the current active network connections:

```
S Chassis(rw)->show netstat
INET sockets
Prot  Recv-Q Send-Q Local Address               Foreign Address             State
ICMP  0      0      0.0.0.0.*                   0.0.0.0.*
TCP   0      0      0.0.0.0.111                 0.0.0.0.*                   LISTEN
TCP   0      0      0.0.0.0.80                  0.0.0.0.*                   LISTEN
UDP   0      0      127.0.0.1.20033             127.0.0.1.20032
.
.
.
OSPFIGP 0      0    0.0.0.0.*                   0.0.0.0.*

INET6 sockets
Prot  Recv-Q Send-Q Local Address               Foreign Address             State
TCP   0      0      ::.23                       ::.*                        LISTEN
S Chassis(rw)->
```

The following example displays the statistics for all supported protocols:

```
S Chassis(rw)->show netstat stats
Ip:
    26034 total packets received
    25824 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    187 incoming packets delivered
    6391 requests sent out
    21 dropped because of missing route
Icmp:
    14 ICMP messages received
    0 input ICMP message failed
    ICMP input histogram:
        destination unreachable: 14
    6184 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 1
        echo request: 6183
Tcp:
    2 active connection openings
    2 passive connection openings
    0 failed connection attempts
    0 connection resets received
    4 connections established
```

```
    153 segments received
    153 segments send out
    0 segments retransmitted
    0 bad segments received
    0 resets sent
Udp:
    42 packets received
    1 packets to unknown port received
    0 packet receive errors
    57 packets sent
S Chassis(rw)->
```

Table 46-1 provides an explanation of the command output.

Table 46-1 show netstat Output Details

Output...	What it displays...
Proto	Type of protocol running on the connection.
Recv-Q	Number of queries received over the connection.
Send-Q	Number of queries sent over the connection.
Local Address	IP address of the connection's local host.
Foreign Address	IP address of the connection's foreign host.
State	Communications mode of the connection (listening, learning or forwarding).

show users

Use this command to display information about the active console port or Telnet session(s) logged in to the switch.

Syntax

show users

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to use the **show users** command. In this output, there are two Telnet users logged in with Read-Write access privileges from IP addresses 134.141.192.119 and 134.141.192.18:

```
S Chassis(rw)->show users
  Session  User  Location
  -------- ----- -------------------------
* telnet   rw    134.141.192.119
  telnet   rw    134.141.192.18
```

tell

Use this command to send a message to one or all users.

Syntax

tell {*dest* | **all**} "*message*"

Parameters

dest	Specifies the user to which this message will be sent. Valid syntax is *user@location*. Use the command "show users" on page 46-3 to display active user names and locations.
all	Sends a broadcast message to all users.
"*message*"	Text message.

Defaults

None.

Mode

All command modes.

Example

This example shows how to tell all users about a system reset:

```
S Chassis(rw)->show users
  Session  User  Location
  -------- ----- -------------------------
* console  admin console (via com.1.1)
  telnet   rw    134.141.192.18
S Chassis(rw)->tell rw@134.141.192.18 "System reset in 15 minutes"
```

User rw@134.141.192.18 will receive:

```
Message from admin@console: "System reset in 15 minutes"
```

disconnect

Use this command to close an active console port or Telnet session from the switch CLI.

Syntax

disconnect {*ip-address* | **console**}

Parameters

ip-address	Specifies the IP address of the Telnet session to be disconnected. This address is displayed in the output shown in "show users" on page 46-3.
console	Closes an active console port.

Defaults

None.

Mode

All command modes.

Example

This example shows how to close the current console session:

```
S Chassis(rw)->disconnect console
Disconnect current session? (y/n)
```

47

SMON Commands

This chapter describes Switched Network Monitoring (SMON) commands and how to use them. For information about configuring SMON, refer to the "Network Monitoring Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show smon priority	47-1
set smon priority	47-2
clear smon priority	47-3
show smon vlan	47-3
set smon vlan	47-4
clear smon vlan	47-5

show smon priority

Use this command to display SMON user priority statistics. SMON generates aggregated statistics for IEEE 802.1Q VLAN environments.

Syntax

show smon priority [*port-string*] [**priority** *priority*]

Parameters

port-string	(Optional) Displays SMON priority statistics being collected by specific port(s).
priority *priority*	(Optional) Displays SMON statistics based on encoded user priority, Valid values are **0** - **7**.

Defaults

- If *port-string* is not specified, SMON statistics for all ports will be displayed.
- If *priority* is not specified, statistics for all priority queues will be displayed.

Mode

All command modes.

Example

This example shows how to display SMON priority 0 statistics for 1-Gigabit Ethernet port 14 in module 3:

```
S Chassis(rw)->show smon priority ge.3.14 0
Show Priority Statistics
------------------------
Interface = ge.3.14
Owner     = none
Creation  = 0 days 0 hours 6 minutes 39 seconds
Status    = enabled
--------------------

Priority 0 Packets              Octets
----------
Total      7981308              2332402460
Overflow   0                    0
```

set smon priority

Use this command to create, start, or stop priority-encoded SMON user statistics counting.

Syntax

set smon priority {**create** | **enable** | **disable**} *port-string* [*owner*]

Parameters

create | **enable** | **disable**	Creates, enables, or disables SMON priority statistics counting. Create automatically enables (starts) counters.
port-string	Specifies one or more source ports on which to collect statistics.
owner	(Optional) Specifies an administratively assigned name of the owner of this entity.

Defaults

If *owner* is not specified, none will be applied.

Mode

All command modes.

Usage

The S-Series platform supports a maximum of 128 SMON priority sessions. Resources available to SMON priority are shared with other SMON tasks and port mirroring. Depending upon your configuration needs, you may not be able to configure the maximum number of supported SMON priority sessions.

Example

This example shows how to set the device to gather SMON priority statistics from 1-Gigabit Ethernet port 14 in module 3:

```
S Chassis(rw)->set smon priority ge.3.14
```

clear smon priority

Clears priority-encoded user statistics on one or more ports.

Syntax

clear smon priority [*port-string*]

Parameters

port-string	(Optional) Clears statistics for specific port(s).

Defaults

If *port-string* is not specified, priority statistics will be cleared on all ports.

Mode

All command modes.

Example

This example shows how to clear SMON priority statistics on 1-Gigabit Ethernet source port 14 in module 3:

```
S Chassis(rw)->clear smon priority ge.3.14
```

show smon vlan

Use this command to display SMON VLAN statistics.

Syntax

show smon vlan [*port-string*] [**vlan** *vlan-id*]

Parameters

port-string	(Optional) Displays SMON VLAN statistics being collected by specific port(s).
vlan *vlan-id*	(Optional) Displays SMON statistics associated with a specific VLAN.

Defaults

- If *port-string* is not specified, SMON statistics for all ports will be displayed.
- If *vlan-id* is not specified, statistics for all VLANs will be displayed.

Mode

All command modes.

Example

This example shows how to display SMON VLAN 1 statistics for the SMON enabled port ge.1.1:

```
S Chassis(rw)->show smon vlan vlan 1
Show VLAN Statistics
--------------------
Interface = vtap.0.1
Owner     = none
Creation  = 20 days 1 hours 44 minutes 27 seconds
Status    = enabled
--------------------

VLAN 1                Packets               Octets
Total                 404                   28418
Overflow              0                     0
NonUnicast            302                   19591
NonUnicast Overflow   0                     0
S Chassis(rw)->
```

set smon vlan

Use this command to create, start, or stop SNMP VLAN-related statistics counting.

Syntax

set smon vlan {**create** | **enable** | **disable**} *port-string* [*owner*]

Parameters

create | **enable** | **disable**	Creates, enables, or disables SMON VLAN statistics counting. Create automatically enables (starts) counters.
port-string	Specifies one or more source ports on which to collect statistics.
owner	(Optional) Specifies an administratively assigned name of the owner of this entity.

Defaults

If *owner* is not specified, none will be applied.

Mode

All command modes.

Usage

The S-Series platform supports 16 SMON VLAN switch-wide VLAN sessions. Resources available to SMON VLAN sessions are shared with other SMON tasks and port mirroring. Depending upon your configuration needs, you may not be able to configure the maximum number of supported SMON VLAN sessions.

Example

This example shows how to set the device to gather SMON VLAN-related statistics from 1-Gigabit Ethernet port 14 in module 3:

```
S Chassis(rw)->set smon vlan enable ge.3.14
```

clear smon vlan

Use this command to delete an SMON VLAN statistics counting configuration.

Syntax

clear smon vlan [*port-string*]

Parameters

port-string	(Optional) Clears statistics counting configuration(s) for specific port(s).

Defaults

If *port-string* is not specified, VLAN statistics counting configurations will be cleared for all ports.

Mode

All command modes.

Example

This example shows how to clear an SMON VLAN statistics counting configuration 1-Gigabit Ethernet port 14 in module 3:

S Chassis`(rw)->clear smon vlan enable ge.3.14`

48

RMON Commands

This chapter describes Remote Network Monitoring commands and how to use them. For information about configuring RMON, refer to the "Network Monitoring Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show rmon stats	48-2
set rmon stats	48-4
clear rmon stats	48-5
show rmon history	48-5
set rmon history	48-7
clear rmon history	48-8
show rmon alarm	48-9
set rmon alarm properties	48-10
set rmon alarm status	48-11
clear rmon alarm	48-12
show rmon event	48-13
set rmon event properties	48-14
set rmon event status	48-15
clear rmon event	48-15
set rmon event properties	48-14
set rmon host properties	48-17
set rmon host status	48-17
clear rmon host	48-18
show rmon topN	48-18
set rmon topN properties	48-20
set rmon topN status	48-20
clear rmon topN	48-21
show rmon matrix	48-21
set rmon matrix properties	48-23
set rmon matrix status	48-24

For information about...	Refer to page...
clear rmon matrix	48-24
show rmon channel	48-25
set rmon channel	48-25
clear rmon channel	48-26
show rmon filter	48-27
set rmon filter	48-28
clear rmon filter	48-28
show rmon capture	48-29
set rmon capture	48-30
clear rmon capture	48-31

show rmon stats

Use this command to display RMON statistics measured for one or more ports.

Syntax

show rmon stats [*port-string*] [**wide**] [**bysize**]

Parameters

port-string	(Optional) Displays RMON statistics for specific port(s).
wide	(Optional) Display most important stats, one line per entry.
bysize	(Optional) Display counters by packet length.

Defaults

If *port-string* is not specified, RMON stats will be displayed for all ports.

Mode

All command modes.

Example

This example shows how to display RMON statistics for port 4 on module 1:

```
S Chassis(rw)->show rmon stats tg.1.4

Port: tg.1.4
--------------------
Index          = 1052
Owner          = monitor
Data Source    = ifIndex.13004
Direction      = rx+tx

Drop Events    = 0             Packets           = 0
```

```
Collisions     = 0              Octets             = 0
Jabbers        = 0              0    -   64 Octets = 0
Broadcast Pkts = 0              65   -  127 Octets = 0
Multicast Pkts = 0              128  -  255 Octets = 0
CRC Errors     = 0              256  -  511 Octets = 0
Undersize Pkts = 0              512  - 1023 Octets = 0
Oversize Pkts  = 0              1024 - 1518 Octets = 0
Fragments      = 0
S Chassis(rw)->
```

Table 48-1 provides an explanation of the command output.

Table 48-1 show rmon stats Output Details

Output...	What it displays...
Port	Port designation.
Owner	Name of the entity that configured this entry. Monitor is default.
Data Source	Data source of the statistics being displayed.
Direction	The direction (transmit/receive) from which statistics are collected.
Drop Events	Total number of times that the switch was forced to discard frames due to lack of available switch device resources. This does not display the number of frames dropped, only the number of times the switch was forced to discard frames.
Collisions	Total number of collisions that have occurred on this interface.
Jabbers	Total number of frames that were greater than 1518 bytes and had either a bad FCS or a bad CRC.
Packets	Total number of frames (including bad frames, broadcast frames, and multicast frames) received on this interface.
Broadcast Pkts	Total number of good frames that were directed to the broadcast address. This value does not include multicast frames.
Multicast Pkts	Total number of good frames that were directed to the multicast address. This value does not include broadcast frames.
CRC Errors	Number of frames with bad Cyclic Redundancy Checks (CRC) received from the network. The CRC is a 4-byte field in the data frame that ensures that the data received is the same as the data that was originally sent.
Undersize Pkts	Number of frames received containing less than the minimum Ethernet frame size of 64 bytes (not including the preamble) but having a valid CRC.
Oversize Pkts	Number of frames received that exceeded 1518 data bytes (not including the preamble) but had a valid CRC.
Fragments	Number of received frames that are not the minimum number of bytes in length, or received frames that had a bad or missing Frame Check Sequence (FCS), were less than 64 bytes in length (excluding framing bits, but including FCS bytes) and had an invalid CRC. It is normal for this value to increment since fragments are a normal result of collisions in a half-duplex network.

Table 48-1 show rmon stats Output Details (continued)

Output...	What it displays...
Octets	Total number of octets (bytes) of data, including those in bad frames, received on this interface.
0 – 64 Octets	Total number of frames, including bad frames, received that were 64 bytes in length (excluding framing bits, but including FCS bytes).
65 – 127 Octets	Total number of frames, including bad frames, received that were between 65 and 127 bytes in length (excluding framing bits, but including FCS bytes).
128 – 255 Octets	Total number of frames, including bad frames, received that were between 128 and 255 bytes in length (excluding framing bits, but including FCS bytes).
256 – 511 Octets	Total number of frames, including bad frames, received that were between 256 and 511 bytes in length (excluding framing bits, but including FCS bytes).
512 – 1023 Octets	Total number of frames, including bad frames, received that were between 512 and 1023 bytes in length (excluding framing bits, but including FCS bytes).
1024 – 1518 Octets	Total number of frames, including bad frames, received that were between 1024 and 1518 bytes in length (excluding framing bits, but including FCS bytes).

set rmon stats

Use this command to configure an RMON statistics entry.

Syntax

set rmon stats *index port-string* [*owner*] [**direction** {**rx+tx** | **rx** | **tx**}]

Parameters

index	Specifies an index for this statistics entry.
port-string	Specifies port to which this entry will be assigned.
owner	(Optional) Assigns a management station owner for this entry.
direction	(Optional) Specifies the configuration of statistics collection direction.
rx+tx	Configures the direction of statistics collection for both receive and transmit.
rx	Configures the direction of statistics collection for receive only.
tx	Configures the direction of statistics collection for transmit only.

Defaults

If *owner* is not specified, **monitor** will be applied.

If **direction** is not specified, statistics collection is both receive and transmit.

Mode

All command modes.

Usage

The recording of current statistics measured by the RMON probe for each monitored interface on the device is a function of the RMON statistics group. The statistics group function monitors packet types: broadcast, multicast, dropped, collisions, CRC errored, over and undersized, fragments, and jabbers. RMON gathers the sum of received and transmitted counters by default.

RMON statistics can be configured to gather the sum of received and transmitted counter, received only, or transmitted only by setting the statistics direction.

Example

This example shows how to configure RMON statistics entry 2 for tg.1.20:

```
S Chassis(rw)->set rmon stats 2 tg.1.20
```

clear rmon stats

Use this command to delete one or more RMON statistics entries.

Syntax

clear rmon stats {*index-list* | **to-defaults** | **counters** *port-string*}

Parameters

index-list	Specifies one or more stats entries to be deleted, causing them to disappear from any future RMON queries.
to-defaults	Resets all history entries to default values. This will cause entries to reappear in RMON queries.
counters *port-string*	Resets RMON counters for the specified port(s).

Defaults

None.

Mode

All command modes.

Example

This example shows how to delete RMON statistics entry 2:

```
S Chassis(rw)->clear rmon stats 2
```

show rmon history

Use this command to display RMON history properties and statistics. The RMON history group records periodic statistical samples from a network.

Syntax

show rmon history [*port-string*] [**wide**] [**interval** {**30sec** | **5min** | **25min**}]

Parameters

port-string	(Optional) Displays RMON history entries for specific port(s).
wide	(Optional) Display most important stats, one line per entry.
interval	(Optional) Summarize history over a fixed interval. • **30sec** - Accumulated in the last 30 seconds • **5min** - Accumulated in the last 5 minutes • **25min** - Accumulated in the last 25 minutes

Defaults

If *port-string* is not specified, information about all RMON history entries will be displayed.

Mode

All command modes.

Example

This example shows how to display RMON history entries for port 32 in module 3. For a description of the types of statistics shown, refer to Table 48-1:

```
S Chassis(rw)->show rmon history ge.3.32

Port: ge.3.32
-------------------------------------
Index 3063
Owner             = monitor
Status            = valid
Data Source       = ifIndex.32032
Interval          = 30
Buckets Requested = 50
Buckets Granted   = 50

Sample 210       Interval Start: 0 days 1 hours 44 minutes 29 seconds
Drop Events       = 0                    Undersize Pkts    = 0
Octets            = 233067               Oversize Pkts     = 0
Packets           = 3577                 Fragments         = 0
Broadcast Pkts    = 1                    Jabbers           = 0
Multicast Pkts    = 23                   Collisions        = 0
CRC Align Errors  = 0                    Utilization(%)    = 0
.
.
.
Sample 259       Interval Start: 0 days 2 hours 8 minutes 59 seconds
Drop Events       = 0                    Undersize Pkts    = 0
Octets            = 233244               Oversize Pkts     = 0
Packets           = 3577                 Fragments         = 0
Broadcast Pkts    = 1                    Jabbers           = 0
```

```
Multicast Pkts    = 24                  Collisions        = 0
CRC Align Errors  = 0                   Utilization(%)    = 0


Port: ge.3.32
-------------------------------------
Index 3064
Owner             = monitor
Status            = valid
Data Source       = ifIndex.32032
Interval          = 1800
Buckets Requested = 50
Buckets Granted   = 50

Sample 1         Interval Start: (time = 0)
Drop Events       = 0                   Undersize Pkts    = 0
Octets            = 13920203            Oversize Pkts     = 0
Packets           = 213520              Fragments         = 0
Broadcast Pkts    = 60                  Jabbers           = 0
Multicast Pkts    = 1412                Collisions        = 0
CRC Align Errors  = 0                   Utilization(%)    = 0
.
.
.
Sample 4         Interval Start: 0 days 1 hours 29 minutes 59 seconds
Drop Events       = 0                   Undersize Pkts    = 0
Octets            = 13988922            Oversize Pkts     = 0
Packets           = 214585              Fragments         = 0
Broadcast Pkts    = 60                  Jabbers           = 0
Multicast Pkts    = 1410                Collisions        = 0
CRC Align Errors  = 0                   Utilization(%)    = 0
```

set rmon history

Use this command to configure an RMON history entry.

Syntax

set rmon history *index* [*port-string*] [**buckets** *buckets*] [**interval** *interval*] [**owner** *owner*] [**direction** {**rx+tx** | **rx** | **tx**}]

Parameters

index	Specifies an index number for this entry.
port-string	(Optional) Assigns this entry to a specific port.
buckets *buckets*	(Optional) Specifies the maximum number of entries to maintain.

interval *interval*	(Optional) Specifies the sampling interval in seconds.
owner *owner*	(Optional) Specifies a management station owner for this entry.
direction	(Optional) Specifies the configuration of the RMON history collection direction.
rx+tx	Configures the direction of history collection for both receive and transmit.
rx	Configures the direction of history collection for receive only.
tx	Configures the direction of history collection for transmit only.

Defaults

- If *buckets* is not specified, the maximum number of entries maintained will be 50 entries.
- If not specified, *interval* will be set to 1800 seconds.
- If *owner* is not specified, **monitor** will be applied.
- If **direction** is not specified, history collection is both receive and transmit.

Mode

All command modes.

Usage

RMON history is a periodic statistical sampling of RMON statistics. RMON history can be configured to gather the periodic sum of received and transmitted counters, received only, or transmitted only by setting the history direction.

Example

This example shows how configure RMON history entry 1 on port ge.2.1 to sample every 30 seconds:

```
S Chassis(rw)->set rmon history 1 ge.2.1 interval 30
```

clear rmon history

Use this command to delete one or more RMON history entries or reset one or more entries to default values.

Syntax

clear rmon history {*index-list* | **to-defaults**}

Parameters

index-list	Specifies one or more history entries to be deleted, causing them to disappear from any future RMON queries.
to-defaults	Resets all history entries to default values. This will cause entries to reappear in RMON queries.

Defaults

None.

Mode

All command modes.

Example

This example shows how to delete RMON history entry 1:

```
S Chassis(rw)->clear rmon history 1
```

show rmon alarm

Use this command to display RMON alarm entries.

Syntax

show rmon alarm [*index*]

Parameters

index	(Optional) Displays RMON alarm entries for a specific entry index ID.

Defaults

If *index* is not specified, information about all RMON alarm entries will be displayed.

Mode

All command modes.

Usage

The RMON alarm group periodically takes statistical samples from RMON variables and compares them with previously configured thresholds. If the monitored variable crosses a threshold an RMON event is generated.

Example

This example shows how to display RMON alarm entry 1:

```
S Chassis(rw)->show rmon alarm 1

Index 1
----------------------
Owner               = deepak
Status              = valid
Variable            = 1.3.6.1.2.1.16.1.1.1.5.3029
Sample Type         = absolute       Startup Alarm       = rising
Interval            = 60             Value               = 5404
Rising Threshold    = 0              Falling Threshold   = 0
Rising Event Index  = 1              Falling Event Index = 0
```

Table 48-2 provides an explanation of the command output.

Table 48-2 show rmon alarm Output Details

Output...	What it displays...
Index	Index number for this alarm entry.
Owner	Text string identifying who configured this entry.
Status	Whether this event entry is enabled (valid) or disabled.
Variable	MIB object to be monitored.
Sample Type	Whether the monitoring method is an absolute or a delta sampling.
Startup Alarm	Whether alarm generated when this entry is first enabled is rising, falling, or either.
Interval	Interval in seconds at which RMON will conduct sample monitoring.
Rising Threshold	Minimum threshold for causing a rising alarm.
Falling Threshold	Maximum threshold for causing a falling alarm.
Rising Event Index	Index number of the RMON event to be triggered when the rising threshold is crossed.
Falling Event Index	Index number of the RMON event to be triggered when the falling threshold is crossed.

set rmon alarm properties

Use this command to configure an RMON alarm entry, or to create a new alarm entry with an unused alarm index number.

Syntax

```
set rmon alarm properties index [interval interval] [object object] [type
{absolute | delta}] [startup {rising | falling | either}] [rthresh rthresh]
[fthresh fthresh] [revent revent] [fevent fevent] [owner owner]
```

Parameters

index	Specifies an index number for this entry. Maximum number of entries is 50**.** Maximum value is **65535**.
interval *interval*	(Optional) Specifies an interval (in seconds) for RMON to conduct sample monitoring. Default value: **3600**.
object *object*	(Optional) Specifies a MIB object to be monitored. **Note:** This parameter is not mandatory for executing the command, but must be specified in order to enable the alarm entry configuration.
type absolute | **delta**	(Optional) Specifies the monitoring method as: sampling the absolute value of the object, or the difference (delta) between object samples. Default value: **absolute**.

startup rising | **falling** | **either**	(Optional) Specifies the type of alarm generated when this event is first enabled as: • Rising - Sends alarm when an RMON event maximum threshold condition is reached, for example, more than 30 collisions per second. • Falling - Sends an alarm when RMON event falls below a minimum threshold condition, for example when the network is behaving normally again. • Either - Sends alarm when either a rising or falling threshold is reached.
rthresh *rthresh*	(Optional) Specifies a minimum threshold for causing a rising alarm.
fthresh *fthresh*	(Optional) Specifies a maximum threshold for causing a falling alarm.
revent *revent*	(Optional) Specifies the index number of the RMON event to be triggered when the rising threshold is crossed.
fevent *fevent*	(Optional) Specifies the index number of the RMON event to be triggered when the falling threshold is crossed.
owner *owner*	(Optional) Specifies the name of the entity that configured this alarm entry.

Defaults

- interval - **3600** seconds
- type - **absolute**
- startup - **rising**
- rthresh - **0**
- fthresh - **0**
- revent - **0**
- fevent - **0**
- owner - **monitor**

Mode

All command modes.

Example

This example shows how to configure a rising RMON alarm. This entry will conduct monitoring of the delta between samples every 30 seconds:

```
S Chassis(rw)->set rmon alarm properties 3 interval 30 object
   1.3.6.1.4.1.5624.1.2.29.1.2.1.0 type delta rthresh 1 revent 2 owner Manager
```

set rmon alarm status

Use this command to enable an RMON alarm entry.

Syntax

set rmon alarm status *index* **enable**

Parameters

index	Specifies an index number for this entry. Maximum number or entries is 50**.** Maximum value is **65535**.
enable	Enables this alarm entry.

Defaults

None.

Mode

All command modes.

Usage

An RMON alarm entry can be created using this command, configured using the **set rmon alarm properties** command ("set rmon alarm properties" on page 48-10), then enabled using this command. An RMON alarm entry can be created and configured at the same time by specifying an unused index with the set properties command.

An alarm is a notification that a statistical sample of a monitored variable has crossed a configured threshold.

Example

This example shows how to enable RMON alarm entry 3:

```
S Chassis(rw)->set rmon alarm status 3 enable
```

clear rmon alarm

Use this command to delete an RMON alarm entry.

Syntax

clear rmon alarm *index*

Parameters

index	Specifies the index number of entry to be cleared.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear RMON alarm entry 1:

```
S Chassis(rw)->clear rmon alarm 1
```

show rmon event

Use this command to display RMON event entry properties.

Syntax

show rmon event [*index*]

Parameters

index	(Optional) Displays RMON properties and log entries for a specific entry index ID.

Defaults

If *index* is not specified, information about all RMON entries will be displayed.

Mode

All command modes.

Example

This example shows how to display RMON event entry 1:

```
S Chassis(rw)->show rmon event 1

Index 1
----------------
Owner           = deepak1
Status          = valid
Description     = event1check
Type            = log-and-trap
Community       =
Last Time Sent = 0 days 0 hours 0 minutes 1 seconds

Log Number 1 for Index 1 occurred at 0 days 0 hours 0 minutes 1 seconds
RisingAlarm: alarmIndex 1, alarmVariable 1.3.6.1.2.1.16.1.1.1.5.3029,
alarmSampleType 1, alarmValue 0, alarmRisingThreshold 0
S Chassis(rw)->
```

Table 48-3 provides an explanation of the command output.

Table 48-3 show rmon event Output Details

Output...	What it displays...
Index	Index number for this event entry.
Owner	Text string identifying who configured this entry.
Status	Whether this event entry is enabled (valid) or disabled.
Description	Text string description of this event.
Type	Whether the event notification will be a log entry, an SNMP trap, both, or none.

Table 48-3 show rmon event Output Details (continued)

Output...	What it displays...
Community	SNMP community name if message type is set to trap.
Last Time Sent	When an event notification matching this entry was sent.

set rmon event properties

Use this command to configure an RMON event entry, or to create a new event entry with an unused event index number.

Syntax

set rmon event properties *index* [**description** *description*] [**type** {**none** | **log** | **trap** | **both**}] [**community** *community*] [**owner** *owner*]

Parameters

index	Specifies an index number for this entry. Maximum number of entries is 100. Maximum value is **65535**.
description *description*	(Optional) Specifies a text string description of this event.
type none | **log** | **trap** | **both**	(Optional) Specifies the type of RMON event notification as: none, a log table entry, an SNMP trap, or both a log entry and a trap message.
community *community*	(Optional) Specifies an SNMP community name to use if the message type is set to **trap**. For details on setting SNMP traps and community names, refer to the *Extreme Networks S-Series Configuration Guide*.
owner *owner*	(Optional) Specifies the name of the entity that configured this entry.

Defaults

- If **description** is not specified, none will be applied.
- If not specified, **type none** will be applied.
- If *owner* is not specified, **monitor** will be applied.

Mode

All command modes.

Example

This example shows how to create and enable an RMON event entry called “STP topology change” that will send both a log entry and an SNMP trap message to the “public” community:

```
S Chassis(rw)->set rmon event properties 2 description “STP topology change” type
both community public owner Manager
```

set rmon event status

Use this command to enable an RMON event entry. An event entry describes the parameters of an RMON event that can be triggered.

Syntax

set rmon event status *index* **enable**

Parameters

index	Specifies an index number for this entry. Maximum number of entries is 100. Maximum value is **65535**.
enable	Enables this event entry.

Defaults

None.

Mode

All command modes.

Usage

An RMON event entry can be created using this command, configured using the **set rmon event properties** command ("set rmon event properties" on page 48-14), then enabled using this command. An RMON event entry can be created and configured at the same time by specifying an unused index with the set properties command.

Events can be fired by RMON alarms and can be configured to create a log entry, generate a trap, or both.

Example

This example shows how to enable RMON event entry 1:

```
S Chassis(rw)->set rmon event status 1 enable
```

clear rmon event

Use this command to delete an RMON event entry and any associated log entries.

Syntax

clear rmon event *index*

Parameters

index	Specifies the index number of the entry to be cleared.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear RMON event 1:

```
S Chassis(rw)->clear rmon event 1
```

show rmon host

Use this command to display RMON properties and statistics associated with each host discovered on the network.

Syntax

show rmon host [*port-string*] [**address** | **creation**]

Parameters

port-string	(Optional) Displays RMON properties and statistics for specific port(s).
address | **creation**	(Optional) Sorts the display by MAC address or creation time of the entry.

Defaults

- If *port-string* is not specified, information about all ports will be displayed.
- If **address** or **creation** are not specified, entries will not be sorted.

Mode

All command modes.

Example

This example displays RMON host properties and statistics for port 10 on module 3. For a description of the types of statistics shown, refer to Table 48-1:

```
S Chassis(rw)->show rmon host ge.3.10

Port ge.3.10
---------------------------------------
Index  310
Owner          = monitor
Status         = valid
Data Source    = ifIndex.32010
Table Size     = 100
Last Deletion  = (time = 0)

Host 00-11-88-fd-95-52   Creation Order 1
In Pkts        = 0                   Out Pkts          = 20624
In Octets      = 0                   Out Octets        = 3114067
Broadcast Pkts = 379                 Multicast Pkts    = ---
Out Errors     = ---
```

```
Host 01-80-c2-00-00-02   Creation Order 2
In Pkts        = 22692               Out Pkts          = 0
In Octets      = 2859192             Out Octets        = 0
Broadcast Pkts = 0                   Multicast Pkts    = ---
Out Errors     = ---
S Chassis(rw)->
```

set rmon host properties

Use this command to configure an RMON host entry.

Syntax

set rmon host properties *index port-string* [*owner*]

Parameters

index	Specifies an index number for this entry. An entry will automatically be created if an unused index number is chosen. Maximum number of entries is 5. Maximum value is **65535**.
port-string	Configures RMON host monitoring on a specific port.
owner	(Optional) Specifies the name of the entity that configured this entry.

Defaults

If *owner* is not specified, **monitor** will be applied.

Mode

All command modes.

Example

This example shows how to configure RMON host entry 1 on port 5 in module 1:

```
S Chassis(rw)->set rmon host properties 1 tg.1.5
```

set rmon host status

Use this command to enable an RMON host entry.

Syntax

set rmon host status *index* **enable**

Parameters

index	Specifies an index number for this entry. Maximum number of entries is 5. Maximum value is **65535**.
enable	Enables this host entry.

Defaults

None.

Mode

All command modes.

Example

This example shows how to enable RMON host entry 1:

```
S Chassis(rw)->set rmon host status 1 enable
```

clear rmon host

Use this command to delete an RMON host entry.

Syntax

clear rmon host *index*

Parameters

index	Specifies the index number of the entry to be cleared.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear RMON host entry 1:

```
S Chassis(rw)->clear rmon host 1
```

show rmon topN

Use this command to displays RMON TopN properties and statistics.

Syntax

show rmon topN [*index*]

Parameters

index	(Optional) Displays RMON properties and statistics for a specific entry index ID.

Defaults

If *index* is not specified, information about all entries will be displayed.

Mode

All command modes.

Usage

TopN monitoring prepares tables that describe the hosts topping a list ordered by one of their statistics. TopN lists are samples of one of the hosts base statistics over a specific interval.

Example

This example displays RMON TopN properties and statistics for index 1:

```
S Chassis(rw)->show rmon topN 1


Index  1
-------------------------------------
HostIndex      = 1
Owner          = monitor
Status         = valid
Rate Base      = InPkts
Duration       = 0
Start Time     = (time = 0)
Time Remaining = 0
Requested Size = 10
Granted Size   = 10
S Chassis(rw)->
```

Table 48-4 provides an explanation of the command output. Properties are set using the **set rmon topN properties** command as described in "set rmon topN properties" on page 48-20.

Table 48-4 show rmon topN Output Details

Output...	What it displays...
Index	Index number for this event entry. Each entry defines one top N report prepared for one interface.
Status	Whether this event entry is enabled (valid) or disabled.
Owner	Text string identifying who configured this entry.
Start Time	System up time when this report was last started.
HostIndex	Index number of the host table for which this top N report will be prepared.
Rate Base	Type of counter (and corresponding integer value) activated with this entry: as InPackets (1), OutPackets (2), InOctets (3), OutOctets (4), OutErrors (5), Broadcast packets (6), or Multicast packets (7).
Duration	Collection time (in seconds) for this report.
Time Remaining	Collection time left for this report if still in progress.
Requested Size	Maximum number of hosts requested for the top N table.
Granted Size	Actual maximum number of hosts in the top N table. Depending on system resources, this may differ from the Requested Size value.
Rate	Amount of change in the counter type (InPackets, OutPackets, etc.) during the sampling interval.
Address	MAC address of the host.

set rmon topN properties

Use this command to configure an RMON topN entry (report).

Syntax

```
set rmon topn properties index [hindex hindex] [rate {inpackets | outpackets | inoctets | outoctets | errors | bcast | mcast}] [duration duration] [size size] [owner owner]
```

Parameters

index	Specifies an index number for this entry. An entry will automatically be created if an unused index number is chosen. Maximum number of entries is 10. Maximum value is **65535**.
hindex *hindex*	(Optional) Specifies an index number of the host table.
rate inpackets | **outpackets** | **inoctets** | **outoctets** | **errors** | **bcast** | **mcast**	(Optional) Specifies the type of counter to activate with this entry as InPackets, OutPackets, InOctets, OutOctets, OutErrors, Broadcast packets, or Multicast packets.
duration *duration*	(Optional) Specifies the sampling interval in seconds. Value must be a minimum of **60**.
size *size*	(Optional) Specifies the maximum number of entries to maintain.
owner *owner*	(Optional) Specifies the name of the entity that configured this entry.

Defaults

- If host index is not specified, none will be applied.
- If counter type is not specified, **inpackets** will be applied.
- If *duration* is not specified, none will be applied.
- If *size* is not specified, **10** will be applied.
- If *owner* is not specified, **monitor** will be applied.

Mode

All command modes.

Example

This example shows how to configure RMON TopN entry 1, for host 1 with a sampling interval of 60 seconds and a maximum number of entries of 20:

```
S Chassis(rw)->set rmon topN properties 1 1 inpackets 60 20
```

set rmon topN status

Use this command to enable an RMON topN entry.

Syntax

```
set rmon topN status index enable
```

Parameters

index	Specifies an index number for this entry. Maximum number of entries is 10. Maximum value is **65535**.
enable	Enables this TopN entry.

Defaults

None.

Mode

All command modes.

Example

This example shows how to enable RMON TopN entry 1:

```
S Chassis(rw)->set rmon topN status 1 enable
```

clear rmon topN

Use this command to delete an RMON TopN entry.

Syntax

clear rmon topN *index*

Parameters

index	Specifies the index number of the entry to be cleared.

Defaults

None.

Mode

All command modes.

Example

This example shows how to delete RMON TopN entry 1:

```
S Chassis(rw)->clear rmon topN 1
```

show rmon matrix

Use this command to display RMON matrix properties and statistics.

Syntax

show rmon matrix [*port-string*] [**source** | **dest**]

Parameters

port-string	(Optional) Displays RMON properties and statistics for a specific port(s).
source | **dest**	(Optional) Sorts the display by source or destination address.

Defaults

- If *port-string* is not specified, information about all ports will be displayed.
- If not specified, information about source and destination addresses will be displayed.

Mode

All command modes.

Usage

The RMON matrix stores statistics for conversations between sets of two addresses.

Example

This example shows how to display RMON matrix properties and statistics. A control entry displays first, followed by actual entries corresponding to the control entry:

```
S Chassis(rw)->show rmon matrix


Port ge.3.27
--------------------------------------
Index  1
Owner          = monitor
Status         = valid
Data Source    = ifIndex.32027
Table Size     = 100
Last Deletion  = (time = 0)

Source      00-09-6b-3f-28-79    Destination 00-01-f4-00-71-aa
Packets   = 5                    Octets    = 1825
Errors    = ---

Source      00-09-6b-3f-28-79    Destination 00-01-f4-da-04-90
Packets   = 21                   Octets    = 1638
Errors    = ---

Source      00-09-6b-3f-28-79    Destination 00-e0-63-d6-89-5f
Packets   = 116                  Octets    = 9048
Errors    = ---
S Chassis(rw)->
```

Table 48-5 provides an explanation of the command output. Properties are set using the **set rmon matrix properties** command as described in "set rmon matrix properties" on page 48-23.

Table 48-5 show rmon matrix Output Details

Output...	What it displays...
Matrix Index	Index number for this RMON matrix entry.
Owner	Text string identifying who configured this entry.
Status	Whether this matrix entry is enabled (valid) or disabled.
Data Source	Interface for which host monitoring is being conducted.
Table size	Number of entries in the matrix table for this interface.
Last deletion	System up time when the last entry was deleted from the matrix table associated with this entry.
Source	Source of the data from which this entry creates a traffic matrix.
Destination	Destination of the data from which this entry creates a traffic matrix.
Packets	Number of packets (including bad packets) transmitted from the source address to the destination address.
Octets	Number of octets (excluding framing bits, but including FCS octets) contained in all packets transmitted from the source address to the destination address.
Errors	Errors recorded.

set rmon matrix properties

Use this command to configure an RMON matrix entry.

Syntax

set rmon matrix properties *index port-string* [*owner*]

Parameters

index	Specifies an index number for this entry. An entry will automatically be created if an unused index number is chosen. Maximum number of entries is 2. Maximum value is **65535**.
port-string	Specifies port(s) on which to monitors statistics.
owner	(Optional) Specifies the name of the entity that configured this entry.

Defaults

If *owner* is not specified, **monitor** will be applied.

Mode

All command modes.

Example

This example shows how to configure RMON matrix entry 1 for tg.1.1

```
S Chassis(rw)->set rmon matrix properties 1 tg.1.1
```

set rmon matrix status

Use this command to enable an RMON matrix entry.

Syntax

set rmon matrix status *index* **enable**

Parameters

index	Specifies an index number for this entry. Maximum number of entries is 2. Maximum value is **65535**.
enable	Enables or disables this matrix entry.

Defaults

None.

Mode

All command modes.

Example

This example shows how to enable RMON matrix entry 1:

```
S Chassis(rw)->set rmon matrix status 1 enable
```

clear rmon matrix

Use this command to delete an RMON matrix entry.

Syntax

clear rmon matrix *index*

Parameters

index	Specifies the index number of the entry to be cleared.

Defaults

None.

Mode

All command modes.

Example

This example shows how to delete RMON matrix entry 1:

```
S Chassis(rw)->clear rmon matrix 1
```

show rmon channel

Use this command to display RMON channel entries for one or more ports.

Syntax

show rmon channel [*port-string*]

Parameters

port-string	(Optional) Displays RMON channel entries for a specific port(s).

Defaults

If *port-string* is not specified, information about all channels will be displayed.

Mode

All command modes.

Example

This example shows how to display RMON channel information for tg.2.12:

```
S Chassis(rw)->show rmon channel tg.2.12
Port tg.2.12    Channel index= 628      EntryStatus= valid
-------------------------------------------------------------
Control             off       AcceptType          matched
OnEventIndex        0         OffEventIndex       0
EventIndex          0         Status              ready
Matches             4498
Description         Thu Dec 16 12:57:32 EST 2004
Owner               NetSight smith
```

set rmon channel

Use this command to configure an RMON channel entry.

Syntax

set rmon channel *index port-string* [**accept** {**matched** | **failed**}] [**control** {**on** | **off**}] [**onevent** *onevent*] [**offevent** *offevent*] [**event** *event*] [**estatus** {**ready** | **fired** | **always**}] [**description** *description*] [**owner** *owner*]

Parameters

index	Specifies an index number for this entry. An entry will automatically be created if an unused index number is chosen. Maximum number of entries is 2. Maximum value is **65535**.
port-string	Specifies the port on which traffic will be monitored.
accept matched | **failed**	(Optional) Specifies the action of the filters on this channel as: • **matched** - Packets will be accepted on filter matches • **failed** - Packets will be accepted if they fail a match

control on | **off**	(Optional) Enables or disables control of the flow of data through the channel.
onevent *onevent*	(Optional) Specifies the index of the RMON event that will turn this channel on.
offevent *offevent*	(Optional) Specifies the index of the RMON event that will turn this channel off.
event *event*	(Optional) Specifies the event to be triggered when the channel is on and a packet is accepted.
estatus ready | **fired** | **always**	(Optional) Specifies the status of the event as: • **ready** - A single event may be generated. • **fired** - No additional events may be generated. • **always** - An event will be generated for every match.
description *description*	(Optional) Specifies a description for this channel.
owner *owner*	(Optional) Specifies the name of the entity that configured this entry.

Defaults

- If an **action** is not specified, packets will be accepted on filter matches.
- If not specified, **control** will be set to **off**.
- If **onevent** and **offevent** are not specified, none will be applied.
- If event status is not specified, **ready** will be applied.
- If a **description** is not specified, none will be applied.
- If **owner** is not specified, it will be set to **monitor**.

Mode

All command modes.

Example

This example shows how to configure RMON channel 54313 for port ge.2.12 with a description of "capture all":

```
S Chassis(rw)->set rmon channel 54313 ge.2.12 description "capture all"
```

clear rmon channel

Use this command to clear an RMON channel entry.

Syntax

clear rmon channel *index*

Parameters

index	Specifies the channel entry to be cleared.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear RMON channel entry 2:

```
S Chassis(rw)->clear rmon channel 2
```

show rmon filter

Use this command to display one or more RMON filter entries.

Syntax

show rmon filter [**index** *index* | **channel** *channel*]

Parameters

index *index* | **channel** *channel*	(Optional) Displays information about a specific filter entry, or about all filters which belong to a specific channel.

Defaults

If no options are specified, information for all filter entries will be displayed.

Mode

All command modes.

Example

This example shows how to display all RMON filter entries and channel information:

```
S Chassis(rw)->show rmon filter
Index= 55508    Channel Index= 628      EntryStatus= valid
------------------------------------------------------------
Data Offset         0         PktStatus           0
PktStatusMask       0         PktStatusNotMask    0
Owner               ETS,NAC-D
-----------------------------
Data
ff ff ff ff ff ff
-----------------------------
DataMask
ff ff ff ff ff ff
-----------------------------
DataNotMask
00 00 00 00 00 00
```

set rmon filter

Use this command to configure an RMON filter entry.

Syntax

set rmon filter *index channel_index* [**offset** *offset*] [**status** *status*] [**smask** *smask*] [**snotmask** *snotmask*] [**data** *data*] [**dmask** *dmask*] [**dnotmask** *dnotmask*] [**owner** *owner*]

Parameters

index	Specifies an index number for this entry. An entry will automatically be created if an unused index number is chosen. Maximum number of entries is 10. Maximum value is **65535**.
channel_index	Specifies the channel to which this filter will be applied.
offset *offset*	(Optional) Specifies an offset from the beginning of the packet to look for matches.
status *status*	(Optional) Specifies packet status bits that are to be matched.
smask *smask*	(Optional) Specifies the mask applied to status to indicate which bits are significant.
snotmask *snotmask*	(Optional) Specifies the inversion mask that indicates which bits should be set or not set.
data *data*	(Optional) Specifies the data to be matched.
dmask *dmask*	(Optional) Specifies the mask applied to data to indicate which bits are significant.
dnotmask *dnotmask*	(Optional) Specifies the inversion mask that indicates which bits should be set or not set.
owner	(Optional) Specifies the name of the entity that configured this entry.

Defaults

- If *owner* is not specified, it will be set to **monitor**.
- If no other options are specified, none (0) will be applied.

Mode

All command modes.

Example

This example shows how to create RMON filter 1 and apply it to channel 10:

```
S Chassis(rw)->set rmon filter 1 10 offset 30 data 0a154305 dmask ffffffff
```

clear rmon filter

Use this command to clear an RMON filter entry.

Syntax

clear rmon filter {**index** *index* | **channel** *channel*}

Parameters

index *index*	Specifies the filter entry to clear or all entries belonging to a specific channel.
channel *channel*	Specifies a channel for which all entries are cleared.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear RMON filter entry 1:

```
S Chassis(rw)->clear rmon filter index 1
```

show rmon capture

Use this command to display RMON capture entries and associated buffer control entries.

Syntax

show rmon capture [*index*] [**nodata**]

Parameters

index	(Optional) Displays the specified buffer control entry and all captured packets associated with that entry.
nodata	(Optional) Displays only the buffer control entry specified by index.

Defaults

If no options are specified, all buffer control entries and associated captured packets will be displayed.

Mode

All command modes.

Example

This example shows how to display RMON capture entries and associated buffer entries:

```
S Chassis(rw)->show rmon capture
Buf.control= 28062  Channel= 38283      EntryStatus= valid
------------------------------------------------------------
FullStatus          avail     FullAction          lock
Captured packets    251       Capture slice       128
Download size       100       Download offset     0
Max Octet Requested 50000     Max Octet Granted   50000
Start time          1 days 0 hours 51 minutes 15 seconds
```

```
Owner               monitor


captureEntry= 1        Buff.control= 28062
-----------------------------------------
Pkt ID      9          Pkt time    1 days 0 hours 51 minutes 15 seconds
Pkt Length  93         Pkt status  0
Data:
00 00 5e 00 01 01 00 01 f4 00 7d ce 08 00 45 00
00 4b b4 b9 00 00 40 11 32 5c 0a 15 43 05 86 8d
bf e5 00 a1 0e 2b 00 37 cf ca 30 2d 02 01 00 04
06 70 75 62 6c 69 63 a2 20 02 02 0c 92 02 01 00
02 01 00 30 14 30 12 06 0d 2b 06 01 02 01 10 07
01 01 0b 81 fd 1c 02 01 01 00 11 0b 00
```

set rmon capture

Use this command to configure an RMON capture entry, or to enable or disable an existing entry.

Syntax

set rmon capture *index* {*channel* [**action** {**lock** | **wrap**}] [**slice** *slice*] [**loadsize** *loadsize*] [**offset** *offset*] [**asksize** *asksize*] [**owner** *owner*]}

Parameters

index	Specifies a buffer control entry.
channel	Specifies the channel to which this capture entry will be applied.
action lock | **wrap**	(Optional) Specifies the action of the buffer when it is full as: • **lock** - Packets will cease to be accepted • **wrap** - Oldest packets will be overwritten
slice *slice*	(Optional) Specifies the maximum octets from each packet to be saved in a buffer (default: 100).
loadsize *loadsize*	(Optional) Specifies the maximum octets from each packet to be downloaded from the buffer (default: 100).
offset *offset*	(Optional) Specifies that the first octet from each packet that will be retrieved.
asksize *asksize*	(Optional) Specifies that the requested maximum octets will be saved in this buffer.
owner	(Optional) Specifies the name of the entity that configured this entry.

Defaults

- If not specified, **action** defaults to **lock**.
- If not specified, offset defaults to **0**.
- If not specified, asksize defaults to **1** (which will request as many octets as possible)
- If **slice** and **loadsize** are not specified, **100** will be applied.

- If *owner* is not specified, it will be set to **monitor**.

Mode

All command modes.

Usage

Configuring RMON capture causes hardware based forwarding to be disabled, resulting in all traffic from the port to be forwarded by the CPU.

Example

This example shows how to create RMON capture entry 1 to "listen" on channel 628:

```
S Chassis(rw)->set rmon capture 1 628
```

clear rmon capture

Use this command to clears an RMON capture entry.

Syntax

clear rmon capture *index*

Parameters

index	Specifies the capture entry to be cleared.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear RMON capture entry 1:

```
S Chassis(rw)->clear rmon capture 1
```

49

NetFlow Commands

This chapter describes NetFlow commands and how to use them. For information about configuring NetFlow, refer to the "NetFlow Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show netflow	49-1
set netflow cache	49-3
clear netflow cache	49-3
set netflow export-data	49-4
clear netflow export-data	49-5
set netflow export-destination	49-5
clear netflow export-destination	49-6
set netflow export-interval	49-7
clear netflow export-interval	49-7
set netflow port	49-9
clear netflow port	49-10
set netflow export-version	49-10
clear netflow export-version	49-11
set netflow template	49-11
clear netflow template	49-13

show netflow

Use this command to display NetFlow configuration information and statistics.

Syntax

show netflow [**config** [*port-string*]] [**statistics** [**export**]]

Parameters

config	(Optional) Show the NetFlow configuration.
statistics	(Optional) Show the NetFlow statistics.

export	(Optional) Show the NetFlow export statistics.
port-string	(Optional) Specifies the port or ports to display.

Defaults

- If **config** is entered, but no *port-string*, information for all ports is displayed.
- If **statistics** is entered but not **export**, all statistics are displayed.
- If no options are entered, all NetFlow configuration and statistics information is displayed

Mode

All command modes, Read Only.

Example

This example shows how to display both NetFlow configuration information and statistics:

```
S Chassis(rw)->show netflow

Cache Status:           enabled
Export Version:               9
Export Interval:             30 (min)
Number of Entries:       1048575
Inactive Timer:              40 (sec)
Template Refresh-rate:       20 (packets)
Template Timeout:            30 (min)

Enabled Optional Export Data:
-----------------------------
None

Destination IP                          UDP Port
--------------------------------------- --------
10.10.1.1                               2055
10.10.1.2                               2055
10.10.1.3                               2055
10.10.1.4                               2055

Enabled Ports Both Ingress and Egress:
--------------------------------------
ge.1.1-5

Disabled Ports:
-----------------
lag.0.1-62
ge.1.6-48
tg.1.1-4
```

```
Export Statistics:
-----------------------------------
Network Packets Sampled:          10
Exported Packets:                  0
Exported Records:                  0
Export Packets Failed:             0
Export Records Dropped:            0
```

set netflow cache

Use this command to enable (create) or disable (free up) a NetFlow cache on each module in the Extreme Networks S-Series system.

Syntax

set netflow cache {**enable** | **disable**}

Parameters

enable | **disable**	Enable or disable the NetFlow cache.

Defaults

None.

Mode

All command modes.

Usage

A NetFlow cache maintains NetFlow information for all active flows. By default, NetFlow caches are not created.

Use the **set netflow cache enable** command to enable the NetFlow cache on the system.

Use either the **set netflow cache disable** or the **clear netflow cache** command to disable the NetFlow cache on the system.

Example

This example shows how to enable, or create, a NetFlow cache on each module in the system:

```
S Chassis(rw)->set netflow cache enable
```

clear netflow cache

Use this command to remove, or free up, the NetFlow caches on each module in the Extreme Networks S-Series system.

Syntax

clear netflow cache

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

When either the **clear netflow cache** or **set netflow cache disable** command is executed, NetFlow is effectively disabled on the system.

Example

This example shows how to remove the NetFlow caches on all modules and disable NetFlow:

```
S Chassis(rw)->clear netflow cache
```

set netflow export-data

Use this command to enable NetFlow Version 9 optional MAC and VLAN export data.

Syntax

set netflow export-data {**enable** | **disable**} {**mac** | **vlan**}

Parameters

enable | **disable**	Enables or disables the export of optional Version 9 export data.
mac	Specifies that the incoming source (IN_SRC_MAC) and outgoing destination (OUT_DST_MAC) MAC addresses are included in the export data sent to the collector.
vlan	Specifies that the VLANs associated with the ingress (SRC_VLAN) and egress (DST_VLAN) interfaces are included in the export data sent to the collector.

Defaults

None.

Mode

All command modes.

Usage

The export of optional MAC and VLAN data is disabled by default. Including these export data options in the flow record makes the record larger and results in fewer records and exported packets. The optional NetFlow export data records are only supported for NetFlow Version 9.

If the **mac** option is enabled, both incoming source and destination MAC addresses are included in the export data for the collector.

If the **vlan** option is enabled, VLANs associated with both the ingress and egress interfaces are included in the export data for the collector.

Use the **enable** parameter to enable the exporting of either the MAC or VLAN export data option.

Use the **disable** parameter to disable the exporting of either the MAC or VLAN export data option.

Use the **clear netflow export-data** command to disable both the MAC and VLAN export data options.

Example

This example shows how to enable the VLAN export data option for the NetFlow collector:

```
S Chassis(rw)->set netflow export-data enable vlan
S Chassis(rw)->
```

clear netflow export-data

Use this command to reset the NetFlow optional export data to default values.

Syntax

clear netflow export-data

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

NetFlow supports the export of MAC incoming source and outgoing destination MAC addresses and VLANs associated with the ingress and egress interfaces. The export of optional MAC and VLAN data is disabled by default.

Use the **clear netflow export-data** command to reset both MAC and VLAN export data configuration to the default value of disabled.

Example

This example shows how to reset the NetFlow MAC and VLAN export data configuration to the default value of disabled:

```
S Chassis(rw)->clear netflow export-data
S Chassis(rw)->
```

set netflow export-destination

Use this command to configure up to four NetFlow collector destinations.

Syntax

set netflow export-destination *ip-address* [*udp-port*]

Parameters

ip-address	Specifies the IPv4 or IPv6 address of the NetFlow collector.
udp-port	(Optional) Specifies the UDP port number used by the NetFlow collector. Default is **2055**.

Defaults

If the UDP port is not specified, the UDP port is set to **2055**.

Mode

All command modes.

Usage

NetFlow destination collectors are configured one at a time.

By default, no collector address is configured. Up to four collector destinations per Extreme Networks S-Series system can be configured. If you attempt to enter five collector destinations the following error displays:

```
Set failed.  If previously configured, you must "clear netflow export-destination"
first.
```

This message indicates that you have configured the maximum number of export destinations for the device. Remove a configured export destination using the **clear netflow export-destination** *ip-address* command before adding an additional export destination.

Example

This example shows how to set the IP addresses of two NetFlow collectors to **10.10.1.1** and **10.10.1.2**:

```
S Chassis(rw)->set netflow export-destination 10.10.1.1
S Chassis(rw)->set netflow export-destination 10.10.1.2
S Chassis(rw)->
```

clear netflow export-destination

Use this command to clear the specified NetFlow collector IP address.

Syntax

clear netflow export-destination *ip-address* [*udp-port*]

Parameters

ip-address	Specifies the IPv4 or IPv6 address of the NetFlow collector to clear.
udp-port	(Optional) Specifies the UDP port number used by NetFlow collector.

Defaults

If the UDP port is not specified, the UDP port associated with this export destination is cleared along with the rest of the export destination configuration.

Mode

All command modes.

Example

This example shows how to clear the **10.10.1.1** NetFlow collector address:

```
S Chassis(rw)->clear netflow export-destination 10.10.1.1
```

set netflow export-interval

Use this command to configure the NetFlow export interval.

Syntax

set netflow export-interval *interval*

Parameters

interval	Set the active flow timer value, between 1 to 60 minutes. The default value is 30 minutes.

Defaults

None.

Mode

All command modes.

Usage

Each S-Series blade in the system will transmit a NetFlow packet when:

- It has accumulated the maximum number of NetFlow records per packet, which is 20, or
- It has accumulated fewer than 20 NetFlow records and the active flow timer has expired, or
- The flow expires (ages out or is invalidated).

Example

This example shows how to set the NetFlow export interval to 10 minutes:

```
S Chassis(rw)->set netflow export-interval 10
```

clear netflow export-interval

Use this command to clear the NetFlow export interval to its default value of 30 minutes.

Syntax

clear netflow export-interval

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to return the NetFlow export interval to its default value:

```
S Chassis(rw)->clear netflow export-interval
```

set netflow export-rate

Use this command to control number of NetFlow records per second that can be generated per module.

Syntax

set netflow export-rate *rate* [*slot*]

Parameters

rate	Specifies the number of entries per second per module. Valid values are **1** - **20000** entries per second. Default value is **10000** entries per second.
slot	(Optional) Specifies the chassis slot number the configured rate is applied to.

Defaults

- The NetFlow export rate defaults to 10000 entries per second.
- If the *slot* option is not specified, the rate configuration applies to all modules in the chassis.

Mode

All command modes.

Usage

Use the **show netflow** command to display the current and maximum supported export data rate for this device.

Use the **clear netflow export-rate** command to reset the export rate to the default value.

Example

This example shows how to set the NetFlow export rate to 12000 entries per second:

```
S Chassis(rw)->set netflow export-rate 12000
S Chassis(rw)->
```

clear netflow export-data

Use this command to reset the NetFlow optional export data to default values.

Syntax

clear netflow export-rate [*slot*]

Parameters

slot	(Optional) Specifies the chassis slot number to clear.

Defaults

- If the *slot* option is not specified, the rate configuration is cleared on all modules in the chassis.

Mode

All command modes.

Example

This example shows how to reset the NetFlow export rate on all modules in the device:

```
S Chassis(rw)->clear netflow export-rate
S Chassis(rw)->
```

set netflow port

Use this command to enable or disable NetFlow collection on a port.

Syntax

set netflow port *port-string* {**enable** | **disable**}

Parameters

port-string	Specifies the port or ports on which to enable or disable NetFlow collection.
enable | **disable**	Enables or disables NetFlow collection.

Defaults

None.

Mode

All command modes.

Example

This example shows how to enable NetFlow collection on port ge.1.1:

```
S Chassis(rw)->set netflow port ge.1.1 enable
```

clear netflow port

Use this command to return a port to the default NetFlow collection state of disabled.

Syntax

clear netflow port *port-string*

Parameters

port-string	Specifies the port or ports on which to disable NetFlow collection.

Defaults

None.

Mode

All command modes.

Example

This example shows how to disable NetFlow collection on port ge.1.1:

```
S Chassis(rw)->clear netflow port ge.1.1
```

set netflow export-version

Use this command to set the NetFlow flow record format used to export data.

Syntax

set netflow export-version {**5** | **9**}

Parameters

5 | **9**	Specifies the NetFlow flow record format to use when exporting NetFlow packets, either Version **5** or **9**. The default is Version **5**.

Defaults

None.

Mode

All command modes.

Usage

NetFlow supports a single Version 5 template. NetFlow Version 9 supports 15 IPv4 and 15 IPv6 Extreme Networks predefined templates. The NetFlow enabled device automatically selects the appropriate Version 9 template based upon the contents of the flow and the data record types supported in the template. Template data record types are defined by the NetFlow standard.

See the "NetFlow Configuration" chapter of the *Extreme Networks S-Series Configuration Guide* for both NetFlow Version 5 and Version 9 template details.

For Version 9 templates, the source and destination MAC address data records and VLANs associated with both the ingress and egress interfaces data records can be optionally included when exporting data records to the collector. Enabling the export of optional data records to the NetFlow collector is set using "set netflow export-data" on page 49-4. Including these export data options in the flow record makes the record larger and results in fewer records and exported packets.

Use the **clear netflow export-version** command to reset the export version to the default value of Version 5.

Use the **show netflow config** command ("show netflow" on page 49-1) to display the current NetFlow version.

Example

This example shows how to set the flow record format to Version 9:

```
S Chassis(rw)->set netflow export-version 9
```

clear netflow export-version

Use this command to return the NetFlow flow record format used to export data to the default of Version 5.

Syntax

clear netflow export-version

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

Use the **show netflow config** command to display the current NetFlow version.

Example

This example shows how to return the flow record format to Version 5:

```
S Chassis(rw)->clear netflow export-version
```

set netflow template

Use this command to configure the NetFlow Version 9 template refresh rate and timeout values.

Syntax

set netflow template {[**refresh-rate** *packets*] [**timeout** *minutes*]}

Parameters

refresh-rate *packets*	The number of export packets sent that causes a template to be retransmitted by an individual module. The value of *packets* can range from 1 to 600. The default value is 20 packets.
timeout *minutes*	The length of the timeout period, in minutes, after which a template is retransmitted by all blades in the system. The value of *minutes* can range from 1 to 3600. The default value is 30 minutes.

Defaults

At least one of the **refresh-rate** or **timeout** parameters must be specified, although both can be specified on a single command line.

Mode

All command modes.

Usage

Version 9 template records have a limited lifetime and must be periodically refreshed. Templates are retransmitted when either:

- The packet refresh rate is reached, or
- The template timeout is reached.

Template refresh based on the timeout period is performed on every blade. Since each module handles its own packet transmissions, template refresh based on number of export packets sent is managed by each blade independently.

The refresh rate defines the maximum delay a new or restarted NetFlow collector would experience before it learns the format of the data records being forwarded. Refresh rates affect NetFlow collectors during their start up when they must ignore incoming data flow reports until the required template is received.

Setting the appropriate refresh rate for your Extreme Networks S-Series system must be determined, since the default settings of a 20 flow report packet refresh rate and a 30 minute timeout may not be optimal for your environment. For example, a switch processing an extremely slow flow rate of, say, 20 flow report packets per half hour, would refresh the templates only every half hour using the default settings, while a switch sending 300 flow report packets per second would refresh the templates 15 times per second.

Extreme Networks recommends that you configure your Extreme Networks S-Series system so it does not refresh templates more often than once per second.

Use the **show netflow config** command (“show netflow” on page 49-1) to display the currently configured values.

Example

This example shows how to set the Version 9 template packet refresh rate to 50 packets and the timeout value to 45 minutes:

```
S Chassis(rw)->set netflow template refresh-rate 50 timeout 45
```

clear netflow template

Use this command to reset the Version 9 template refresh rate and/or timeout values to their default values.

Syntax

```
clear netflow template {[refresh-rate] [timeout]}
```

Parameters

refresh-rate	Clear the template packet refresh rate to the default value of 20 flow report packets.
timeout	Clear the template timeout to the default value of 30 minutes.

Defaults

At least one of the **refresh-rate** or **timeout** parameters must be specified, although both can be specified on one command line.

Mode

All command modes.

Example

This example shows how to return the Version 9 template packet refresh rate to 20 flow report packets and the timeout value to 30 minutes:

```
S Chassis(rw)->set netflow template refresh-rate 50 timeout 30
```

50

Connectivity Fault Management (CFM) Commands

This chapter describes the Connectivity Fault Management (CFM) set of commands and how to use them. For information about CFM and its configuration, refer to the "Connectivity Fault Management (CFM) Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

The S-Series CFM CLI provides the commands for configuring CFM maintenance domains (MD), maintenance associations (MA) within those domains, and maintenance association endpoints (MEPs) at the edge of MAs. The CFM CLI commands are arranged in a hierarchy of configuration modes (levels, or contexts) that reflect the architecture of CFM. This chapter has the same organization, with commands listed alphabetically for each configuration mode. CFM **show** and **clear** commands are listed in separate sections.

For information about...	Refer to page...
Global Configuration Commands	50-1
Default Maintenance Domain (MD) Configuration Commands	50-7
Maintenance Domain Configuration Commands	50-11
Maintenance Association Configuration Commands	50-15
Maintenance Association Component Configuration Commands	50-19
Maintenance End-Point Configuration Commands	50-20
CFM Clear Commands	50-32
CFM Show Commands	50-35

Global Configuration Commands

The commands described in this section are available at global configuration mode.

For information about...	Refer to page...
cfm default-md	50-2
cfm enable	50-3
cfm logging filter	50-3
cfm md	50-4
cfm vlan-table	50-6

cfm default-md

Use this command to enter system level Default Maintenance Domain (MD) Configuration mode, to configure either default MD values or default MD per-VLAN values.

Syntax

cfm default-md {**default | vid** *vlan-id*}

no cfm default-md {**default | vid** *vlan-id*}

Parameters

default	Enter "Default Maintenance Domain (MD)" mode to configure system level default maintenance domain values.
vlan *vlan-id*	Enter "Default Maintenance Domain (MD)" mode for a specific VLAN to configure default maintenance domain values.

Defaults

None.

Mode

Global configuration command.

Usage

The "no" form of this command resets any system Default MD mode configuration to default values.

When you use the **default** parameter, you move into Default Maintenance Domain mode and can configure system level default values for maintenance domains. When you use the **vid** parameter, you move into Default Maintenance Domain mode for a specific VLAN and can configure default values for that VLAN.

Refer to "Default Maintenance Domain (MD) Configuration Commands" on page 50-7 for commands available in the Default Maintenance Domain configuration mode.

Examples

This example shows how to enter the system level default MD configuration command mode. Note that the command prompt changes to indicate that you have moved to Default Maintenance Domain mode for configuring default maintenance domain values.

```
S Chassis(rw-config)->cfm default-md default
S Chassis(su-config-cfm-default-md-def)->
```

This example enters default configuration mode for VLAN 20. Note that the command prompt changes to indicate that you have moved to Default Maintenance Domain mode for configuring VLAN 20.

```
S Chassis(rw-config)->cfm default-md vid 20
S Chassis(su-config-cfm-default-md.20)->
```

cfm enable

Use this command to globally enable CFM.

Syntax

cfm enable

no cfm enable

Parameters

None.

Defaults

CFM is disabled by default.

Mode

Global configuration command.

Usage

CFM must be enabled globally for CFM to be operational.

The "no" form of this command resets the CFM global state to the default setting of disabled.

Example

This example shows how to globally enable CFM on the device:

```
S Chassis(rw-config)->cfm enable
S Chassis(rw-config)->
```

cfm logging filter

Use this command to filter the sending of CFM Syslog messages by maintenance domains (MDs), maintenance associations (MAs), and maintenance end points (MEPs).

Syntax

cfm logging filter md {**string-name** *name* | **dns-like-name** *dns-name* | **mac-int-name** *mac-name* | **no-name** | index index} [**ma string-name** *name* | **vid-name** *vid-name* | **id-name** *id-name* | **index** *index*} [**mep** *mep-id*]

no cfm logging filter

Parameters

md	Specifies an MD context.
ma	(Optional) Specifies an MA context.
string-name *name*	Specifies an MD or MA string name of up to 43 printable characters.
dns-like-name *dns-name*	Specifies an MD string that represents a standard domain name server convention.

mac-int-name *mac-name*	Specifies an MD string that follows a MAC address format plus an integer index ID value separated by a period (.) in the format *xx-xx-xx-xx-xx-xx.ID* or *xx:xx:xx:xx:xx:xx.ID*, where *x* is a hex value and the *ID* range is **0** - **65535**.
no-name	Specifies a NULL string (“”) MD name.
index *index*	Specifies an MD or MA index value.
vid-name *vid-name*	Specifies an MA VLAN integer value between **0** - **4094**.
id-name *id-name*	Specifies an MA ID integer value between **0** - **65535** (MA mode only).
mep *mep-id*	(Optional) Specifies a MEP ID. Valid values are **1** - **8191**.

Defaults

If an MA or end-point is not specified, Syslog messages are sent for all MAs and end-points for the specified MD. If no CFM logging filter configuration exists, all CFM Syslog messages are sent.

Mode

Global Configuration command only.

Usage

This command allows you to limit the sending of CFM Syslog messages to the specified criteria.

The “no” form of this command sets the CFM logging filter configuration to the default value: all CFM Syslog messages are sent.

Example

This example shows how to configure Syslog to display Syslog messages for all MEPs in the **myMA1** maintenance association of the **myMD1** maintenance domain:

```
S Chassis(rw-config)->cfm logging filter md string-name myMD1 ma string-name myMA1
S Chassis(rw-config)->
```

cfm md

Use this command to enter Maintenance Domain (MD) Configuration mode for a specific named MD. If the maintenance domain does not exist, this command will create it.

Syntax

cfm md {**string-name** *name* | **dns-like-name** *dns-name* | **mac-int-name** *mac-name* | **no-name**}

no cfm md {**string-name** *name* | **dns-like-name** *dns-name* | **mac-int-name** *mac-name* | **no-name**}

Parameters

string-name *name*	Specifies an MD string name of up to 43 printable characters.
dns-like-name *dns-name*	Specifies an MD string of up to 43 printable characters that represents a standard domain name server convention.

mac-int-name *mac-name*	Specifies an MD string that follows a MAC address format plus an integer index ID value separated by a period (.) in the format *xx-xx-xx-xx-xx-xx.ID* or *xx:xx:xx:xx:xx:xx.ID*, where *x* is a hex value and the *ID* range is **0** - **65535**.
no-name	Specifies that a NULL string (“”) will be used for the MD name.

Defaults

None.

Mode

Global configuration command.

Usage

A maintenance domain (MD) is a collection of network devices, typically owned and operated by a single organization. Management of devices within a domain falls under the control of that single organization. MDs must be contiguous, so that all the devices belonging to a domain have uninterrupted network connectivity with each other. MDs may be nested or adjacent, but can not share network devices with other domains. MDs are intended to provide connectivity to systems outside of the domain. MDs are uniquely identified by an MD Name.

One of four naming conventions can be used to identify a CFM MD:

- **String-name** – A string of up to 43 printable characters. This format provides descriptive freedom in naming the association.
- **Dns-like-name** – A string of up to 43 printable characters that represents a standard domain name server convention. This option is for management purposes. A check is done to assure that you have entered a legally formatted DNS name.
- **Mac-int-name** – A MAC address format plus an integer index ID value. You must follow a supported MAC address format as described in the parameter table.
- **No-name** – A no name option that sets a NULL string as the MD name. It can only be used for a single MD on each device.

A non-configurable index value is associated with every MD and MA. This index value appears in the prompt to provide context to the prompt. For example, the prompt (rw-config-cfm-md.1) is for the MD index 1 configuration context. Use “show cfm md” on page 50-38 to display the index value for each configured MD.

The “no” form of this command deletes the specified MD.

Refer to “Maintenance Domain Configuration Commands” on page 50-11 for descriptions of the commands available in Maintenance Domain configuration mode.

Examples

This example shows how to enter configuration command mode for the **myMD1** maintenance domain. This maintenance domain instance is assigned index 1.

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(rw-config-cfm-md.1)->
```

This example shows how to enter configuration command mode for the **www.extremenetworks.com** maintenance domain. This maintenance domain instance is assigned index 2.

```
S Chassis(rw-config)->cfm md dns-like-name www.extremenetworks.com
```

```
S Chassis(rw-config-cfm-md.2)->
```

cfm vlan-table

Use this command to configure a logical grouping of multiple service IDs to a primary service.

Syntax

cfm vlan-table primary-selector *primary-selector* **selector-list** *selector-list* [**enable** | **disable**]

no cfm vlan-table [**primary-selector** *primary-selector* | **primary-selector** *primary-selector* **selector-list** *selector-list*]

Parameters

primary-selector *primary-vlan*	Specifies the primary service ID the members of the selector list are associated with. Valid values are **1** - **4094**.
selector-list *selector-list*	Specifies a list of service IDs to be associated with the primary service. Valid values are **1** - **4094**.

Defaults

If enable or disable are not specified, the specified VLAN table configuration is configured but not active (the configured selector list is not associated with the primary selector).

When using the "no" option, if no option is specified, all configured VLAN tables are deleted. If a primary selector is specified, the VLAN table for that primary selector is deleted. If both the primary selector and the selector list are specified, the selector list for that primary selector is deleted.

Mode

Global configuration command.

Usage

The current CFM implementation only supports VLAN services. When configuring a CFM service, the configured ID for the service is checked against configured VLAN tables. The primary selector defines the ID of the service being modified. If a VLAN table with a primary selector exists matching the CFM service ID being configured, the VLAN table selector list is applied to that service ID. For example: if the configured service is VLAN 10 and a VLAN table configuration for primary selector 10 is configured and enabled, the selector list associated with primary selector 10 is applied to the CFM service.

One or more service IDs may be provided in the selector list. IDs specified in the selector list are associated with the primary service. Specifying the **enable** command option activates the association between the IDs in the selector list and the CFM service. Specifying the **disable** command option disables the association of the IDs in the selector list with the CFM service. The VLAN table remains configured, but is not active.

Maintenance points (MIP or MEP) associated with a CFM service will be able to receive CFM PDUs on any of the active IDs defined in the VLAN table selector list. MEPs may be configured with a Primary VID, which must be included within the list of selectors defined by the enabled VLAN table, otherwise there is a one-to-one relationship between the VID and the service. With a primary VID defined, the MEP can transmit tagged PDUs using that primary service. If no primary VID is defined by the maintenance point, the primary selector of the service, as defined in the MA configuration, will be used by the maintenance point to tag its transmitted PDUs.

The “no” form of this command removes all VLAN tables, a specific primary selector VLAN table or the selector list for a specified primary selector as specified in the Defaults section above. A lack of entries in the VLAN table provides a one to one relationship between a service ID and the service.

Examples

This example shows how to configure and enable a VLAN table with a primary selector of 10 and a selector list of 11 through 15.

```
S Chassis(rw-config)->cfm vlan-table primary-selector 10 selector-list 11-15
enable
S Chassis(rw-config)->
```

Default Maintenance Domain (MD) Configuration Commands

The commands listed in this section are available at the Default Maintenance Domain Configuration mode, and in other configuration mode contexts as noted.

Enter this mode from global configuration mode using the cfm default-md command.

For information about...	Refer to page...
id-permission	50-7
level	50-9
mhf-creation	50-10

id-permission

Use this command to configure the ID permission setting for the content sent in the SenderID TLV by the maintenance points for the maintenance domain (default or named) or maintenance association component being configured.

Syntax

id-permission {**chassis** | **manage** | **chassis-manage** | **none** | **defer**}

no id-permission

Parameters

chassis	Specifies that the chassis contents (including the chassis MAC address) of the SenderID TLV is sent by the maintenance points for this context.
manage	Specifies that the management contents (including the method of remote management) of the SenderID TLV is sent by the maintenance points for this context.
chassis-manage	Specifies that the chassis and management contents of the SenderID TLV is sent by the maintenance points for this context.
none	Specifies that the SenderID TLV is not sent by the maintenance points for this context. The default value is **none**.
defer	Specifies that in a VLAN default or MA component context, the SenderID TLV behavior defers to the next highest configuration level settings.

Defaults

The SenderID TLV is not sent by the maintenance point.

Mode

Default MD Configuration mode.
Maintenance Domain Configuration mode.
Maintenance Association Component Configuration mode.

Usage

Enabling ID permission includes in PDUs sent by a maintenance point (MIP or MEP) informational TLVs that identify the bridge.

The **defer** option is only valid in the Default Maintenance Domain VLAN service context, the (named) Maintenance Domain context, or the Maintenance Association Component context. When **defer** is used in the:

- Default MD VLAN service context, the **id-permision** value defaults to the value set for the default MD
- MA component context, the **id-permision** value defaults to the value set for the (named) Maintenance Domain within which the MA component resides

The "no" form of this command sets the ID permission setting to the default value of **none**.

Example

This example sets the IP permission value for the system level default maintenance domain.

```
S Chassis(rw-config)->cfm default-md default
S Chassis(su-config-cfm-default-md-def)->id-permission chassis
S Chassis(su-config-cfm-default-md-def)->
```

This example sets the IP permission value for VLAN 111 at the default maintenance domain level.

```
S Chassis(rw-config)->cfm default-md vid 111
S Chassis(su-config-cfm-default-md.111)->id-permission manage
S Chassis(su-config-cfm-default-md.111)->
```

This example shows how to configure the maintenance points to send both the chassis and management content in the SenderID TLV for the **myMD1** maintenance domain:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->id permission chassis-manage
S Chassis(su-config-cfm-md.1)->
```

This example shows how to configure the maintenance points to defer to the MD setting for ID permission for the **myMA1** maintenance association component context:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->ma-comp
S Chassis(su-config-cfm-macomp)->id-permission defer
S Chassis(su-config-cfm-macomp)->
```

level

Use this command to set the maintenance domain level for the current context.

Syntax

level *level*

no level

Parameters

level	Specifies the level for this MD for this command mode context. Valid values are **0** - **7**. The default value is **0**.

Defaults

The MD level defaults to **0**.

Mode

Default MD Configuration mode.
Maintenance Domain Configuration mode.

Usage

The CFM service network is partitioned into maintenance levels. Each maintenance level is defined by the reach and scope of the organization which administers the network equipment. Higher maintenance levels exist at the edge of the network. Network customers typically own these higher levels. Lower maintenance levels typically reside closer to the network core, and are usually reserved for service providers or network operators. Maintenance levels are hierarchical in nature. Higher maintenance levels encapsulate lower maintenance levels.

The "no" form of this command sets the maintenance domain level to the default value of **0**.

Example

This example shows how to set the system default maintenance domain level to **5**:

```
S Chassis(rw-config)->cfm default-md default
S Chassis(su-config-cfm-default-md-def)->level 5
S Chassis(su-config-cfm-default-md-def)->
```

This example shows how to configure the default maintenance domain VLAN level to 5 for VLAN 111:

```
S Chassis(rw-config)->cfm default-md vid 111
S Chassis(su-config-cfm-default-md.111)->level 5
S Chassis(su-config-cfm-default-md.1)->
```

This example shows how to configure the level to 5 for the **myMD1** maintenance domain:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->level 5
S Chassis(su-config-cfm-md.1)->
```

mhf-creation

Use this command to set whether the creation of maintenance intermediate-point (MIP) half function (MHF) is allowed for the current context.

Syntax

```
mhf-creation {default | explicit | none | defer}
no mhf-creation
```

Parameters

default	Specifies that an MHF can be created for this MD or MA context.
explicit	Specifies that an MHF can be created for this MD or MA context, only if a MEP exists at the next lower MD level.
none	Specifies that MHF creation is not allowed for the MD or MA context. Defaults to **none**.
defer	Specifies that in a MD default VLAN service context, the MHF creation defers to the system default MD configuration, or in MA component context, the MHF creation defers to the configuration for the MD in which this MA component resides.

Defaults

MHF creation is not allowed.

Mode

Default MD Configuration mode.
Maintenance Domain Configuration mode.
Maintenance Association Component Configuration mode.

Usage

A Maintenance Intermediate Point (MIP) resides in the interior of an MD. MIPs are created on ports that reside along the path between Maintenance End Points (MEPs). The MIP supplements the function to the MEPs of the domain. MIPs passively collect information by snooping the continuity check messages (CCMs) that pass through them. The information is collected in a database. These MIP databases act as highway "mile-markers" along the continuity check message path. MIPs may respond to loopback and linktrace requests received from MEPs in its MD.

The **defer** option is only valid in a VLAN system default or MA component configuration context.

The "no" form of this command resets the MHF creation setting to the default value of **none**.

Examples

This example shows how to set the system default maintenance domain value to allow an MHF to be created only when a MEP in the next lowest MD exists:

```
S Chassis(rw-config)->cfm default-md default
```

```
S Chassis(su-config-cfm-default-md-def)->mhf-creation explicit
S Chassis(su-config-cfm-default-md-def)->
```

This example shows how to set MHF creation for the **myMA1** MA component context to defer to the **myMD1** MHF creation setting:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->ma-comp
S Chassis(su-config-cfm-macomp)->mhf-creation defer
```

Maintenance Domain Configuration Commands

The commands listed in this section are available in the Maintenance Domain (MD) Configuration mode, and in other command mode contexts as noted. Use the links in the following table to go to the descriptions of the commands.

Enter this mode from global configuration mode using "**cfm md**" on page 50-4.

For information about...	Refer to page...
enable	50-11
id-permission	50-7
level	50-9
ma	50-12
mhf-creation	50-10
name	50-14

enable

Use this command to activate the CFM configuration for the current context.

Syntax

enable

no enable

Parameters

None.

Defaults

MDs, MAs, MA components, and MEPs are not in service by default.

Mode

Maintenance Domain Configuration mode.
Maintenance Association Configuration mode.
Maintenance Association Component Configuration mode.
MEP Configuration mode.

Usage

Changes made in the MD, MA, MA component, or MEP contexts do not take affect until the **enable** command is entered. If **enable** has already been entered in a given context, you must first enter **no enable** before making any further changes. If you attempt to make changes in a context that has already been enabled, you receive an error message like the following MD context error message:

```
Error: MD must be disabled ("no enable") before changes can be made.
```

Once changes are completed, enter **enable** again for the changes to take affect.

For a given context to be operational, its parent context must be enabled. MD is the parent of MA and MA components. MA and MA components are the parents of MEPs.

Use the “no” form to de-activate settings for this context. When de-activating settings, the configuration is no longer administratively operational but the configuration remains unchanged.

Example

This example shows how to activate the **myMD1** maintenance domain:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->enable
S Chassis(su-config-cfm-md.1)->
```

This example shows how to activate **myMA1** for the **myMD1** maintenance domain:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->enable
S Chassis(su-config-cfm-ma.1)->
```

This example shows how to activate **myMA1** component configuration:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->ma-comp
S Chassis(su-config-cfm-macomp)->enable
S Chassis(su-config-cfm-macomp)->
```

This example shows how to enable MEP **1000** on **myMA1**:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->mep 1000
S Chassis(su-config-cfm-mep.1000)->enable
S Chassis(su-config-cfm-mep.1000)->
```

ma

Use this command to enter Maintenance Association (MA) Configuration mode for the specified MA.

Syntax

ma {**string-name** *name* | **vid-name** vlan | **id-name** *id*}

no ma {**string-name** *name* | **vid-name** vlan | **id-name** *id*}

Parameters

string-name *name*	Specifies the MA name as a string of up to 43 characters.
vid-name *vlan*	Specifies the MA name as a VLAN ID. Valid values are **0** - **4094**.
id-name *index*	Specifies the MA name as an index value. Valid values are **0** - **65535**.

Defaults

None.

Mode

Maintenance Domain Configuration mode.

Usage

A maintenance association (MA) uniquely identifies a service within an MD. A service may be defined by an individual VLAN. There may be multiple MAs within a domain. Subsets of devices residing within the domain are collectively configured to form these associations. The devices belonging to a particular association will communicate among themselves to implement the various features provided by CFM.

One of three naming conventions can be used to identify a CFM MA:

- **String-name** – A string of up to 43 printable characters. This format provides descriptive freedom in naming the association.
- **Vid-name** – An integer value between 0 - 4094. This format restricts the association name to the VLAN range. For management purposes, **show** command output will label this format as a VLAN type. Use this format when the association is directly related to monitoring a VLAN.
- **Id-name** – An integer value between 0 - 65535. This format restricts the association name to an integer range. Use this format when a sequential naming scheme is being used to manage the associations.

A non-configurable index value is associated with every MD and MA. This index value appears in the prompt to provide context to the prompt. For example, the prompt (rw-config-cfm-ma.1) is for the MA index 1 configuration context. Use "show cfm md ma" on page 50-40 to display the index value for each configured MA.

Examples

This example shows how to enter configuration command mode for the **myMD1** maintenance domain and enter MA configuration mode for the maintenance association named **myMA1**:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(rw-config-cfm-md.1)->ma string-name myMA1
S Chassis(rw-config-cfm-ma.1)->
```

This example shows how to enter configuration command mode for the **myMD1** maintenance domain and enter MA configuration mode for the maintenance association identified by **vid-name** type **1000**. Note that since this is the second maintenance association created in maintenance domain **myMD1**, the MA index number is 2 (shown in the prompt).

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(rw-config-cfm-md.1)->ma vid-name 1000
S Chassis(srw-config-cfm-ma.2)->
```

name

Use this command in Maintenance Domain Configuration mode to change the name of the maintenance domain currently being configured.

Syntax

name {**string-name** *name* | **dns-like-name** *dns-name* | **mac-int-name** *mac-name* | **no-name**}

no name {**string-name** *name* | **dns-like-name** *dns-name* | **mac-int-name** *mac-name* | **no-name**}

Parameters

string-name *name*	Specifies an MD or MA string name of up to 43 printable characters.
dns-like-name *dns-name*	Specifies an MD string that represents a standard domain name server convention (MD mode only).
mac-int-name *mac-name*	Specifies an MD string that follows a MAC address format plus an integer index ID value separated by a period (.) in the format *xx-xx-xx-xx-xx-xx.ID* or *xx:xx:xx:xx:xx:xx.ID*, where *x* is a hex value and the *ID* range is **0** - **65535** (MD mode only).
no-name	Specifies that a NULL string (“”) will be used for the MD name (MD mode only).

Defaults

None.

Mode

Maintenance Domain Configuration mode.

Usage

This command allows you to change the name for the maintenance domain of the current context.

The “no” form of this command deletes the specified maintenance command configuration.

Examples

This example shows how to change the name of the **myMD1** maintenance domain to **yourMD1**. Note that the index number for this maintenance domain does not change.

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->name md string-name yourMD1
```

This example shows how to change the name of the **www.extremenetworks.com** maintenance domain to **www.extremenetworks.support.com**:

```
S Chassis(rw-config)->cfm md dns-like-name www.extremenetworks.com
S Chassis(su-config-cfm-md.2)->name dns-like-name
www.extremenetworks.support.com
S Chassis(su-config-cfm-md.2)->
```

Maintenance Association Configuration Commands

The commands listed in this section are available at the Maintenance Association (MA) Configuration mode, and in other contexts as noted. Use the links in the following table to go to the descriptions of the commands.

Enter this mode from the Maintenance Domain Configuration mode using the ma command.

For information about...	Refer to page...
ccm-interval	50-15
enable	50-11
ma-comp	50-16
mep	50-17
mep-list	50-17
name	50-18

ccm-interval

Use this command to set the interval between continuity check messages (CCM)s.

Syntax

```
ccm-interval {1sec | 10sec | 1min | 10min}
no ccm-interval
```

Parameters

1sec	Sets the interval between CCM transmissions used by all MEPs in the MA to **1** second (Default).
10sec	Sets the interval between CCM transmissions used by all MEPs in the MA to **10** seconds.
1min	Sets the interval between CCM transmissions used by all MEPs in the MA to **1** minute.
10min	Sets the interval between CCM transmissions used by all MEPs in the MA to **10** minutes.

Defaults

The CCM interval defaults to **1** second.

Mode

Maintenance Association Configuration mode.

Usage

All maintenance end points (MEPs) in an association are configured for the same CCM interval. The source MEP sends a continuity check message at the interval set by this command. If the remote end-point does not receive the continuity check message within a period of 3.5 times the configured CCM interval, an error is logged. Intermediate-points (MIPs) do not actively log errors.

Should the remote end-point not be configured for the same CCM interval as the source end-point, CFM logs a configuration error and potentially triggers a defect.

Example

This example sets the interval between CCM transmissions used by all MEPs in the **myMA1** maintenance association to **10** seconds:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->ccm-interval 10sec
```

ma-comp

Use this command to enter MA component configuration mode for the MA.

Syntax

ma-comp

no ma-comp

Parameters

None.

Defaults

None

Mode

Maintenance Association Configuration mode.

Usage

Use this command to enter Maintenance Association Component Configuration mode. Once in MA Component Configuration mode, you can configure the association VLAN ID, maintenance intermediate-point (MIP) half-function creation behavior, and ID permission settings for the current MA context.

Use the “no” form of this command to remove the settings for this context.

Example

This example enters MA component configuration mode for the **myMA1** maintenance association:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->ma-comp
S Chassis(su-config-cfm-macomp)->
```

mep

Use this command to enter Maintenance End-Point (MEP) Configuration mode for the specified end-point.

Syntax

mep *mep-id*

no mep *mep-id*

Parameters

mep-id	Specifies an ID for the MEP. Valid values are **1** - **8191**.

Defaults

None.

Mode

Maintenance Association Configuration mode.

Usage

A maintenance association end-point (MEP) resides at the edge of an MD. A MEP is associated with a single MA that monitors a single VLAN. The MEP must belong to the VLAN associated with the MA. The VLAN associated with the MA is configured in MA Component Configuration Mode using “vid” on page 50-19. The MEP serves as the logical boundary between devices operating at different domain levels. MEPs are uniquely identified by an integer value that is unique within the MA it belongs to.

Use this command to access the configuration mode for the specified MEP.

The “no” form of this command deletes a MEP configuration.

Example

This example enters configuration mode for the **myMA1** MEP **1000**:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->mep 1000
S Chassis(su-config-cfm-mep.1000)->
```

mep-list

Use this command to specify the MEPs that are or will be present in the MA.

Syntax

mep-list *mep-list* [**enable** | **disable**]

no mep-list [mep-list]

Parameters

mep-list	Specifies a list of MEPs separated by a comma (“,”) or, if a range of end-points, by a dash (“**-**”).
enable | **disable**	(Optional) Enables or disables the MEP list for this MA context.

Defaults

MEP lists are disabled by default.

If a mep-list is not specified for the “no” form of this command, all list members are deleted from the list.

Mode

Maintenance Association Configuration mode.

Usage

The MA must have knowledge of the local and remote MEP IDs for the local end-points to recognize the remote end-points. All MEPs in an association must be listed in the association MEP list and the MEP list must be enabled for MEPs to be operational.

The “no” form removes all list members if the MEP list is not specified. If a MEP list is specified, only members of the specified MEP list are deleted.

Examples

This example shows how to create and enable the MEP list for MEPs **30** through **35**, **1000**, and **1005** on the **myMA1** maintenance association:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->mep-list 30-35,1000,1005 enable
```

This example shows how to remove MEP **1000** from the current MEP list:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->no mep-list 1000
```

name

Use this command to change the Maintenance Association name.

Syntax

name {**string-name** *name* | **vid-name** *vid-name* | **id-name** *id-name*}

no name {**string-name** *name* | **vid-name** *vid-name* | **id-name** *id-name*}

Parameters

string-name *name*	Specifies an MA string name of up to 43 printable characters.
vid-name *vid-name*	Specifies a VLAN integer value between **0** - **4094** (MA mode only).
id-name *id-name*	Specifies an ID integer value between **0** - **65535** (MA mode only).

Defaults

None.

Mode

Maintenance Association Configuration mode.

Usage

This command allows you to change the MA name for the current context.

The “no” form of this command deletes the specified maintenance command configuration.

Examples

This example shows how to change the MA name for the **myMA1** maintenance association to **yourMA1**:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->name string-name yourMA1
S Chassis(su-config-cfm-ma.1)->
```

Maintenance Association Component Configuration Commands

The commands listed in this section are available at the Maintenance Association (MA) Component Configuration mode, and other modes as noted. Use the links in the following table to go to the descriptions of the commands.

Enter this mode from the Maintenance Association Configuration mode via the ma-comp command.

For information about...	Refer to page...
enable	50-11
id-permission	50-7
mhf-creation	50-10
vid	50-19

vid

Use this command to specify the VLAN the maintenance association or MEP is associated with.

Syntax

vid *vlan-id*

no vid

Parameters

vlan-id	Specifies the VLAN associated with this MA or MEP context. Valid values are 0 - 4094. Default value is 0.

Defaults

If this command is not entered, the VLAN for the MA or end-point defaults to **0** (no VLAN configured).

Mode

Maintenance Association Component Configuration mode.
Maintenance End-Point (MEP) Configuration mode.

Usage

When using CFM to monitor a VLAN, the VLAN must be configured for the MA within the MA component configuration mode.

The MA monitors a single VLAN. If you wish to monitor multiple VLANs in your system, create an MA for each VLAN to be monitored.

Examples

This example sets VLAN **1000** as the configured VLAN for the **myMA1** component configuration:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->ma-comp
S Chassis(su-config-cfm-macomp)->vid 1000
S Chassis(su-config-cfm-macomp)->
```

This example sets VLAN **1000** as the configured VLAN for the **myMA1** MEP **1000**:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->mep 1000
S Chassis(su-config-cfm-mep.1000)->vid 1000
```

Maintenance End-Point Configuration Commands

The commands listed in this section are available at the maintenance end-point (MEP) configuration mode. Use the links in the following table to go to the descriptions of the commands.

Enter this mode from Maintenance Association Configuration mode using the mep command.

For information about...	Refer to page...
active	50-21
alarm-defect-syslog	50-22
alarm-defect-trap	50-23
alarm-time	50-24
cci-enabled	50-25
direction	50-25
enable	50-11
linktrace	50-26

For information about...	Refer to page...
loopback	50-28
port	50-29
priority	50-29
remote-mep active	50-30
reset-time	50-31
vid	50-19

active

Use this command to set the administrative state of the MEP (maintenance end point) state machines.

Syntax

active

no active

Parameters

None.

Defaults

The MEP stat machines administrative state default to inactive.

Mode

Maintenance End-Point Configuration mode

Usage

Setting the MEP state machines to active activates the various state machines within the MEP as defined in IEEE 802.1Q-2011. The MEP state machines must be set to active for the MEP to be operational.

If the MEP state machines are set to inactive, PDUs are not processed, timers are not activated, and defects are not detected.

If the MEP state machine status is active and the MEP is not enabled using “enable” on page 50-11, the MEP will have a Row Status of "Active" in “show cfm md ma mep remote-mep” on page 50-50, but will not perform any functions such as send and receive PDUs or generate defects.

The “no” form of this command sets the MEP administrative state machine state to the default value of inactive.

Example

This example sets the administrative state for the **myMA1** MEP **1000** to active:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->mep 1000
S Chassis(su-config-cfm-mep.1000)->active
```

```
S Chassis(su-config-cfm-mep.1000)->
```

alarm-defect-syslog

Use this command to set the lowest priority defect that will generate a fault alarm syslog message.

Syntax

alarm-defect-syslog {**all-def** | **mac-rem-err-xcon** | **rem-err-xcon** | **err-xcon** | **xcon** | **no-xcon**}

no alarm-defect-syslog {**all-def** | **mac-rem-err-xcon** | **rem-err-xcon** | **err-xcon** | **xcon** | **no-xcon**}

Parameters

all-def	Specifies that the DefRDICCM, DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM defects will generate a fault alarm syslog message. See Table 50-1 on page 50-22 for defect descriptions.
mac-rem-err-xcom	Specifies that the DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM defects will generate a fault alarm syslog message (default).
rem-err-xcon	Specifies that the DefRemoteCCM, DefErrorCCM, and DefXconCCM defects will generate a fault alarm syslog message.
err-xcon	Specifies that the DefErrorCCM, and DefXconCCM defects will generate a fault alarm syslog message.
xcon	Specifies that the DefXconCCM defect will generate a fault alarm syslog message.
no-xcon	Specifies that no fault alarm Syslog messages will be generated.

Defaults

The Syslog defect alarm setting defaults to **mac-rem-err-xcom**.

Mode

Maintenance End-Point Configuration mode.

Usage

Table 50-1 describes the supported MEP defects.

Table 50-1 MEP Defect Definitions

Defect	Description
DefRDICCM	One or more continuity check messages received by this MEP contained the RDI bit. This bit indicates that some other MEP in this MEP's MA is transmitting the RDI bit. This defect clears if continuity check messages from all remote MEPs do not have the RDI bit set. Devices set the RDI bit if they have received continuity check messages from a remote MEP that indicates a defect.
DefMACstatus	The port status is not indicating "UP" for all remote MEPs on received continuity check messages, or the interface status for any remote MEP on received continuity check messages is not indicating "UP".

Table 50-1 MEP Defect Definitions

Defect	Description
DefRemoteCCM	This MEP is not receiving continuity check messages from a MEP in its configured list.
DefErrorCCM	This MEP is receiving continuity check messages from a remote MEP that either uses an invalid MEP ID or uses a continuity check interval that does not match the receiving MEP.
DefXconCCM	This MEP is receiving continuity check messages from a remote MEP that either uses an MD level lower than the receiving MEP or uses a different MD or MA name than the receiving MEP.

The "no" form for this command resets the Syslog defect alarm setting to the default value of **mac-rem-err-xcom**.

Example

This example sets the Syslog defect alarm setting for the **myMA1** MEP **1000** to generate a Syslog message if any supported defect generates an alarm:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->mep 1000
S Chassis(su-config-cfm-mep.1000)->alarm-defect-syslog all-def
```

alarm-defect-trap

Use this command to set the lowest priority defect that will generate a fault alarm trap message.

alarm-defect-trap {**all-def** | **mac-rem-err-xcon** | **rem-err-xcon** | **err-xcon** | **xcon** | **no-xcon**}

no alarm-defect-trap {**all-def** | **mac-rem-err-xcon** | **rem-err-xcon** | **err-xcon** | **xcon** | **no-xcon**}

Parameters

all-def	Specifies that the DefRDICCM, DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM defects will generate a fault alarm trap. See Table 50-1 on page 50-22 for defect descriptions.
mac-rem-err-xcom	Specifies that the DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM defects will generate a fault alarm trap (default).
rem-err-xcon	Specifies that the DefRemoteCCM, DefErrorCCM, and DefXconCCM defects will generate a fault alarm trap.
err-xcon	Specifies that the DefErrorCCM, and DefXconCCM defects will generate a fault alarm trap.
xcon	Specifies that the DefXconCCM defect will generate a fault alarm trap.
no-xcon	Specifies that no fault alarm traps will be generated.

Defaults

The trap defect alarm setting defaults to **mac-rem-err-xcom**.

Mode

Maintenance End-Point Configuration mode.

Usage

See Table 50-1 on page 50-22 for a description of supported MEP defects.

The “no” form for this this command resets the trap defect alarm setting to the default value of **mac-rem-err-xcom**.

Example

This example sets the trap defect alarm setting for the **myMA1** MEP **1000** to generate a trap if any supported defect generates an alarm:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->mep 1000
S Chassis(su-config-cfm-mep.1000)->alarm-defect-trap all-def
```

alarm-time

Use this command to set the minimum time a defect must be present before an alarm is generated.

Syntax

alarm-time *time*

no alarm-time

Parameters

time	Specifies the minimum amount of time in centiseconds a defect must be present before an alarm is generated. Valid values are 250 - 1000 centiseconds. The default value is 250 (2.5 seconds).

Defaults

The minimum amount of time a defect must be present before an alarm is generated defaults to 2.5 seconds.

Mode

Maintenance End-Point Configuration mode.

Usage

The “no” form of this command resets the minimum amount of time a defect must be present before an alarm is generated to the default value of 2.5 seconds.

Example

This example shows how to set the minimum amount of time a defect must be present before an alarm is generated to 3 seconds:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->mep 1000
```

```
S Chassis(su-config-cfm-mep.1000)->alarm-time 300
```

cci-enabled

Use this command to enable generation and reception of continuity check messages.

Syntax

cci-enabled

no cci-enabled

Parameters

None.

Defaults

Continuity check messages are not generated or received by default.

Mode

Maintenance End-Point Configuration mode.

Usage

The “no” form resets the command to the default value of no continuity check messages being generated or received.

Example

This example shows how to enable the sending and receiving of continuity check messages for MEP **1000** on **myMA1**:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->mep 1000
S Chassis(su-config-cfm-mep.1000)->cci-enabled
S Chassis(su-config-cfm-mep.1000)->
```

direction

Use this command to configure whether the MEP faces, sends PDUs towards, and receives PDUs from the bridge relay (up) or faces, sends PDUs towards, and receives PDUs from the bridge port (down).

Syntax

direction {**down** | **up**}

no direction

Parameters

up	Specifies the the MEP faces the bridge relay and sends continuity check messages towards and receives continuity check messages from the bridge relay entity.

down	Specifies the MEP faces the link and sends continuity check messages towards and receives continuity check messages from the bridge port (Default).

Defaults

The MEP direction defaults to down.

Mode

Maintenance End-Point Configuration mode.

Usage

This command configures a maintenance end-point (MEP) with a direction of “up” or “down”. The direction a MEP faces is relative to the link and the bridge relay. A down-MEP sends CFM frames towards and receives CFM frames from the link. An up-MEP sends CFM frames towards the bridge relay and receives CFM frames from the bridge relay. See “mep” on page 50-17 for MEP information.

The “no” form resets the MEP direction to the default value of down.

Example

This example shows how to set the direction for the **myMA1** MEP **1000** to up:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->mep 1000
S Chassis(su-config-cfm-mep.1000)->direction up
S Chassis(su-config-cfm-mep.1000)->
```

linktrace

Use this command to transmit CFM linktrace messages to the specified MEP or MAC address.

Syntax

tracelink {**mep** *mep-id* | **mac** *mac-addr*} [**ttl** *time-to-live*] [**fdb-only**]

Parameters

mep *mep-id*	Specifies the MEP to send the linktrace messages to.
mac *mac-addr*	Specifies the MAC address of the device to send the linktrace messages to. Valid values are MAC addresses in the address format: *xx-xx-xx-xx-xx-xx* or *xx:xx:xx:xx:xx:xx* or *xxxx.xxxx.xxxx* where *x* is a hex value.
ttl *time-to-live*	(Optional) Specifies the time-to-live for the linktrace messages. Valid values are **0** - **255**. Default value is **64**.
fdb-only	(Optional) Specifies that only the bridge's filter database is used to determine the egress port.

Defaults

- If the time-to-live is not specified, the maximum number of hops for the linktrace message defaults to **64**.
- If the **fdb-only** option is not specified, either the filter database or the MIP Continuity Check Message (CCM) database or both can be used to determine reachability and egress ports for the intended target MAC address.

Mode

Maintenance End-Point Configuration mode.

Usage

The CFM linktrace protocol is used to help verify a path and identify where in a path a connectivity problem exists by indicating that an incompete path between the initiating device and the target device exists. Linktrace messages (LTM) are sent to either a specified end-point or to the MAC address of a maintenance intermediate-point.

The **fdb-only** option determines whether each hop along the linktrace path uses the local filter database exclusively or is allowed to also use the local MIP CCM database to determine reachability to the target. If the **fdb-only** option is not specified, both databases are used to determine reachability to the target.

The **mep** option requires that the remote MEP has already communicated with this MEP and there is an entry in the MEP database for the remote MEP. The linktrace will fail if the **mep** option is used and the remote MEP has not yet communicated with this MEP.

The LTM shares the same priority as the continuity check message and can not be separately configured. The priority for continuity check messages and LTMs is set using “priority” on page 50-29.

Example

This example shows how to send linktrace messages to MEP **2000** from the **myMA1** MEP **1000**:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->mep 1000
S Chassis(su-config-cfm-mep.1000)->linktrace mep 2000

Linktrace to 00-00-00-10-00-03, Transaction ID 29481

MD Name: abc
MA Name: abc
MEP ID : 1, Interface ge.4.18
=====================================================
Hop  TTL        Source MAC      Next hop MAC    Relay
---- ---- ----------------- ----------------- -------
   1   63 00-1f-45-9e-3e-d1 00-00-00-10-00-00  MIP-DB
   2   62 00-00-00-10-00-00 00-00-00-00-00-00     Hit

S Chassis(su-config-cfm-mep.1000)->
```

loopback

Use this command to transmit CFM loopback messages to the specified MEP or MAC address.

Syntax

loopback {**mep** *mep-id* | **mac** *mac-addr*} [**messages** *num-messages*] [**priority** *priority*] [**data** *data*]

Parameters

mep *mep-id*	Specifies the MEP to send the loopback messages to.
mac *mac-addr*	Specifies the MAC address of the device to send the loopback messages to. Valid values are MAC addresses in the address format: *xx-xx-xx-xx-xx-xx* or *xx:xx:xx:xx:xx:xx* or *xxxx.xxxx.xxxx* where *x* is a hex value.
messages *num-messages*	(Optional) Specifies the number of loopback messages to transmit. Valid values are **1** - **1024**. Default value is **1**.
priority *priority*	(Optional) Specifies the priority to be used in the VLAN tag. Valid values are 0 - 7. The default value is the continuity check message priority value (see "priority" on page 50-29).
data *data*	(Optional) Specifies the data to be included in the Data TLV.

Defaults

- The number of loopback messages transmitted defaults to 1.
- The priority used in the VLAN tag defaults to the continuity check message priority value.
- If the data option is not specified, no data is sent with the Data TLV.

Mode

Maintenance End-Point Configuration mode.

Usage

The loopback protocol sends loopback messages (LBM) to either a specified maintenance end-point (MEP) or to the MAC address of a maintenance intermediate-point (MIP). The CFM loopback protocol displays whether there is connectivity between the initiating device and the target device. If an operational path to the MEP or MIP exists, the remote MEP or MIP will respond. If no response is received by the source MEP, no operational path exists. If no response is received use "linktrace" on page 50-26 to help verify where in the path the problem occurred.

The LBM priority can be configured using the **priority** option. The linktrace message shares the same priority as the continuity check message and can not be separately configured.

The **mep** option requires that the remote MEP has already communicated with this MEP and there is an entry in the MEP database for the remote MEP. The loopback will fail if the **mep** option is used and the remote MEP has not yet communicated with this MEP.

Example

This example shows how to send 5 loopback messages to MAC address **01:3a:b2:af:65:de** from the **myMA1** MEP **1000**:

```
S Chassis(rw-config)->cfm md string-name myMD1
```

```
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->mep 1000
S Chassis(su-config-cfm-mep.1000)->loopback mac 01:3a:b2:af:65:de messages 5
Sending 5 Ethernet CFM loopback messages to 01-3a-b2-af-65-de
...
Success rate is 100 percent (5/5)
S Chassis(su-config-cfm-mep.1000)->
```

port

Use this command to configure the bridge port the MEP is attached to.

Syntax

port *port*

no port

Parameters

port	Specifies the bridge port the MEP is attached to.

Defaults

None.

Mode

Maintenance End-Point Configuration mode.

Usage

The “no” form of this command deletes the MEP bridge port configuration.

Example

This example shows how to set **tg.1.1** as the port the **myMA1** MEP 1000 is attached to:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->mep 1000
S Chassis(su-config-cfm-mep.1000)->port tg.1.1
S Chassis(su-config-cfm-mep.1000)->
```

priority

Use this command to configure the 802.1 priority for continuity check messages and linktrace message sent by this MEP.

Syntax

priority *priority*

no priority

Parameters

priority	Specifies the priority for continuity check messages or linktrace messages sent by the MEP. Valid values are **0** - **7**. The default value is **1**.

Defaults

Continuity check message and linktrace message priority defaults to **1**.

Mode

Maintenance End-Point Configuration mode.

Usage

Continuity check priority values are inserted into the VLAN tag.

The "no" form of this command resets the continuity check message and linkstate message to the default value of **1**.

Example

This example shows how to set set the continuity check message and linkstate message priority for MEP **1000** to **3**:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->mep 1000
S Chassis(su-config-cfm-mep.1000)->priority 3
S Chassis(su-config-cfm-mep.1000)->
```

remote-mep active

Use this command to enable a remote MEP in the database for the current MEP.

Syntax

remote-mep *remote-mep-id* **active**

no remote-mep *remote-mep-id* **active**

Parameters

remote-mep-id	Specifies the remote MEP to enable in the database for the current MEP. Valid values are **1** - **8191**.

Defaults

End-points in the remote MEP database default to disabled.

Mode

Maintenance End-Point Configuration mode.

Usage

The local MEP exchanges continuity check messages with the remote MEP if the remote MEP is set to active. You must enable a remote MEP within the local MEP configuration context for the remote MEP to exchange PDUs with the local MEP and to be considered for defect generation.

Use “mep-list” on page 50-17 to enter remote MEPs into the remote MEP database.

The “no” form of this command disables the specified remote MEP in the database of the current MEP.

Example

This example shows how to enable remote MEP **2000** in the **myMA1** MEP **1000** database:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->mep 1000
S Chassis(su-config-cfm-mep.1000)->remote-mep 2000 active
S Chassis(su-config-cfm-mep.1000)->
```

reset-time

Use this command to configure the time a MEP defect must be absent before an alarm is reset.

Syntax

reset-time *time*

no reset-time

Parameters

time	Specifies the number of centiseconds a MEP defect must be absent before an alarm is reset. Valid values are 250 - 1000 centiseconds. The default value is **1000** centiseconds (10 seconds).

Defaults

1000 centiseconds (10 seconds).

Mode

Maintenance End-Point Configuration mode.

Usage

The “no” form of this command resets the amount of time a MEP defect must be absent before an alarm is reset to the default value of 250 centiseconds.

Example

This example shows how to set the amount of time a **myMA1** MEP **1000** defect must be absent before an alarm is reset to **3.5** seconds:

```
S Chassis(rw-config)->cfm md string-name myMD1
S Chassis(su-config-cfm-md.1)->ma string-name myMA1
S Chassis(su-config-cfm-ma.1)->mep 1000
```

```
S Chassis(su-config-cfm-mep.1000)->reset-time 350
S Chassis(su-config-cfm-mep.1000)->
```

CFM Clear Commands

This section lists the CFM **clear** commands. These commands are available in all configuration modes.

For information about...	Refer to page...
clear cfm bridge mip-ccm	50-32
clear cfm ccm-database	50-32
clear cfm counters	50-34

clear cfm bridge mip-ccm

Use this command to clear the CFM bridge MIP CCM database.

Syntax

clear cfm bridge mip-ccm

Parameters

None.

Defaults

None.

Mode

All command modes.

Examples

This example how to clear all CFM bridge MIP CCM database entries:

```
S Chassis(rw)->clear cfm bridge mip-ccm
S Chassis(rw)->
```

clear cfm ccm-database

Use this command to clear the check continuity message database for a specified MEP or all end-points for the specified context.

Syntax

Clear the CCM database for the specified or all end-points in the specified MD:

clear cfm ccm-database md {**string-name** *name* | **dns-like-name** *dns-name* | **mac-int-name** *mac-name* | **no-name** | **index** *index*} [**mep** *mep-id*]

Clear the CCM database for the specified or all endpoints in the specified MA:

```
clear cfm ccm-database md {string-name name | dns-like-name dns-name |
mac-int-name mac-name | no-name | index index} ma {string-name name | vid-name
vlan | id-name id | index index} [mep mep-id]
```

Clear the CCM database for the specified end-point:

```
clear cfm ccm-database md {string-name name | dns-like-name dns-name |
mac-int-name mac-name | no-name | index index} ma {string-name name | vid-name
vlan | id-name id | index index} mep mep-id
```

Parameters

md	Specifies an MD context.
ma	Specifies an MA context.
string-name *name*	Specifies the MD or MA string name of the CCM database to clear. Valid values are up to 43 printable characters.
dns-like-name *dns-name*	Specifies the MD DNS like string name of the CCM database to clear. Valid values are up to 43 printable characters.
mac-int-name *mac-name*	Specifies the MD MAC address formatted string name of the CCM database to clear. A valid value is a MAC address formatted string plus an integer index ID value separated by a period (.) in the format *xx-xx-xx-xx-xx-xx.ID* or *xx:xx:xx:xx:xx:xx.ID*, where *x* is a hex value and the *ID* range is **0** - **65535**.
no-name	Specifies the NULL string named MD of the CCM database to clear.
index *index*	Specifies the MD index value or the MA index of the CCM database to clear.
vid-name *vlan*	Specifies the MA VLAN ID name of the CCM database to clear.
id-name *id*	Specifies the MA ID name of the CCM database to clear.
index *index*	Specifies the MA index value of the CCM database to clear.
mep *mep-id*	(Optional) Specifies a maintenance end-point of the CCM database to clear.

Defaults

If the **mep** option is not specified, the CCM database for all end-points in the specified context are cleared.

Mode

All command modes.

Usage

This command only clears MEP database entries. MIP database entries are not affected.

Example

This example how to clear the CCM database for all end-points in the **myMA1** maintenance association:

```
S Chassis(rw)->clear cfm ccm-database md string-name myMD1 ma string-name myMA1
S Chassis(rw)->
```

clear cfm counters

Use this command to clear the MEP counters for a specified MEP or all end-points for the specified context.

Syntax

Clear the MEP counters for the specified or all end-points in the specified MD:

clear cfm counters md {**string-name** *name* | **dns-like-name** *dns-name* | **mac-int-name** *mac-name* | **no-name** | **index** *index*} [**mep** *mep-id*]

Clear the MEP counters for the specified or all endpoints in the specified MA:

clear cfm counters md {**string-name** *name* | **dns-like-name** *dns-name* | **mac-int-name** *mac-name* | **no-name** | **index** *index*} **ma** {**string-name** *name* | **vid-name** vlan | **id-name** *id* | **index** *index*} [**mep** *mep-id*]

Clear the MEP counters for the specified end-point:

clear cfm counters md {**string-name** *name* | **dns-like-name** *dns-name* | **mac-int-name** *mac-name* | **no-name** | **index** *index*} **ma** {**string-name** *name* | **vid-name** vlan | **id-name** *id* | **index** *index*} **mep** *mep-id*

Parameters

md	Specifies an MD context.
ma	Specifies an MA context.
string-name *name*	Specifies the MA or MA string name of the MEP counters to clear. Valid values are up to 43 printable characters.
dns-like-name *dns-name*	Specifies the MD DNS like string name of the MEP counters to clear. Valid values are up to 43 printable characters.
mac-int-name *mac-name*	Specifies the MD MAC address formatted string name of the MEP counters to clear. A valid value is a MAC address formatted string plus an integer index ID value separated by a period (.) in the format *xx-xx-xx-xx-xx-xx.ID* or *xx:xx:xx:xx:xx:xx.ID*, where *x* is a hex value and the *ID* range is **0** - **65535**.
no-name	Specifies the NULL string named MD of the MEP counters to clear.
index *index*	Specifies the MD index value or the MA index of the MEP counters to clear.
vid-name *vlan*	Specifies the MA VLAN ID name of the MEP counters to clear.
id-name *id*	Specifies the MA ID name of the MEP counters to clear.
index *index*	Specifies the MA index value of the MEP counters to clear.
mep *mep-id*	(Optional) Specifies a MEP of the MEP counters to clear.

Defaults

If the **mep** option is not specified, all end-point counters for the specified context are cleared.

Mode

All command modes.

Examples

This example how to clear the CCM database for all end-points in the myMaintenanceAssocation:

```
S Chassis(rw)->clear cfm ccm-database md string-name myMD1 ma string-name
myMaitenanceAssocation
S Chassis(rw)->
```

CFM Show Commands

This section lists the CFM **show** commands. These commands are available in all configuration modes.

For information about...	Refer to page...
show cfm all	50-35
show cfm bridge mip-ccm	50-37
show cfm default-md	50-37
show cfm md	50-38
show cfm md ma	50-40
show cfm md ma ma-comp	50-41
show cfm md ma mep	50-42
show cfm md ma mep ccm-errors	50-45
show cfm md ma mep linktrace	50-47
show cfm md ma mep-list	50-49
show cfm md ma mep remote-mep	50-50
show cfm md mip-ccm	50-52
show cfm stack-table	50-54
show cfm status	50-55

show cfm all

Use this command to display CFM status and configuration for all CFM MDs, associations, and end-points.

Syntax

show cfm all

Parameters

None.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to display CFM configuration and status for all MDs, associations, and end-points:

```
S Chassis(rw)->show cfm all
CFM global status is enabled

System Default MD values
  MD Level         : 0
  MHF Creation     : None
  MHF ID-permission: None


================================================================================

        MD               MD Name    MD      MHF     MHF       Next            MD
     Index             Name Type Level   Create    Perm   MA Index        Status
---------- ---------------- ---- ----- -------- ------- ---------- -------------
         2                 None     4     None    None          2        Active


--------------------------------------------------------------------------------
        MA                                     MA    Name      CCM            MA
     Index                                   Name    Type Interval        Status
---------- ---------------------------------------- ------- -------- -------------
         1                                  2000 Integer     1sec        Active

    Bridge                      MHF                MHF       MA Comp
    CompId        Selector   Create       ID-permission        Status
---------- --------------- -------- ------------------- -------------
         1        VID 2000    Defer       SendIdChassis        Active

      MEP-List
        Status
--------------
        Active : 1600-1601,1605-1610,1615-1624,8191

 MEP           Active        MEP  MEP    CCI               MAC           MEP
  ID         Selector       Port  Dir Enable              Addr        Status
---- ---------------- ---------- ---- ------ ----------------- -------------
1601         VID 2000    ge.2.15   Up   True 00-1f-45-9f-40-46        ActiveS
Chassis(rw)->
```

show cfm bridge mip-ccm

Use this command to display maintenance intermediate point (MIP) continuity check message database entries for MHFs that do not belong to a specific MD and MA.

Syntax

show cfm bridge mip-ccm [**vid** *vlan-id*]

Parameters

vid *vlan-id*	(Optional) Specifies the VLAN for the display of MIP continuity check message database entries.

Defaults

If the **vid** option is not specified, the output displays information for all VLANs in the database.

Mode

All command modes.

Examples

This example displays the bridge MIP continuity check message database information:

```
S Chassis(rw)->show cfm bridge mip-ccm
MPID        MAC Address       Port   FID  TimeStamp  Type    Value
----- ----------------- ---------- ----- ---------- ----- --------
   10 00-00-00-00-00-01    ge.2.17    10    4695000   VID       10
   10 00-00-00-00-00-02    ge.2.17    10    4695000   VID       10
   10 00-00-00-00-00-03    ge.2.17    10    4697000   VID       10
S Chassis(rw)->
```

show cfm default-md

Use this command to display the system level default MD or CFM service default values.

Syntax

show cfm default-md [**default** | **vid** *vlan-id*]

Parameters

default	(Optional) Displays system level MD default values.
vid *vlan-id*	(Optional) Displays CFM service default values for the specified VLAN.

Defaults

If no option is specified, both system level MD defaults and CFM service defaults for each service are displayed.

Mode

All command modes.

Examples

This example displays both system level defaults and CFM service defaults for each VLAN configured for defaults:

```
S Chassis(rw)->show cfm default-md
System Default MD values
  MD Level          : 0
  MHF Creation      : None
  MHF ID-permission: None

Default MD Values
VLAN ID MD level MHF-creation   MHF ID-permission Status
------- -------- ------------ ------------------- ------
     10        5        Defer               Defer   True
     20        5        Defer               Defer   True
S Chassis(rw)->
```

Table 50-2 provides an explanation of the command output.

Table 50-2 show cfm default-md Output Display

Output...	What it displays...
MD Level	The system default MD level.
MHF Creation	The maintenance intermediate-point creation behavior system default.
MHF ID-permission	The system default setting for the content sent in the SenderID TLV by the MD.
VLAN ID	The VLAN this MD default row applies to.
Status	**True** if this VLAN default configuration is enabled. **False** if this VLAN default configuration is disabled.

show cfm md

Use this command to display MD information for all or the specified MD.

Syntax

show cfm md [**string-name** *name* | **dns-like-name** *dns-name* | **mac-int-name** *mac-name* | **no-name** | **index** *index*]

Parameters

string-name *name*	(Optional) Displays MD configuration information for the specified MD string name. Valid values are up to 43 printable characters.
dns-like-name *dns-name*	(Optional) Displays MD configuration information for the specified DNS like MD string name. Valid values are up to 43 printable characters.

mac-int-name *mac-name*	(Optional) Displays MD configuration information for the specified MAC address formatted MD string name. Valid value is a MAC address formatted string plus an integer index ID value separated by a period (.) in the format *xx-xx-xx-xx-xx-xx.ID* or *xx:xx:xx:xx:xx:xx.ID*, where *x* is a hex value and the *ID* range is **0** - **65535**.
no-name	(Optional) Displays MD configuration information for the no name MD name.
index *index*	(Optional) Displays MD configuration information for the specified MD index value.

Defaults

If no option is specified, configuration information for all MDs is displayed.

Mode

All command modes.

Examples

This example displays MD information for **myMD1**:

```
S Chassis(rw)->show cfm md string-name myMD1


Maintenance Domain
 Index             : 3
 Name type         : Char string
 Name              : myMD1
 Level             : 0
 MHF creation      : None
 MHF ID-permission: None
 MA next index     : 5
 Row status        : Active
S Chassis(rw)->
```

Table 50-3 provides an explanation of the command output.

Table 50-3 show cfm md Output Display

Output...	What it displays...
Index	The MD index value.
Name type	The MD name type.
Name	The MD name.
Level	The MD level.
MHF creation	The maintenance intermediate-point creation behavior setting.
MHF ID-permission	The configuration setting for the content sent in the SenderID TLV by the MD.
MA next index	The next MA index value CFM will assign to a new MA.
Row status	The MD status.

show cfm md ma

Use this command to display configuration and status for a specified or all MAs for the specified MD.

Syntax

show cfm md {**string-name** *name* | **dns-like-name** *dns-name* | **mac-int-name** *mac-name* | **no-name** | **index** *index*} **ma** [**string-name** *name* | **vid-name** vlan | **id-name** *id* | **index** *index*]

Parameters

md	Specifies an MD context.
string-name *name*	(Optional for **ma**) Specifies the MD or MA string name for the MA configuration or status to display. Valid values are up to 43 printable characters.
dns-like-name *dns-name*	Specifies the MD DNS like MD string name for the MA configuration or status to display. Valid values are up to 43 printable characters.
mac-int-name *mac-name*	Specifies the MD MAC address formatted string name for the MA configuration or status to display. A valid value is a MAC address formatted string plus an integer index ID value separated by a period (.) in the format *xx-xx-xx-xx-xx-xx.ID* or *xx:xx:xx:xx:xx:xx.ID*, where *x* is a hex value and the *ID* range is **0** - **65535**.
no-name	Specifies the NULL string named MD for the MA configuration or status to display.
index *index*	(Optional for **ma**) Specifies the MD index value or the MA index for the MA configuration or status to display .
vid-name *vlan*	(Optional) Specifies the MA VLAN ID name for the MA configuration or status to display.
id-name *id*	(Optional) Specifies the MA ID name for the MA configuration or status to display.

Defaults

If no MA name option is specified, all MAs are displayed.

Mode

All command modes.

Examples

This example displays configuration information for all MAs in the **myMD1** MD:

```
S Chassis(rw)->show cfm md string-name myMD1 ma
MD Name: myMD1
        MA                                      MA    Name      CCM            MA
     Index                                    Name    Type Interval        Status
---------- ---------------------------------- ------- -------- -------------
         1               myMA1    Char     1sec        Active
         2                                  Doc1    Char     1sec        Active
S Chassis(rw)->
```

Table 50-4 provides an explanation of the command output.

Table 50-4 show cfm md ma Output Display

Output...	What it displays...
MD Name	The MD name the MAs displayed belong to.
MA Index	The MA index for this display line.
MA Name	The MA name.
Name Type	The configured MA name type.
CCM Interval	The interval between the sending of continuity check messages.
MA Status	The Status of the MA.

show cfm md ma ma-comp

Use this command to display the MA component configuration information.

Syntax

show cfm md {**string-name** *name* | **dns-like-name** *dns-name* | **mac-int-name** *mac-name* | **no-name** | **index** *index*} **ma** {**string-name** *name* | **vid-name** vlan | **id-name** *id* | **index** *index*} **ma-comp**

Parameters

md	Specifies an MD context.
ma	Specifies an MA context.
string-name *name*	Specifies the MD or MA string name of the MA component configuration to display. Valid values are up to 43 printable characters.
dns-like-name *dns-name*	Specifies the MD DNS like maintenance domain string name of the MA component configuration to display. Valid values are up to 43 printable characters.
mac-int-name *mac-name*	Specifies the MD MAC address formatted string name of the MA component configuration to display. A valid value is a MAC address formatted string plus an integer index ID value separated by a period (.) in the format *xx-xx-xx-xx-xx-xx.ID* or *xx:xx:xx:xx:xx:xx.ID*, where *x* is a hex value and the *ID* range is **0** - **65535**.
no-name	Specifies the NULL string named MD of the MA component configuration to display.
index *index*	Specifies the MD index value or the MA index of the MA component configuration to display.
vid-name *vlan*	Specifies the MA VLAN ID name of the MA component configuration to display.
id-name *id*	Specifies the MA ID name of the MA component configuration to display.
index *index*	Specifies the MA index value of the MA component configuration to display.

Defaults

None.

Mode

All command modes.

Examples

This example displays the component configuration for the **myMD1** index **1** MA:

```
S Chassis(rw)->show cfm md string-name myMD1 ma index 1 ma-comp

MD Name: myMD1
MA Name: myMA1
    Bridge    Sel        Sel      MHF                 MHF       MA Comp
    CompId   Type      Value   Create       ID-permission        Status
---------- ------ ---------- -------- ------------------- -------------
         1    VID          0    Defer               Defer        Active
S Chassis(rw)->
```

Table 50-5 provides an explanation of the command output.

Table 50-5 show cfm md ma ma-comp Output Display

Output...	What it displays...
MD Name	The MD name for the MA component configuration information to display.
MA Name	The MA name for the component configuration information to display.
Bridge CompID	The ID of the MA bridge component.
Sel Type	The service type protected: VID.
Sel Value	Protected service value.
MHF Create	The maintenance intermediate-point creation behavior setting.
MHF ID-permission	The configuration setting for the content sent in the SenderID TLV by the MD.
MA Comp Status	The MA component configuration status. Active (enabled) or Inactive (not enabled).

show cfm md ma mep

Use this command to display the MEP configuration information.

Syntax

show cfm md {**string-name** *name* | **dns-like-name** *dns-name* | **mac-int-name** *mac-name* | **no-name** | **index** *index*} **ma** {**string-name** *name* | **vid-name** vlan | **id-name** *id* | **index** *index*} **mep** [**mep-id** *mep-id*] [**-verbose**]

Parameters

md	Specifies an MD context.

ma	Specifies an MA context.
string-name *name*	Specifies the MD or MA string name of the MEP to display. Valid values are up to 43 printable characters.
dns-like-name *dns-name*	Specifies the MD DNS like maintenance domain string name of the MEP to display. Valid values are up to 43 printable characters.
mac-int-name *mac-name*	Specifies the MD MAC address formatted string name of the MEP to display. A valid value is a MAC address formatted string plus an integer index ID value separated by a period (.) in the format *xx-xx-xx-xx-xx-xx.ID* or *xx:xx:xx:xx:xx:xx.ID*, where *x* is a hex value and the *ID* range is **0** - **65535**.
no-name	Specifies the NULL string named MD of the MEP to display.
index *index*	Specifies the MD index value or the MA index of the MEP to display.
vid-name *vlan*	Specifies the MA VLAN ID name of the MEP to display.
id-name *id*	Specifies the MA ID name of the MEP to display.
index *index*	Specifies the MA index value of the MEP to display.
mep-id *mep-id*	(Optional) Specifies a MEP to display.
-verbose	(Optional) A detailed level of MEP configuration information will display.

Defaults

- If the MEP ID is not specified, all MEPs are displayed.
- If -verbose is not specified, a standard level of configuration information is displayed.

Mode

All command modes.

Examples

This example displays the MEP configuration information for the MA index **1** associated with the **myMD1** MD:

```
S Chassis(rw)->show cfm md string-name myMD1 ma index 1 mep

MD Name: myMD1
MA Name: myMA1
 MEP          Active         MEP  MEP    CCI               MAC            MEP
  ID        Selector        Port  Dir Enable             Addr         Status
---- -------------- ---------- ---- ------ ----------------- -------------
  59           None     tg.1.1 Down   True 00-1f-45-a0-9d-ab        Active
S Chassis(rw)->
```

This example displays the **verbose** level MEP configuration information for the MA index **1** associated with the **myMD1** MD:

```
S Chassis(rw)->show cfm md string-name myMD1 ma index 1 mep -verbose
MD Name: myMD1
MA Name: myMA1
  MEP ID: 59
```

```
    Active Selector  : None
    Primary VID      : 0
    IfIndex          : 13001
    Port             : tg.1.1
    MAC Address      : 00-1f-45-a0-9d-ab
    Direction        : Down
    Active           : True
    CCI Enabled      : True
    CCM/LTM Priority : 6
    FNG State        : Defect Reported
    HighestPriDefect : DefXconCCM
    FNG Alarm Time   : 500
    FNG Reset Time   : 500
    Low Pr Def       : RemErrXcon
    Low Pr Def Syslog: RemErrXcon
    Row Status       : Active
S Chassis(rw)->
```

Table 50-6 provides an explanation of the command output.

Table 50-6 show cfm md ma mep Output Display

Output...	What it displays...
MD Name	The name of the MD to which the MEP belongs.
MA Name	The name of the MA to which the MEP belongs.
MEP ID	The MEP.
Active Selector	Protected service value for this MEP. Defaults to MA component configuration if no VLAN is configured for this end-point.
Primary VID	The VLAN the MEP uses as a tagging option for its transmitted frames.
MEP Port	The bridge port the MEP is attached to.
MEP Dir or Direction	Specifies the direction of the MEP. Down: sends PDU messages away from the MAC relay entity. Up: sends PDU messages towards the MAC relay entity.
CCI Enable	Specifies whether the MEP generates continuity check messages. True: continuity check messages are generated. False: continuity check messages are not generated.
CCM/LTM Priority	The continuity check message and linktrace message priority for the end-point.
MAC Addr	The MEP MAC address.
MEP Status or Active	The MEP configuration status: Active (enabled) or Inactive (not enabled).
FNG State	Defect reported status. Either a defect is currently being reported or the status is reset.
HighestPriDefect	Displays the highest priority defect reported. See “MEP Defect Definitions” on page 50-22 for descriptions of reported defects.

Table 50-6 show cfm md ma mep Output Display

Output...	What it displays...
FNG Alarm Time	Displays the minimum time a defect must be present before an alarm is generated.
FNG Reset Time	Displays the time a MEP defect must be absent before an alarm is reset.
Low Pr Def	The lowest priority defect for trap reporting. See “alarm-defect-trap” on page 50-23.
Low Pr Def Syslog	The lowest priority defect for Syslog reporting. See “alarm-defect-syslog” on page 50-22.
Row Status	Displays the administrative status for this MEP state machine.

show cfm md ma mep ccm-errors

Use this command to display the error conditions in the MEP continuity check message database.

show cfm md {**string-name** *name* | **dns-like-name** *dns-name* | **mac-int-name** *mac-name* | **no-name** | **index** *index*} **ma** {**string-name** *name* | **vid-name** vlan | **id-name** *id* | **index** *index*} **mep** [**mep-id** *mep-id*] **ccm-errors** [**-verbose**]

Parameters

md	Specifies an MD context.
ma	Specifies an MA context.
mep	Specifies a MEP context.
string-name *name*	Specifies the MD or association string name of the continuity check message errors to display. Valid values are up to 43 printable characters.
dns-like-name *dns-name*	Specifies the MD DNS like string name of the continuity check message errors to display. Valid values are up to 43 printable characters.
mac-int-name *mac-name*	Specifies the MD MAC address formatted string name of the continuity check message errors to display. A valid value is a MAC address formatted string plus an integer index ID value separated by a period (.) in the format *xx-xx-xx-xx-xx-xx.ID* or *xx:xx:xx:xx:xx:xx.ID*, where *x* is a hex value and the *ID* range is **0** - **65535**.
no-name	Specifies the NULL string named MD of the continuity check message errors to display.
index *index*	Specifies the MD index value or the MA index of the continuity check message errors to display.
vid-name *vlan*	Specifies the MA VLAN ID name of the continuity check message errors to display.
id-name *id*	Specifies the MA ID name of the continuity check message errors to display.
index *index*	Specifies the MA index value of the continuity check message errors to display.
mep-id *mep-id*	(Optional) Specifies a MEP of the continuity check message errors to display.

-verbose	(Optional) A detailed level of continuity check message errors will display.

Defaults

- If no MEP ID is specified, continuity check message error information will display for all end-points.
- If the -verbose option is not specified, a standard level for continuity check message errors will display.

Mode

All command modes.

Examples

This example displays the error conditions in the MEP continuity check message database for MEP **59**, of MA index **1**, of the **myMA1** MA:

```
S Chassis(rw)->show cfm md string-name myMD1 ma index 1 mep mep-id  59 ccm-errors

MD Name: myMD1
MA Name: myMA1
MEP ID : 59
========
Number of out-of-sequence CCMs errors received from all remote MEPs: 23

Outstanding Defects:
DefRDICcm DefMACStatus DefRemoteCCM DefErrorCCM DefXconCCM
       No           No          Yes          No        Yes

Highest Priority Defect occurred: DefXconCCM

Last CCM Failure:
             Tag         RemoteMAC        Type
--------------- ----------------- -----------
            None 00-1f-45-e9-2b-19  DefXconCCM
S Chassis(rw)->
```

Table 50-7 provides an explanation of the command output.

Table 50-7 show cfm md ma mep ccm-errors Output Display

Output...	What it displays...
MD Name	The MD name.
MA Name	The MA name
MEP ID	The MEP ID.
Outstanding Defects	Specifies whether there are outstanding defects for each defect type. See Table 50-1 on page 50-22 for a description of defect types.

Table 50-7 show cfm md ma mep ccm-errors Output Display

Output...	What it displays...
Highest Priority Defect occurred	The defect type of the highest priority defect that has occurred. See Table 50-1 on page 50-22 for a description of defect types.
Last CCM Failure	The last continuity check message failure details.
Tag	The VLAN-ID of the CCM packet as reported in the CCM error table header.
RemoteMac	The remote end-point MAC address.
Type	Specifies the defect type reported. See Table 50-1 on page 50-22 for a description of defect types.

show cfm md ma mep linktrace

Use this command to display linktrace database information for all or the specified end-point.

show cfm md {**string-name** *name* | **dns-like-name** *dns-name* | **mac-int-name** *mac-name* | **no-name** | **index** *index*} **ma** {**string-name** *name* | **vid-name** vlan | **id-name** *id* | **index** *index*} **mep** [**mep-id** *mep-id*] **linktrace**

Parameters

md	Specifies an MD context.
ma	Specifies an MA context.
mep	Specifies a maintenance end-point context.
string-name *name*	Specifies the MD or association string name of the linktrace database information to display. Valid values are up to 43 printable characters.
dns-like-name *dns-name*	Specifies the MD DNS like string name of the linktrace database information to display. Valid values are up to 43 printable characters.
mac-int-name *mac-name*	Specifies the MD MAC address formatted string name of the linktrace database information to display. A valid value is a MAC address formatted string plus an integer index ID value separated by a period (.) in the format *xx-xx-xx-xx-xx-xx.ID* or *xx:xx:xx:xx:xx:xx.ID*, where *x* is a hex value and the *ID* range is **0** - **65535**.
no-name	Specifies the NULL string named MD of the linktrace database information to display.
index *index*	Specifies the MD index value or the MA index of the linktrace database information to display.
vid-name *vlan*	Specifies the MA VLAN ID name of the linktrace database information to display.
id-name *id*	Specifies the MA ID name of the linktrace database information to display.
index *index*	Specifies the MA index value of the linktrace database information to display.
mep-id *mep-id*	(Optional) Specifies a MEP of the linktrace database information to display.

Defaults

- If a MEP ID is not specified, information for all end-points is displayed.
- If the **-verbose** option is not specified, a standard level of information is displayed that displays only the direct path between the originating MEP and the target maintenance point. If **-verbose** is specified, all paths linktrace discovered through the topology are displayed.

Mode

All command modes.

Examples

This example displays the linktrace database information for MEP **59**, for the MA index **1**, for the **myMD1** MD:

```
S Chassis(rw)->>show cfm md string-name myMD1 ma index 1 mep mep-id 59 linktrace
MD Name: abc
MA Name: abc
MEP ID : 1, Interface ge.4.18
=====================================================
Hop  TTL        Source MAC      Next hop MAC    Relay
---- ---- ----------------- ----------------- -------
Transaction ID 29476
   1    63 00-1f-45-9e-3e-d1 00-00-00-10-00-00  MIP-DB
   2    62 00-00-00-10-00-00 00-00-00-00-00-00     Hit

Transaction ID 29477
   1    63 00-1f-45-9e-3e-d1 00-00-00-10-00-00  MIP-DB
   2    62 00-00-00-10-00-00 00-00-00-00-00-00     Hit

Transaction ID 29479
   1    63 00-1f-45-9e-3e-d1 00-00-00-00-00-00     Hit

Transaction ID 29480
   1    63 00-1f-45-9e-3e-d1 00-00-00-10-00-00  MIP-DB
   2    62 00-00-00-10-00-00 00-00-00-00-00-00     Hit

Transaction ID 29481
   1    63 00-1f-45-9e-3e-d1 00-00-00-10-00-00  MIP-DB
   2    62 00-00-00-10-00-00 00-00-00-00-00-00     Hit
S Chassis(rw)->
```

Table 50-8 provides an explanation of the command output.

Table 50-8 show cfm md ma mep linktrace Output Display

Output...	What it displays...
MD Name	The maintenance domain name.
MA Name	The MA name

Table 50-8 show cfm md ma mep linktrace Output Display

Output...	What it displays...
MEP ID	The maintenance end-point ID.
Interface	Source port for this linktrace
Hop	Hops from the source for this entry.
TTL	Time-To-Live; the maximum number of hops remaining before the link trace terminates.
Source MAC	The linktrace source MAC address.
Next hop MAC	The linktrace next hop MAC address.
Relay	The database the linktrace protocol used for the displayed information: Filter database (FDB), maintenance intermediate-point database (MIP-DB) or the MEP replying is the target maintenance point of the linktrace (Hit).
Transaction ID	A unique transaction ID for this linktrace information.

show cfm md ma mep-list

Use this command to display the MA MEP list.

Syntax

show cfm md {**string-name** *name* | **dns-like-name** *dns-name* | **mac-int-name** *mac-name* | **no-name** | **index** *index*} **ma** {**string-name** *name* | **vid-name** vlan | **id-name** *id* | **index** *index*} **mep-list**

Parameters

md	Specifies an MD context.
ma	Specifies an MA context.
string-name *name*	Specifies the MD or MA string name of the MEP list to display. Valid values are up to 43 printable characters.
dns-like-name *dns-name*	Specifies the MD DNS like maintenance domain string name of the MEP list to display. Valid values are up to 43 printable characters.
mac-int-name *mac-name*	Specifies the MD MAC address formatted string name of the MEP list to display. A valid value is a MAC address formatted string plus an integer index ID value separated by a period (.) in the format *xx-xx-xx-xx-xx-xx.ID* or *xx:xx:xx:xx:xx:xx.ID*, where *x* is a hex value and the *ID* range is **0** - **65535**.
no-name	Specifies the NULL string named MD of the MEP list to display.
index *index*	Specifies the MD index or the MA index of the MEP list to display.
vid-name *vlan*	Specifies the MA VLAN ID name of the MEP list to display.
id-name *id*	Specifies the MA ID name of the MEP list to display.
index *index*	Specifies the MA index value of the MEP list to display.

Defaults

None.

Mode

All command modes.

Examples

This example displays MEP list information for the **myMA1** MA:

```
S Chassis(rw)->show cfm md string-name myMD1 ma index 1 mep-list
MD Name: myMD1
MA Name: myMA1
MEP List        Status
-------- -------------
    1000        Active
    2000        Active
S Chassis(rw)->
```

Table 50-9 provides an explanation of the command output.

Table 50-9 show cfm md ma mep-list Output Display

Output...	What it displays...
MD Name	The name of the MD to which the MEP list belongs.
MA Name	The name of the MA to which the MEP list belongs.
MEP List	A member of the MEP list.
Status	The MEP configuration status: Active (enabled) or Inactive (not enabled).

show cfm md ma mep remote-mep

Use this command to display the MEP's remote MEP configuration information.

Syntax

show cfm md {**string-name** *name* | **dns-like-name** *dns-name* | **mac-int-name** *mac-name* | **no-name** | **index** *index*} **ma** {**string-name** *name* | **vid-name** vlan | **id-name** *id* | **index** *index*} **mep** [**mep-id** *mep-id*] **remote-mep** [**mep-id** *mep-id*] [**-verbose**]

Parameters

md	Specifies an MD context.
ma	Specifies an MA context.
mep	Specifies a maintenance end-point context.
string-name *name*	Specifies the MD or MA string name of the of the remote MEP to display. Valid values are up to 43 printable characters.
dns-like-name *dns-name*	Specifies the MD DNS like maintenance domain string name of the remote MEP to display. Valid values are up to 43 printable characters.

mac-int-name *mac-name*	Specifies the MD MAC address formatted string name of the remote MEP to display. A valid value is a MAC address formatted string plus an integer index ID value separated by a period (.) in the format *xx-xx-xx-xx-xx-xx.ID* or *xx:xx:xx:xx:xx:xx.ID*, where *x* is a hex value and the *ID* range is **0** - **65535**.
no-name	Specifies the NULL string named MD of the remote MEP to display.
index *index*	Specifies the MD index value or the MA index of the remote MEP to display.
vid-name *vlan*	Specifies the MA VLAN ID name of the remote MEP to display.
id-name *id*	Specifies the MA ID name for the end-point of the remote end-point to display.
index *index*	Specifies the MA index value of the remote MEP to display.
mep-id *mep-id*	(Optional) Specify a maintenance end-point or its remote end-point.
-verbose	(Optional) A detailed level of maintenance remote end-point configuration information will display.

Defaults

- If the MEP ID or the remote end-point ID is not specified, all maintenance and associated remote end-points are displayed.
- If **-verbose** is not specified, a standard level of configuration information is displayed.

Mode

All command modes.

Examples

This example displays the remote-end-point configuration information for the MA index **1**, MEP **59**, for the **myMD1** MD:

```
S Chassis(rw)->show cfm md string-name myMD1 ma index 1 mep mep-id  59 remote-mep

MD Name: myMD1
MA Name: myMA1
MEP ID : 59
Remote    RMep              RMep   RMep    RDI
 MepId   State               MAC Active    Set
------ ------- ----------------- ------ ------
    57  Failed 00-11-88-fd-93-4e   True  False
S Chassis(rw)->
```

This example displays the **verbose** level remote MEP configuration information for the MA index **1**, MEP **59**, for the **myMD1** MD:

```
S Chassis(rw)->show cfm md string-name myMD1 ma index 1 mep 59 remote-mep -verbose

MD Name: myMD1
MA Name: myMA1
MEP ID : 59
  RMEP ID 57
```

```
    State                    : Failed
    MAC Address              : 00-11-88-fd-93-4e
    Active                   : True
    RDI bit set              : False
    OK Time (centiseconds)   : 41601115
    Port Status TLV          : Up
    Interface Status TLV     : Up
    SenderID TLV             : None
S Chassis(rw)->
```

Table 50-10 provides an explanation of the command output.

Table 50-10 show cfm md ma mep remote-mep Output Display

Output...	What it displays...
MD Name	The name of the MD to which the MEP belongs.
MA Name	The name of the MA to which the MEP belongs.
MEP ID	The maintenance end-point ID.
Remote MEP ID or RMEP ID	The Remote maintenance end-point ID.
RMEP State or State	The administrative state of the remote MEP.
RMEP MAC or MAC Address	The MAC address of the remote MEP.
Active	The MEP configuration status: True (enabled) or False (not enabled).
RDI bit set	State of the RDI bit. True: RDI bit is set. False: RDI bit is not set.
OK time (centiseconds)	The system time the remote MEP became active.
Port Status TLV	Status of the physical port the remote MEP resides on.
Interface Status TLV	Status of the remote MEP.
SenderID TLV	ID permission setting for the content sent in the SenderID TLV by the remote MEP.

show cfm md mip-ccm

Use this command to display maintenance intermediate point (MIP) continuity check message information by MD, MA, or MEP.

Syntax

Display by MD:

show cfm md {**string-name** *name* | **dns-like-name** *dns-name* | **mac-int-name** *mac-name* | **no-name** | **index** *index*} **mip-ccm** [**vid** *vlan-id*]

Display by MA:

show cfm md {**string-name** *name* | **dns-like-name** *dns-name* | **mac-int-name** *mac-name* | **no-name** | **index** *index*} **ma** {**string-name** *name* | **vid-name** vlan | **id-name** *id* | **index** *index*} **mip-ccm** [**vid** *vlan-id*]

Display by MEP:

```
show cfm md {string-name name | dns-like-name dns-name | mac-int-name mac-name |
no-name | index index} ma {string-name name | vid-name vlan | id-name id | index
index} mep [mep-id mep-id] mip-ccm [vid vlan-id]
```

Parameters

md	Specifies an MD context.
ma	Specifies an MA context.
mep	Specifies a maintenance end-point context.
string-name *name*	Specifies the MD or MA string name of the MIP continuity check information to display. Valid values are up to 43 printable characters.
dns-like-name *dns-name*	Specifies the MD DNS like string name of the MIP continuity check information to display. Valid values are up to 43 printable characters.
mac-int-name *mac-name*	Specifies the MD MAC address formatted string name of the MIP continuity check information to display. A valid value is a MAC address formatted string plus an integer index ID value separated by a period (.) in the format *xx-xx-xx-xx-xx-xx.ID* or *xx:xx:xx:xx:xx:xx.ID*, where *x* is a hex value and the *ID* range is **0** - **65535**.
no-name	Specifies the NULL string named MD of the MIP continuity check information to display.
index *index*	Specifies the MD index value or the MA index of the MIP continuity check information to display.
vid-name *vlan*	Specifies the MA VLAN ID name of the MIP continuity check information to display.
id-name *id*	Specifies the MA ID name of the MIP continuity check information to display.
index *index*	Specifies the MA index value of the MIP continuity check information to display.
mep-id *mep-id*	(Optional) Specifies a maintenance end-point of the MIP continuity check information to display.
-verbose	(Optional) A detailed level of MIP continuity check information will display.
vid *vlan-id*	(Optional) Specifies the VLAN entry of MIP continuity check message information to display.

Defaults

- If the **mep-id** option is not specified, MIP continuity check information for all end-points will display.
- If the **-verbose** option is not specified, a standard level of information displays.
- If the **vid** option is not specified, the output displays information for all VLANs in the database.

Mode

All command modes.

Examples

This example displays the **myMD1**, association index **2** MIP continuity check message database information:

```
S Chassis(rw)->show cfm md string-name myMD1 ma string-name
myMaintenaceAssocation2 mip-ccm


MD Name: myMD1
MA Name: myMA12
MPID       MAC Address       Port   FID  TimeStamp  Type    Value
-----  -----------------  ----------  -----  ----------  -----  --------
   10  00-00-00-00-00-06    ge.2.17    10     197190   VID       10
   10  00-00-00-00-00-07    ge.2.17    10     197190   VID       10
   10  00-00-00-00-00-08    ge.2.17    10     199190   VID       10
   10  00-00-00-10-00-02    ge.2.17    10     197190   VID       10
   10  00-00-00-10-00-03    ge.2.17    10     197190   VID       10
S Chassis(rw)->
```

Table 50-11 provides an explanation of the command output.

Table 50-11 show cfm md mip-ccm Output Display

Output...	What it displays...
MD Name	Maintenance domain name.
MA Name	MA name.
MPID	Maintenance point ID.
MAC Address	MEP MAC address.
Port	MEP port.
FID	Filter database ID.
TimeStamp	A counter in centiseconds specifying the time since the last continuity check message was received.
Type	Protected service type.
Value	Protected service value.

show cfm stack-table

Use this command to display the stack table which contains maintenance point information for each maintenance point for the device (MEP and MIP).

Syntax

```
show cfm stack-table
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Examples

This example displays maintenance point information by interface:

```
S Chassis(rw)->show cfm stack-table

        MP    Sel       Sel    MD    MP          MD          MA    MP                MAC
      Port   Type       Val   Lvl   Dir       Index       Index    ID            Address
---------- ----- -------- ---- ---- ---------- ---------- ---- -----------------
   ge.1.48   VID      1000    0    Up          1          1 1003 00-1f-45-a0-9d-aa
    tg.1.1   VID         0    0 Down          3          1   59 00-1f-45-a0-9d-ab
    tg.1.1   VID      2000    4 Down          2          1 1601 00-1f-45-a0-9d-ab
S Chassis(rw)->
```

Table 50-12 provides an explanation of the command output.

Table 50-12 show cfm stack-table Output Display

Output...	What it displays...
MP Port	Maintenance end- or intermediate-point port ID.
Sel Type	CFM service type.
Sel Value	CFM service value.
MD Lvl	Maintenance domain level.
MP Dir	Maintenance end- or intermediate-point direction.
MD Index	Maintenance domain index value.
MA Index	MA index value.
MP ID	Maintenance end- or intermediate-point ID. An MP ID of 0 denotes a maintenance intermediate-point (MIP).
MAC Address	MEP MAC address.

show cfm status

Use this command to display the global CFM status for this device.

Syntax

show cfm status

Parameters

None.

Defaults

None.

Mode

All command modes.

Examples

This example displays the global CFM status for the device:

```
S Chassis(rw)->show cfm status
CFM global status is enabled
S Chassis(rw)->
```

51

Virtual Routing and Forwarding (VRF) Commands

This chapter describes the Virtual Routing and Fowarding (VRF) set of commands and how to use them. For information about configuring VRF, refer to the "Virtual Routing and Fowarding (VRF) Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
set router vrf create	51-1
clear router vrf	51-2

set router vrf create

Use this command to create a VRF router.

Syntax

set router vrf create *vrf-name* [**context** *context-name*]

Parameters

vrf-name	Specifies the name of the VRF router. Valid values are up to 32 printable characters.
context *context-name*	(Optional) Specifies the SNMPv3 context for this VRF router. Valid values are up to 28 printable characters. The default value is the specified VRF name.

Defaults

If the **context** *context-name* parameter is not specified, the SNMPv3 context defaults to the VRF name.

Mode

All command modes.

Usage

Space characters are not supported in either a VRF name or SNMPv3 context name.

The **context** *context-name* parameter must be specified if the VRF name is greater than 28 characters.

The **global** VRF router is the default router for the device.

Examples

This example creates the VRF router nat1:

```
S Chassis(su)->set router vrf create nat1
S Chassis(su)->router nat1
S Chassis(su-nat1)->show router
VRF Context    : nat1
RD             : not set
S Chassis(su)->
```

clear router vrf

Use this command to delete the specified VRF and all its configuration from the device or to write a blank configuration to the global router.

Syntax

clear router vrf *vrf-name*

Parameters

vrf-name	Specifies the name of the VRF router to delete.

Defaults

None.

Mode

All command modes.

Usage

This command is a powerful command that removes the specified VRF router.

When the **global** router is specified, the command effectively writes a blank configuration file to persistent memory. Unless the user is attached via a direct console connection, loss of management connectivity to the device should be expected. Before using this command, save the current configuration using the **show config** *outfile* command.

Example

This example shows how to clear the **global** VRF router configuration:

```
S Chassis(rw)->clear router vrf global
```

This example shows how to delete the **nat1** VRF router:

```
S Chassis(rw)->clear router vrf nat1
```

52

Global Configuration Address Family Commands

This chapter describes the global configuration address family set of commands and how to use them. For information about configuring the global configuration address family, refer to the "xxx Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
address-family	52-1
topology	52-2

address-family

Use this command to enter global address family configuration mode.

Syntax

address-family {**ipv4** | **ipv6**} **multicast**

no address-family {**ipv4** | **ipv6**} **multicast**

Parameters

ipv4 | ipv6	Specifies the IPv4 or IPv6 address family.
multicast	Specifies the multicast sub-address family.

Defaults

None.

Mode

Router configuration mode.

Usage

Use the **no** form of this command to disable and remove the address family (and its topology) from the router configuration.

Use the **exit** command to exit address family configuration mode.

Examples

This example shows how to enter the configuration mode for the IPv4 multicast address family:

```
S Chassis(su-router-config)->address-family ipv4 multicast
```

topology

Use this command to create a global topology instance and enter routing topology configuration mode.

Syntax

topology *<topology-name>*

no topology *<topology-name>*

Parameters

<topology-name>	Specifies the name of the topology instance. *<topology-name>* is alphanumeric, case-sensitive string.

Defaults

None.

Mode

Router configuration address-family mode.

Usage

Use the **no** form of this command to disable and remove the topology from the router configuration.

Examples

This example shows how to create topology Router3:

```
S Chassis(su-router-config-af)->topology Router3
```

53

Router Commands

This chapter provides details for the router set of commands, including router information and limits display, entering router configuration mode, and display of the running configuration for the router. For information about configuring routing commands, refer to the "IP Routing Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show router	53-1
show limits	53-3
set limits	53-6
clear limits	53-7
set router vrf create	53-8
clear router vrf	53-9
router	53-9
show running-config	53-10

show router

Use this command to display VRF router and router application information for this system.

Syntax

```
show router [vrf [name] {interfaces [interface-name] | summary [vrf-name]| vpn-id
[oui:vpn-index]]
```

Parameters

vrf *name*	(Optional) Specifies the VRF router name of the router to display. The default value is the current router context.
interfaces	Display all interfaces for the specified VRF.
interface-name	(Optional) Display the specified VRF interface. Use *media.slot.port* format.
summary	Display a summary level of information.
vrf-name	Display a summary level of information for the specified VRF.
vpn-id	Display VPN identifier router information.
oui:*vpn-index*	Display VPN identifier router information for the specified VPN identifier.

Defaults

- If no option is specified, the global router context displays.
- If a VRF name is not specified, all VRFs display.
- If an interface name is not specified, all interfaces for the VRF display.
- If a VPN identifier is not specified, information for all VPN identifiers display.

The **global** router is the default router for the device.

Mode

All command modes.

Example

This example displays the VRF router for the current context:

```
S Chassis(rw)->show router
VRF Context    : global
RD             : not set
S Chassis(rw)->
```

This example displays a summary line for each VRF router on the device:

```
S Chassis(rw)->show router vrf summary

Name(truncated)                  Route distinguisher    Protocols Interfaces
-------------------------------- ---------------------- --------- -----------
global                           not set                ipv4,ipv6 vlan.0.151
                                                                  vlan.0.1051
                                                                  vlan.0.1056
                                                                  vlan.0.1057
                                                                  lo.0.1
                                                                  loop.0.1
nat1                             not set                ipv4,ipv6 vlan.0.212
                                                                  vlan.0.1151
                                                                  lo.0.2
nat2                             not set                ipv4,ipv6 vlan.0.1251
                                                                  vlan.0.1256
                                                                  vlan.0.1257
                                                                  vlan.0.1903
                                                                  lo.0.3
nat3                             not set                ipv4,ipv6 vlan.0.1351
                                                                  vlan.0.1356
                                                                  vlan.0.1357
                                                                  vlan.0.1904
                                                                  lo.0.4
S Chassis(rw)->
```

show limits

Use this command to display the all limits configured for this system or by application or VRF.

Syntax

show limits [**vrf** *vrf*] [**resource-ipv6netmask**] [**application** *application*]

Parameters

vrf *vrf*	(Optional) Displays router limits information for the specified VRF.
resource-ipv6netmask	(Optional) Displays the current IPv6 netmask setting.
application *application*	(Optional) Displays router limits information for the specified application. Entering the command without specifying the application option displays all supported application keywords.

Defaults

If display options are not specified, router limits for all VRFs and supported applications will display.

Pressing <Enter> after the **application** keyword displays all supported applications.

Mode

All command modes.

Examples,

This example displays the limits configured for all applications on this system:

```
S Chassis(rw)->show limits

Chassis limits:
Application                          Limit    In use   Entry size  Total Memory
-------------------------------- --------- --------- ------------ ------------
access-lists                          1000        12         6.2K           6M
  access-list-entries                 5000        44         160B       781.4K
  access-list-entries-per-list        5000         -            -            -
  applied-access-lists                4096         0          80B       321.1K
    applied-ipv4-in                   1024         0           -            -
    applied-ipv4-out                  1024         0           -            -
    applied-ipv6-in                   1024         0           -            -
    applied-ipv6-out                  1024         0           -            -
appsvc-ftp-alg-entries                8000         0          40B       312.5K
appsvc-global-bindings              131072         0         200B          25M
bgp-route-map-clauses                 1000         0         572B       558.6K
crypto-ike-maps                         10         0         252B         2.5K
crypto-ike-policies                     10         0         260B         2.5K
crypto-ike-proposals                    20         0         216B         4.2K
crypto-ipsec-maps                       10         0         208B           2K
dhcp-leases                           5120         0          56B         280K
```

ethernet-cfm	-	0	1B	-
ethernet-oam	-	0	1B	-
fib-ipv4-routes	500000	-	203B	96.8M
fib-ipv6-routes	50000	-	244B	11.6M
fib-nexthops	4096	-	56B	224K
ip-addresses	4373	29	-	-
ip-interface-addresses	128	-	-	-
ip-interfaces	1362	27	-	-
dns-names	1280	0	4B	5K
ipv6-enabled-interfaces	256	11	-	-
lo-interfaces	128	4	-	-
lpbk-interfaces	160	3	-	-
tunnel-interfaces	50	0	-	-
vlan-interfaces	1024	20	-	-
ipsec-dynamic-flow	400	0	268B	104.7K
ipsec-dynamic-instances	192	-	116B	21.8K
ipsec-dynamic-sa	400	0	364B	142.2K
ipsec-static-flow	256	0	268B	67K
ipsec-static-instances	64	-	116B	7.3K
ipsec-static-sa	128	0	364B	45.5K
linkstate-application	1	1	15.5K	15.5K
linkstate-entries	16	0	412B	6.4K
linkstate-if-entries	256	0	28B	7K
mrp	-	0	1B	-
mvrp	-	0	1B	-
multicast-access-lists	1024	2	96B	96K
multicast-flows	8192	87	148B	1.2M
nat-global-bindings	131072	0	20B	2.5M
nat-ip-addresses	2000	0	52B	101.6K
nat-list-rules	10	0	0B	0B
nat-pools	10	0	352B	3.4K
nat-portmapped-addresses	20	0	8.6K	171.9K
nat-static-rules	1000	0	336B	328.1K
nd-dynamic-entries	65535	27	84B	5.2M
nd-static-entries	2048	0	88B	176K
reframer Basic-Routing/Nat	245760	0	136B	31.9M
route-map-clauses	2000	0	572B	1.1M
route-map-names	800	0	152B	118.8K
bgp-route-map-names	100	0	152B	14.8K
filter-route-map-names	100	0	152B	14.8K
policy-route-map-names	512	0	152B	76K
redistribution-route-map-names	100	0	152B	14.8K
route-map-next-hops	128	128	40B	5K
route-map-probe	128	0	88B	11K
routing-protocols	-	-	-	-

```
    bgp-ipv4-rib-in-routes          100000         0          68B          6.5M
    bgp-ipv6-rib-in-routes           16000         0          68B            1M
    dvmrp-flows                       8192         0         276B          2.2M
    dvmrp-routes                      3000         0         160B        468.8K
    isis-ls-entries                  50000         0          64B          3.1M
    ospf-ls-entries                  50000        90         152B          7.2M
    ospfv3-ls-entries                16000         0         152B          2.3M
    pim-flows                         8192        87         124B          992K
    rip-routes                        3000         9          48B        140.6K
slb-global-bindings                131072         0          20B          2.5M
slb-reals                             800         0         260B        203.1K
slb-serverfarms                       400         0         252B         98.4K
slb-sticky-entries                 131072         0          84B         10.5M
slb-vip-addresses                    1000         0         116B        113.3K
slb-vservers                          500         0         1.1K        525.4K
static-routes                        2048         7         176B          352K
trackobj-probe                        128        10         280B           35K
  ACVs                                 64         0         416B           26K
  sessions                           2000         0         296B        578.1K
trackobj-track                        128         0         712B           89K
  trackobj-if-entries                 256         0           0B            0B
twcb-caches                           500         0         264B        128.9K
twcb-global-bindings               131072         0          20B          2.5M
twcb-wcserverfarms                    50         0         972B         47.5K
twcb-webcaches                        50         0         2.7K        133.4K
vrf                                  128         4           0B            0B
  vrf-ip-interfaces                 1362         -           -             -
vrrp-associate-ips                   2048         0          40B           80K
vrrp-critical-ips                    2048         0          40B           80K
vrrp-interface-vrids                    8         -           -             -
vrrp-vrids                           1024         0         244B          244K
  vrid-critical-addresses              10         -           -             -
  vrid-ipv4-addresses                 128         -           -             -
  vrid-ipv6-addresses                  64         -           -             -
Total Memory                            -         -           -        118.6M
```

This example displays the resource limits for TWCB bindings for this system:

```
S Chassis(rw)->show limits application twcb-global-bindings

Application: twcb-global-bindings
Description: Maximum TWCB bindings

VRF NAME                          limit   in use reserved
-------------------------------- -------- -------- --------
global                           131072        0        0
```

```
vrf2_pim                              131072        0        0
mt                                    131072        0        0

Chassis Total Resources .............     131072
Chassis Total Reserved  .............          0
Chassis Total Reserved Available ....          0
Chassis Total Unreserved Available ..     131072
```

set limits

Use this command to set the resource limit for the specified application and VRF.

Syntax

set limits [**vrf** *vrf-name*] [**resource-ipv6netmask** {**default** | **full**}] *application limit*

Parameters

vrf *vrf-name*	(Optional) Specifies the name of the VRF to which the resource limit applies.
resource-ipv6netmask default | **full**	(Optional) Specifies the IPv6 netmask setting: **default** = 64-bit mask, **full** = 128-bit mask. The default is **default**.
application	Specifies the application to which the resource limit applies.
limit	Specifies the resource limit value.

Defaults

The IPv6 netmask defaults to **default** (64-bit).

Mode

All command modes.

Usage

Use the **set limits** command to limit the resources, for the specified application, to a value up to the global limit for that application. Resource limits for all applications, on all VRFs, default to the device global limit for each application. Use **show limits** command to display a router application's global limit.

By setting a resource limit less than the global limit for a VRF, you assure that the VRF will not starve other VRFs for that application's resources.

Not all application limits can be modified on a device. Use the **set limits** *vrf-name* **?** command to display a list of applications for which limits can be set for this device.

Use the **resource-ipv6netmask full** option to set the IPv6 netmask to support for bits 65 – 127.

Note: Setting the resource-ipv6netmask option to full reduces the routing table space supported for IPv4 and IPv6 routes. It is recommended that you not use the **full** option unless you are actually using routes in that bit space.

Use the **clear limits** command to reset the application limit to the application limit's global value.

Examples

This example sets the OSPFv2 link state entries resource limit to **45000** entries on VRF **vr2** and displays the new setting:

```
S Chassis(su)->set limits vrf vr2 application  ospf-ls-entries 45000
S Chassis(su)->show limits vrf vr2 application ospf-ls-entries

Application: ospf-ls-entries
Description: Maximum number of OSPF link-state entries

VRF NAME                            limit   in use reserved
------------------------------- -------- -------- --------
vr2                                 45000        0        0


Chassis Total Resources .............      50000
Chassis Total Reserved  .............          0
Chassis Total Reserved Available ....          0
Chassis Total Unreserved Available ..      50000

S Chassis(su)->
```

clear limits

Use this command to reset the resource limit for the specified application and VRF to the global value.

Syntax

clear limits [**vrf** *vrf-name*] [**resource-ipv6netmask**] *application*

Parameters

vrf vrf-name	Specifies the name of the VRF to which the resource limit applies.
resource-ipv6netmask	Specifies the IPv6 netmask resource limit.
application	Specifies the application to which the resource limit applies.

Defaults

None.

Mode

All command modes.

Usage

Use the **clear limits** command to reset the resource limit, for the specified application, to its global limit or that the IPv6 netmask should be reset to the default value. Use the **show limits** command, specifying the application, to display an application's global limit, or specifying resource-ipv6netmask to display the current IPv6 netmask setting.

Examples

This example resets the OSPF link state entries resource limit on VRF **vr2** to the global limit

```
S Chassis(su)->clear limits vrf vr2 application ospf-ls-entries
S Chassis(su)->
```

set router vrf create

Use this command to create a VRF router.

Syntax

set router vrf create *vrf-name* [**context** *context-name*]

Parameters

vrf-name	Specifies the name of the VRF router. Valid values are up to 31 printable characters.
context *context-name*	Specifies the SNMPv3 context for this VRF router. Valid values are up to 28 printable characters. The default value is the specified VRF name.

Defaults

If the **context** *context-name* parameter is not specified, the SNMPv3 context defaults to the VRF name.

Mode

All command modes.

Usage

Space characters are not supported in either a VRF name or SNMPv3 context name.

The **context** *context-name* parameter must be specified if the VRF name is greater than 28 characters.

The **global** VRF router is the default router for the device.

Examples

This example creates the VRF router nat1:

```
S Chassis(su)->set router vrf create nat1
S Chassis(su)->router nat1
```

```
S Chassis(su-nat1)->show router
VRF Context     : nat1
RD              : not set
S Chassis(su)->
```

clear router vrf

Use this command to delete the specified VRF and all its configuration from the device or to write a blank configuration to the global router.

Syntax

clear router vrf *vrf-name*

Parameters

vrf-name	Specifies the name of the VRF router to delete.

Defaults

None.

Mode

All command modes.

Usage

This command is a powerful command that removes the specified VRF router.

When the **global** router is specified, the command effectively writes a blank configuration file to persistent memory. Unless the user is attached via a direct console connection, loss of management connectivity to the device should be expected. Before using this command, save the current configuration using the **show config** *outfile* command.

Example

This example shows how to clear the **global** VRF router configuration:

```
S Chassis(rw)->clear router vrf global
```

This example shows how to delete the **nat1** VRF router:

```
S Chassis(rw)->clear router vrf nat1
```

router

Use this command to enter router mode for the global or specified VRF router.

Syntax

router [*name*]

Parameters

name	(Optional) Specifies the name of a user-defined VRF. The default value is **global**.

Defaults

If no name is specified, this command enters router mode for the **global** router.

Mode

System configuration command mode.

Usage

This command can be used, but is not required, when configuring the **global** router. Entering the **configure** command from system configuration command mode places you in router configuration command mode for the **global** router.

Once in router command mode, use the **configure** command to enter router configuration command mode for this VRF router context.

The prompt for any VRF router name longer than 8 characters will only display the last 8 characters proceeded by an asterisk character (*).

Example

This example shows how to enter router configuration mode for the **nat1** VRF router:

```
S Chassis(rw)->router nat1
S Chassis(rw-nat1)->configure
S Chassis(rw-nat1-config)->
```

show running-config

Use this command to display the non-default, user-supplied commands entered while configuring the device.

Syntax

show running-config [**all**] [*application* [**all**]]

Parameters

all	(Optional) Displays all the running configuration including default parameters for the current VRF router context.

application	Specifies an application to display: • **access-lists** - Show access list configuration • **arp-nd** - Show ARP and Neighbor Discovery configuration • **bgp** - Show BGP configuration • **dhcp-server** - Show DHCP Server configuration • **dvmrp** - Show DVMRP configuration • **forward-protocol** - Show forword-protocol configuration • **hostDoS** - Show Host DoS configuration • **interface** - Show configuration for one or all interfaces • **nat** - Show nat configuration • **ospf** - Show ospf configuration • **ospfv3** - Show ospfv3 configuration • **pim** - Show PIM configuration • **probe** - Show Probe configuration • **rip** - Show rip configuration • **route-map** - Show route map configuration • **routes** - Show static route configuration • **slb** - Show Server Load Balancing (SLB) configuration • **track** - Show Track configuration • **twcb** - Show twcb configuration

Defaults

If **all** is not specified, only the non-default, user-supplied commands entered while configuring the current VRF router context are displayed.

When specifying a supported application keyword, only configuration for the specified application displays.

If no application is specified, the entire non-default running configuration displays.

Mode

Configuration command, Any router mode.

Example

This example shows how to display all configuration for interface vlan.0.1:

```
S Chassis(rw)->show running-config interface vlan.0.1 all
# **** VRF default (default) ****
configure terminal
!
 interface vlan.0.1
  ip address 10.21.130.59 255.255.128.0
  no ip nat inside
  no ip nat outside
  ip policy priority first
  ip policy load-policy first-available
```

```
  no ip proxy-arp
  no ip gratuitous-arp
  no ip gratuitous-arp-learning
  ip redirects
  no shutdown
  exit
!
exit
!
```

54

Routing Interface Commands

This chapter describes the routing interface set of commands and how to use them. For information about configuring routing interfaces, refer to the "IP Routing Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show interface	54-1
interface	54-2
ip forwarding	54-4
ip ecm-forwarding-algo	54-4
show ip interface	54-5
ip address	54-6
ip checkspoof	54-7
ip icmp unreachable	54-8
ip icmp redirects	54-9
ip icmp echo-reply	54-9
secondary-vlan	54-10
no shutdown	54-11

show interface

Use this command to display information about one or more interfaces (VLANs or loopbacks) configured on the router.

Syntax

show interface [*interface-name*]

Parameters

interface-name	(Optional) Specifies the name of an interface, such as **vlan.0.1**.

Defaults

If an *interface-name* not specified, information for all routing interfaces will be displayed.

Mode

All command modes.

Example

This example shows how to display information for all interfaces configured on the router.

```
S Chassis(rw)->show interface
 vlan.0.1 is Administratively up, Operationally up
   IP Address 10.21.130.59 Mask 255.255.128.0
   MAC-Address is: 0011.880c.9f78
   The name of this device is vlan.0.1
   MTU is 1500 bytes
   The bandwidth is 10000 Mb/s
   Encapsulation ARPA, Loopback not set
   ARP type: ARPA,   ARP Timeout: 3600 seconds
   Policy Routing disabled

 vlan.0.5 is Administratively down, Operationally down
   MAC-Address is: 0011.880c.9f78
   The name of this device is vlan.0.5
   MTU is 1500 bytes
   The bandwidth is 10000 Mb/s
   Encapsulation ARPA, Loopback not set
   ARP type: ARPA,   ARP Timeout: 3600 seconds
   Policy Routing disabled
```

interface

Use this command to configure interfaces for IP routing.

Syntax

interface {**vlan** *vlan-id* | **loopback** *loopback-id* | **tunnel** *tunnel-id* | *interface-name*}

no interface {**vlan** *vlan-id* | **loopback** *loopback-id* | **tunnel** *tunnel-id* | *interface-name*}

Parameters

vlan *vlan-id*	Specifies the number of the VLAN interface to be configured for routing. Valid VLAN interface values: **1** - **4094**.
loopback *loopback-id*	Specifies the number of the loopback interface to be configured for routing. Valid loopback interface values: **1** - **128**.
tunnel *tunnel-id*	Specifies the number of the layer 3 tunnel to be configured for routing. Valid layer 3 tunnel interface values: **1** - **50**.
interface-name	Specifies an interface name to be configured for routing. An interface name is specified in a **vlan.*x*.*y*** format or as an interface alias.

Defaults

None.

Mode

Configuration command, Global configuration mode.

Usage

This command enables interface configuration mode from global configuration mode, and, if the interface has not previously been created, this command creates a new routing interface.

A VLAN routing interface can be configured before its VLAN is created in system configuration mode, but VLANs must be created from the system CLI before they will be operational within IP routing. See the "Configuring VLANs" section of the *Extreme Networks S-Series Configuration Guide* for VLAN configuration details.

Each VLAN, layer 3 tunnel or, loopback interface must be configured for routing separately using the **interface** command. To end configuration on one interface before configuring another, type **exit** at the command prompt. Enabling interface configuration mode is required for completing interface-specific configuration tasks.

To create a layer 3 tunnel, both endpoint devices must support the tunneling protocol. To configure a layer 3 tunnel on the interface, see Chapter 57, **Tunnel Configuration Commands** for layer 3 tunnel configuration command details.

IPv4 and IPv6 forwarding are both enabled by default on loopback interfaces. Without forwarding, a loopback interface is unreachable. This configuration setting cannot be modified.

Each interface's network can be configured for the RIP, BGP, and OSPF routing protocol.

Each Extreme Networks S-Series routing module or Standalone device can support up to 256 routing interfaces. Each interface can be configured for the RIP and/or OSPF routing protocols.

The "no" form of this command removes the specified routing interface configuration.

Examples

This example shows how to enter configuration mode for VLAN 2 using the *interface-name* format:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan.0.2
S Chassis(rw-config-intf-vlan.0.2)->
```

This example shows how to enter configuration mode for loopback 2 using the *interface-name* format:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface loop.0.2
S Chassis(rw-config-intf-loop.0.2)->
```

This example shows how to enter configuration mode for layer 3 tunnel 1:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface tunnel 1
S Chassis(rw-config-intf-tun.0.1)->
```

ip forwarding

Use this command to enable or disable IP forwarding on a routing interface.

Syntax

ip forwarding

no ip forwarding

Parameters

None.

Defaults

None.

Mode

Interface Configuration command mode.

Usage

IP forwarding is enabled by default on an interface. IP forwarding can be disabled on an interface by using the “no” form of this command in interface configuration command mode.

Example

This example shows how to disable IP forwarding on a routing interface:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan.0.2
S Chassis(rw-config-intf-vlan.0.2)->no ip forwarding
```

ip ecm-forwarding-algo

Use this command to set the ECM (Equal Cost Multipath) forwarding algorithm used for forwarding IP packets on routing interfaces.

Syntax

ip ecm-forwarding-algo [**hash-thold** | **round-robin**]

no ip ecm-forwarding-algo

Parameters

hash-thold	(Optional) Sets the ECM forwarding algorithm as hash threshold.
round-robin	(Optional) Sets the ECM forwarding algorithm as round robin.

Defaults

If an algorithm is not specified, hash threshold will be set.

Mode

Configuration command, Global configuration.

Usage

The “no” form of this command removes the round-robin algorithm, resetting the algorithm to hash threshold.

Examples

This example shows how to set the round-robin ECM mode:

```
S Chassis(rw-config)->ip ecm-forwarding-algo round-robin
```

This example shows how to reset the ECM mode to the default forwarding algorithm of hash threshold:

```
S Chassis(rw-config)->no ip ecm-forwarding-algo
```

show ip interface

Use this command to display information, including administrative status, IP address, MTU (Maximum Transmission Unit) size and bandwidth, and ACL configurations, for interfaces configured for IP.

Syntax

show ip interface [*interface-name*] [**brief**]

Parameters

interface-name	(Optional) Displays information for a specific VLAN interface in the routing interface format of **vlan.*x*.*y***. This interface must be configured for IP routing. Valid VLAN interface *y* values: **1** - **4094**.
brief	(Optional) Displays a summary of either all routing interfaces or the specified interface.

Defaults

- If *interface-name* is not specified, status information for all routing interfaces will be displayed.
- If **brief** is not specified, a detailed level of status information displays.

Mode

All command modes**.**

Examples

This example shows how to display configuration information for VLAN 2:

```
S Chassis(rw)->show ip interface vlan.0.2
 vlan.0.2 is Operationally down, Administratively down
   IP forwarding enabled
   Frame Type ARPA
   MAC-Address 00.11.88.0c.9f.78
   Incoming IPv4 Access list is
   Incoming IPv6 Access list is
   Outgoing IPv4 Access list is
   Outgoing IPv6 Access list is
```

```
   Directed-broadcast is disabled
   MTU is 1500 bytes
   ARP Timeout is 2800 seconds
   ARP Retransmit Time is 1 seconds
   ARP Stale-Entry-Timeout is 900 seconds
   Proxy ARP is enabled (no local or default-route)
   Gratuitous ARP updating is set to update on ARP replies and ARP requests
   Gratuitous ARP learning is not set
   ICMP Re-Directs are enabled
   ICMP Echo Replies are always sent
   ICMP Mask Replies are always sent
   NAT INSIDE:  Not Set
   NAT OUTSIDE: Not Set
   TWCB Redirect Outbound WebCache: Not Set
   Policy routing disabled
S Chassis(rw)->
```

This example shows how to display the IP interface information using the brief option:

```
S Chassis(rw)->show ip interface brief
                                                IPv4      IPv6     Admin  Oper
Interface     IP Address       Netmask          Fwding    Fwding   Status Status
------------  ---------------  ---------------  --------  -------- ------ ------
lo.0.1        127.0.0.1        255.255.255.255  -         -        up     up
loop.0.1      1.1.1.1          255.255.255.255  -         -        up     up
vlan.0.1      10.21.130.151    255.255.128.0    disabled  disabled up     up
S Chassis(rw)->
```

ip address

Use this command to set, remove, or disable a primary or secondary IP address for an interface.

Syntax

ip address {*ip-address ip-mask* | *ip-address/prefixLength*} [**primary** | **secondary** | **management**]

no ip address {*ip-address ip-mask* | *ip-address/prefixLength*}

Parameters

ip-address ip-mask | *ip-address/prefixLength*	Specifies the IP address and IP mask or IP address and prefix length of the interface to be added or removed.
ip-mask	Specifies the mask for the associated IP subnet.
primary	(Optional) Specifies that the configured IP address is a primary address.
secondary	(Optional) Specifies that the configured IP address is a secondary address.
management	(Optional) Specifies that the configured IP address is a management address.

Defaults

If either **secondary** or **management** is not specified, the configured address will be the primary address for the interface.

Mode

Configuration command, Interface configuration.

Usage

Only a single primary address is configurable. A secondary IP address cannot be added until a primary IP address exists. A primary address can be changed without removing all the secondary addresses by using the **primary** keyword. A primary IP address cannot be removed until all secondaries are removed. If an attempt is made to change the primary with the primary keyword, a message displays to make sure that is the intended action. If an attempt to enter a secondary address without the secondary keyword being entered is made, a message confirming the intent to change the primary address will display, the primary will not be accidentally overwritten.

Each Extreme Networks S-Series routing module or Standalone device supports up to 256 IP VLAN routing interfaces, 21 Loopback interfaces, with up to 128 secondary addresses (2000 maximum per router) allowed for each primary IP address.

See "ipv6 address" on page 55-3 for IPv6 address configuration command information.

The "no" form of this command removes the specified IP address and disables the interface for IP processing for removed IP addresses. If a primary or secondary IP address is still present, processing will continue for those IP addresses. The interface can only be disabled using the **no shutdown** command.

Example

This example sets the IP address to 192.168.1.1 and the network mask to 255.255.255.0 for VLAN 1 as a primary address:

```
S Chassis(rw)->
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan.0.1
S Chassis(rw-config-intf-vlan.0.1)->ip address 192.168.1.1 255.255.255.0
```

ip checkspoof

Use this command to provide checkspoof protection for transit frames being routed through the system.

Syntax

ip checkspoof {**strict-mode** | **loose-mode**}

no ip checkspoof {**strict-mode** | **loose-mode**}

Parameters

strict-mode	Verifies that the source IP address is reachable from the receive interface.
loose-mode	Verifies that the source IP address is reachable from any interface.

Defaults

None.

Mode

Configuration command, Interface configuration .

Usage

Network configurations that utilize VRRP may have connectivity issues to the backup interfaces when using checkspoof strict-mode. Under this circumstance, traffic may be routed via what appears to be the non-best path to the backup interface, due to the inherent nonsymmetric nature of VRRP routing. Strict-mode checkspoof rejects frames that do not ingress the “best” interface. When utilizing VRRP, use the loose-mode version of checkspoof. This mode verifies that the source IP in the packet is at least in a “known” network.

Example

This example enables strict-mode IP checkspoofing on VLAN 1:

```
S Chassis(rw)->
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan.0.1
S Chassis(rw-config-intf-vlan.0.1)->ip checkspoof strictmode
```

ip icmp unreachable

Use this command to enable sending ICMP destination unreachable messages on an interface.

Syntax

ip icmp unreachable

no ip icmp unreachable

Parameters

None.

Defaults

None.

Mode

Interface Configuration.

Usage

Use the **no ip icmp unreachable** command to disable sending ICMP destination unreachable messages on this interface.

Example

This example shows how to enable the sending of ICMP destination unreachable messages on VLAN 1:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan.0.1
S Chassis(rw-config-intf-vlan.0.1)->ip icmp unreachable
```

ip icmp redirects

Use this command to enable sending ICMP redirect messages on an interface.

Syntax

ip icmp redirect

no ip icmp redirect

Parameters

None.

Defaults

None.

Mode

Interface Configuration.

Usage

Use the **no ip icmp redirect** command to disable sending ICMP redirect messages on this interface.

Example

This example shows how to enable the sending of ICMP redirect messages on VLAN 1:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan.0.1
S Chassis(rw-config-intf-vlan.0.1)->ip icmp redirect
```

ip icmp echo-reply

Use this command to enable sending ICMP echo-reply messages on an interface.

Syntax

ip icmp echo-reply

no ip icmp echo-reply

Parameters

None.

Defaults

None.

Mode

Interface Configuration.

Usage

Use the **no ip icmp echo-reply** command to disable sending ICMP echo-reply messages on an interface.

Example

This example shows how to enable the sending of ICMP echo-reply messages on VLAN 1:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan.0.1
S Chassis(rw-config-intf-vlan.0.1)->ip icmp echo-reply
```

secondary-vlan

Use this command to create a secondary VLAN by assigning the secondary VLAN to a VLAN interface.

Syntax

secondary-vlan *vlan-id*

Parameters

vlan-id	Specify the secondary VLAN ID. Valid values are **1** - **4095**.

Defaults

None.

Mode

Interface Configuration.

Usage

The secondary VLAN configuration on an IP Interface provides the ability to associate multiple L2 VLANs with one L3 IP interface. A secondary VLAN can be configured as a private VLAN. Members of the private VLAN are connected hosts that share the IP interface of the primary VLAN, while at the same time are restricted from directly communicating with each other. Hosts on the primary VLAN, also referred to as the community VLAN, can communicate directly with hosts on both the primary and private VLANs.

Refer to the “Secondary and Private VLAN” section of the *Extreme Networks S-Series Configuration Guide* for a complete private VLAN configuration discussion.

When configuring a secondary VLAN, set both the secondary and primary VLAN constraint to shared, using the same constraint set ID. This setting assures that both the primary and secondary VLAN use the same FID. VLAN constraint is set using the **set vlan constraint** command.

An IP address is only configured for the primary VLAN, not for the secondary VLAN.

Examples

This example shows how to:

- Create the static primary (VLAN **100**) and secondary (VLAN **200**) VLANs
- Assign ports **ge.1.1-2** to the primary VLAN
- Assign ports **ge.1.3-4** to the secondary VLAN
- Configure VLAN 200 as a private VLAN by:
  - Setting egress for VLAN 100 for all ports
  - Setting egress for VLAN 200 only on primary VLAN ports ge.1.1-2
- Setting the VLAN constraint to shared for each VLAN
- Configure the primary interface with a primary IP address of **100.1.1.1/24** and a secondary VLAN of **200**

```
S Chassis(rw)->set vlan name 100 PrimaryVlan
S Chassis(rw)->set vlan name 200 SecondaryVlan
S Chassis(rw)->set port vlan ge.1.1-2 100
S Chassis(rw)->set port vlan ge.1.3-4 200
S Chassis(rw)->set vlan egress 100 ge.1.1-4 untagged
S Chassis(rw)->set vlan egress 200 ge.1.1-2 untagged
S Chassis(rw)->set vlan constraint 100 100 shared
S Chassis(rw)->set vlan constraint 200 100 shared
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 100
S Chassis(rw-config-intf-vlan.0.1)->ip address 100.1.1.1/24 primary
S Chassis(rw-config-intf-vlan.0.1)->secondary-vlan 200
S Chassis(rw-config-intf-vlan.0.1)->
```

no shutdown

Use this command to enable an interface for IP routing and to allow the interface to automatically be enabled at device startup.

Syntax

no shutdown

shutdown

Parameters

None.

Defaults

None.

Mode

Configuration command, Interface configuration.

Usage

The **shutdown** form of this command disables an interface for IP routing.

Example

This example shows how to enable VLAN 1 for IP routing:

```
S Chassis(rw)->
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan.0.1
S Chassis(rw-config-intf-vlan.0.1)->no shutdown
```

55

IPv6 Interface Commands

This chapter details the IPv6 interface set of commands. For information about configuring IPv6 interfaces, refer to the "Interface Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show ipv6 interface	55-1
ipv6 address	55-3
ipv6 checkspoof	55-5
ipv6 forwarding	55-6
ipv6 icmp unreachable	55-6
ipv6 icmp redirects	55-7
ipv6 icmp echo-reply	55-7
ipv6 nd dad attempts	55-8
ipv6 nd managed-config-flag	55-9
ipv6 nd ns-interval	55-9
ipv6 nd other-config-flag	55-10
ipv6 nd prefix	55-11
ipv6 nd ra hoplimit suppress	55-11
ipv6 nd ra interval	55-12
ipv6 nd ra lifetime	55-13
ipv6 nd ra mtu	55-14
ipv6 nd ra suppress	55-14
ipv6 nd reachable-time	55-15

show ipv6 interface

Use this command to display information for configured IPv6 interfaces.

Syntax

show ipv6 interface [*interface-name* [**prefix**]] [**brief**]

Parameters

interface-name	(Optional) Displays information for a specific VLAN interface in the routing interface format of **vlan.*x*.*y***. This interface must be configured for IP routing. Valid VLAN interface *y* values: **1** - **4094**.
prefix	(Optional) Displays a single line of information for each configured or learned prefix for the specified interface.
brief	(Optional) Displays a summary of either all routing interfaces or the specified interface.

Defaults

- If *interface-name* is not specified, status information for all routing interfaces will be displayed.
- If **prefix** is not specified, all status information for the specified interface will be displayed.
- If **brief** is not specified, a detailed level of status information displays.

Mode

All command modes**.**

Examples

This example shows how to display configuration information for VLAN 51:

```
S Chassis(rw)->show ipv6 interface vlan.0.51

 vlan.0.51 is Operationally down, Administratively down
  IPv6 is enabled link-local address is fe80::21f:45ff:fe5b:f5cf%vlan.0.51
  Global unicast address(es):
    2001:11ac:fd34:50::abcd:33, subnet is 2001:11ac:fd34:50::/64
  Joined group address(es):
    (None)
  IPV6 forwarding disabled
  IPV6 address auto-configuration is enabled
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  Sending of ICMP Destination Unreachable Messages is enabled
  Sending of ICMP Redirect Messages is enabled
  Sending of ICMP Echo-Reply Messages is enabled
  ND DAD is enabled, number of DAD attempts: 1

S Chassis(su-config)->
```

This example shows how to display the IP interface information using the **brief** option:

```
S Chassis(su)->show ipv6 interface vlan.0.51 brief
                                                                  Admin  Oper
Interface    IPv6 Address                              Prefix     Status Status
------------ ----------------------------------------  ---------  ------ ------
vlan.0.51    2001:11ac:fd34:50::abcd:33                64         up     up
vlan.0.51    fe80::21f:45ff:fe5b:f5cf%vlan.0.51        10         up     up
```

```
S Chassis(su)->
```

This example shows how to display the IP interface information using the **prefix** option:

```
S Chassis(su)->show ipv6 interface vlan.0.51 prefix
FLAGS:  C = Auto config    O = Onlink
        A = Ipv6 Address   P = Ipv6 Prefix
        S = Advertising Suppressed

IP Address                                    Flags Valid          Preferred
--------------------------------------------- ----- -------------- --------------
2001:11ac:fd34:50::abcd:33/64                 ACO   2592000        604800
S Chassis(su)->
```

ipv6 address

Use this command to set the IPv6 address and enable IPv6 processing on an interface.

Syntax

ipv6 address {*link-local-address* **link-local** | *ipv6-address/length* | *ipv6-prefix/length* **eui-64** | **autoconfig** | *general-prefix sub-bits/length*}

no ipv6 address {*link-local-address* **link-local** | *ipv6-address/length* | *ipv6-prefix/length* **eui-64** | **autoconfig** | *general-prefix sub-bits/length*}

Parameters

link-local-address **link-local**	Specifies an IPv6 link-local address.
ipv6-address/length	Specifies the IPv6 address for this interface.
ipv6-prefix/length **eui-64**	Formulate the IPv6 address using an EUI-64 ID in the lower order 64 bits of the address.
autoconfig	Specifies that autoconfiguration of the IPv6 address is enabled for this interface. IPv6 address autoconfiguration is disabled by default.
general-prefix sub-bits/length	Specifies a configured general prefix followed by the sub-bits and length that complete the address.

Defaults

None.

Mode

Interface configuration.

Usage

Use this command to manually configure a global unicast IPv6 address for an interface. Link local addresses are network addresses which are intended only for communications within one segment of a local network (a link) or a point-to-point connection. They allow addressing hosts without using a globally-routable address prefix. Routers will not forward packets with link-local addresses. A link local address must begin with **fe80:**.

A single link local address is supported per interface. If IPv6 autoconfiguration is enabled, the link local address is autoconfigured. When manually configuring a link local address, if a link local address already exists on the interface, a warning displays asking you if you wish to change it.

EUI-64 is an automatic interface addressing capability. By implementing the IEEE's 64-bit Extended Unique Identifier (EUI-64) format, a host can automatically assign itself a unique 64-bit IPv6 interface identifier without the need for manual configuration or DHCP. This is accomplished on Ethernet interfaces by referencing the already unique 48-bit MAC address and reformatting that value to match the EUI-64 specification as specified in RFC 2373. When configuring an EUI-64 address, the specified prefix must have a length of 64.

A general prefix allows an assigned name to represent a network prefix from which longer IPv6 addresses can be configured. The sub-bits added to the general prefix can both extend the network prefix by adding to the specified prefix length, as well as complete the IPv6 address. See “ipv6 general-prefix” on page 56-17 for general prefix command details.

Use “show ipv6 interface” on page 55-1 to display IPv6 addresses assigned by the **ipv6 address** command.

See “ip address” on page 54-6 for IPv4 address configuration command information.

The **no ipv6 address** command removes the specified IPv6 address configuration for this interface.

Examples

This example sets the IPv6 address for interface VLAN 50 to ba10:1100:aa11:c171:0:0:1111:00/48:

```
S Chassis(su-config)->interface vlan 50
S Chassis(su-config-intf-vlan.0.50)->ipv6 address
ba10:1100:aa11:c171:0:0:1111:00/48
S Chassis(su-config-intf-vlan.0.50)->
```

This example sets the IPv6 link local address for interface VLAN 50 to fe80:1234:5678::300:

```
S Chassis(su-config)->interface vlan 50
SChassis(su-config-intf-vlan.0.50)->ipv6 address fe80:1234:5678::300 link-local
Do you want to replace IPv6 link-local address (y/n) [n]?y
S Chassis(su-config-intf-vlan.0.50)->
```

This example sets an IPv6 EUI-64 address for interface VLAN 50 based upon the prefix 2001:febd:1234:0/64, and displays the EUI-64 address in the interface output:

```
S Chassis(su-config)->interface vlan 50
S Chassis(su-config-intf-vlan.0.50)->ipv6 address 2001:febd:1234:0/64 eui-64
S Chassis(su-config-intf-vlan.0.50)->show ipv6 interface vlan.0.50
 vlan.0.50 is Operationally down, Administratively down
  IPv6 is enabled link-local address is fe80::2e0:63ff:fe6b:1d26%vlan.0.50
  Global unicast address(es):
    2001:febd:1234::2e0:63ff:fe6b:1d26, subnet is 2001:febd:1234::/64 [EUI]
...
S Chassis(su-config-intf-vlan.0.50)->
```

The following example creates a general prefix named “Doc-Prefix” with a prefix value of **2001:11ac:fd34::/48** and assigns the IPv6 address **2001:11ac:fd34:50:0:0:abcd:33** to VLAN 51. The general prefix **Doc-Prefix** is followed by **::50:0:0:abcd:33/64**. The subnet length is changed to **/64** adding **:50** to the general prefix to create a network prefix of **2001:11ac:fd34:50/64**:

```
S Chassis(su)->configure
```

```
S Chassis(su-config)->ipv6 general-prefix Doc-Prefix 2001:11ac:fd34::/48
S Chassis(su-config)->show ipv6 general-prefix
  ipv6 general-prefix Doc-Prefix 2001:11ac:fd34::/48
S Chassis(su-config)->interface vlan 51
S Chassis(su-config-intf-vlan.0.51)->ipv6 address Doc-Prefix ::50:0:0:abcd:33/64
S Chassis(su-config-intf-vlan.0.51)->show ipv6 interface vlan.0.51

 vlan.0.51 is Operationally down, Administratively down
  IPv6 is enabled link-local address is fe80::211:88ff:fe7c:32c1%vlan.0.51
  Global unicast address(es):
    2001:11ac:fd34:50:0:0:abcd:33, subnet is 2001:11ac:fd34:50::/64
...
S Chassis(su-config-intf-vlan.0.51)->
```

ipv6 checkspoof

Use this command to provide checkspoof protection for transit frames being routed through the system.

Syntax

ipv6 checkspoof {**strict-mode** | **loose-mode**}

no ipv6 checkspoof {**strict-mode** | **loose-mode**}

Parameters

strict-mode	Verifies that the source IPv6 address is reachable from the receive interface.
loose-mode	Verifies that the source IPv6 address is reachable from any interface.

Defaults

None.

Mode

Configuration command, Interface configuration .

Usage

Network configurations that utilize VRRP may have connectivity issues to the backup interfaces when using checkspoof strict-mode. Under this circumstance, traffic may be routed via what appears to be the non-best path to the backup interface, due to the inherent nonsymmetric nature of VRRP routing. Strict-mode checkspoof rejects frames that do not ingress the “best” interface. When utilizing VRRP, use the loose-mode version of checkspoof. This mode verifies that the source IP in the packet is at least in a “known” network.

Example

This example enables strict-mode IPv6 checkspoofing on VLAN 1:

```
S Chassis(rw)->
S Chassis(rw)->configure
```

```
S Chassis(rw-config)->interface vlan.0.1
S Chassis(rw-config-intf-vlan.0.1)->ipv6 checkspoof strictmode
```

ipv6 forwarding

Use this command to enable or disable IPv6 forwarding on a routing interface.

Syntax

ipv6 forwarding

no ipv6 forwarding

Parameters

None.

Defaults

None.

Mode

Interface Configuration.

Usage

IPv6 forwarding is disabled by default on an interface.

The **no ipv6 forwarding** command disables IPv6 forwarding on this interface.

Example

This example shows how to enable IPv6 forwarding on interface VLAN 2:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan.0.2
S Chassis(rw-config-intf-vlan.0.2)->ipv6 forwarding
```

ipv6 icmp unreachable

Use this command to enable sending ICMP destination unreachable messages on an interface.

Syntax

ipv6 icmp unreachable

no ipv6 icmp unreachable

Parameters

None.

Defaults

None.

Mode

Interface Configuration.

Usage

Use the **no ipv6 icmp unreachable** command to disable sending ICMP destination unreachable messages on this interface.

Example

This example shows how to enable the sending of ICMP destination unreachable messages on VLAN 50:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan.0.50
S Chassis(rw-config-intf-vlan.0.50)->ipv6 icmp unreachable
```

ipv6 icmp redirects

Use this command to enable sending ICMP redirect messages on an interface.

Syntax

ipv6 icmp redirect

no ipv6 icmp redirect

Parameters

None.

Defaults

None.

Mode

Interface Configuration.

Usage

Use the **no ipv6 icmp redirect** command to disable sending ICMP redirect messages on this interface.

Example

This example shows how to enable the sending of ICMP redirect messages on VLAN 50:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan.0.50
S Chassis(rw-config-intf-vlan.0.50)->ipv6 icmp redirect
```

ipv6 icmp echo-reply

Use this command to enable sending ICMP echo-reply messages on an interface.

Syntax

ipv6 icmp echo-reply

no ipv6 icmp echo-reply

Parameters

None.

Defaults

None.

Mode

Interface Configuration.

Usage

Use the **no ipv6 icmp echo-reply** command to disable sending ICMP echo-reply messages on an interface.

Example

This example shows how to enable the sending of ICMP echo-reply messages on VLAN 50:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan.0.50
S Chassis(rw-config-intf-vlan.0.50)->ipv6 icmp echo-reply
```

ipv6 nd dad attempts

Use this command to configure the number of Neighbor Discovery (ND) neighbor solicitation messages to send during Duplicate Address Detection (DAD) on unicast IPv6 addresses on the interface.

Syntax

ipv6 nd dad attempts *num*

no ipv6 nd dad attempts *num*

Parameters

num	Specifies the number of neighbor solicitation messages to send during DAD. Valid values are **0** - **600** messages. Default value is **1** message.

Defaults

None.

Mode

Interface configuration.

Usage

Duplicate address detection sends neighbor solicitation messages with an unspecified source address targeting its own “tentative” address. Such messages trigger nodes already using the address to respond with a multicast neighbor advertisement indicating that the address is in use.

The **no ipv6 nd dad attempts** command disables the sending of neighbor solicitation messages during DAD. Setting the number of messages to **0** also disables the sending of neighbor solicitation messages during DAD.

Example

This example sets the number of neighbor solicitation messages to send during DAD at **5** for VLAN 50:

```
S Chassis(su-config)->interface vlan 50
S Chassis(su-config-intf-vlan.0.50)->ipv6 nd dad attempts 5
S Chassis(su-config-intf-vlan.0.50)->
```

ipv6 nd managed-config-flag

Use this command to set the managed address configuration flag in router advertisements.

Syntax

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

Parameters

None.

Defaults

None.

Mode

Interface configuration.

Usage

When the managed address configuration flag is set, attached hosts use stateful autoconfiguration to obtain addresses. The managed address configuration flag feature is disabled by default.

The **no ipv6 nd managed-config-flag** command disables the use of stateful autoconfiguration by attached hosts to obtain addresses.

Example

This example enables the use of stateful autoconfiguration by attached hosts to obtain addresses on VLAN 50:

```
S Chassis(su-config)->interface vlan 50
S Chassis(su-config-intf-vlan.0.50)->ipv6 nd managed-config-flag
S Chassis(su-config-intf-vlan.0.50)->
```

ipv6 nd ns-interval

Use this command to set the interval between neighbor solicitation messages.

Syntax

ipv6 nd ns-interval *interval*

no ipv6 nd ns-interval *interval*

Parameters

interval	Specifies the interval between neighbor solicitation messages in milli-seconds. Valid values are **1000** - **4294967295** milli-seconds. Default value is **1000** milli-seconds.

Defaults

None.

Mode

Interface configuration.

Usage

The **no ipv6 nd ns-interval** command resets the interval between neighbor solicitation messages to the default value of 1000ms.

Example

This example sets the interval between neighbor solicitation messages at 1.5 seconds for VLAN 50:

```
S Chassis(su-config)->interface vlan 50
S Chassis(su-config-intf-vlan.0.50)->ipv6 nd ns-interval 1500
S Chassis(su-config-intf-vlan.0.50)->
```

ipv6 nd other-config-flag

Use this command to set the other configuration flag in router advertisements.

Syntax

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Parameters

None.

Defaults

None.

Mode

Interface configuration.

Usage

When the other config flag is set, attached hosts use stateful autoconfiguration to obtain non-address information. If the managed address configuration flag (see “ipv6 nd reachable-time” on page 55-15) is set, the attached host uses stateful autoconfiguration to obtain non-address information regardless of the other config flag setting.

The **no ipv6 nd other-config-flag** command disables the other config flag feature for the interface.

Example

This example enables the use of stateful autoconfiguration by attached hosts to obtain non-address information on VLAN 50:

```
S Chassis(su-config)->interface vlan 50
S Chassis(su-config-intf-vlan.0.50)->ipv6 nd other-config-flag
S Chassis(su-config-intf-vlan.0.50)->
```

ipv6 nd prefix

Use this command to configure the IPv6 prefixes to include in IPv6 Neighbor Discovery (ND) router advertisements for the interface.

Syntax

ipv6 nd prefix *ipv6-prefix/length*

no nd prefix *ipv6-prefix/length*

Parameters

ipv6-prefix/length	Specifies the IPv6 prefix to include in IPv6 ND router advertisements for the interface in the format a:b:c:d:e:f:g:h/x.

Defaults

None.

Mode

Interface configuration.

Usage

The **no ipv6 nd prefix** command removes the specified IPv6 prefix from being included in IPv6 ND router advertisements for the interface.

Example

This example sets the IPv6 prefix ba10:1100:aa11/48 to be included in the ND router advertisements for VLAN 50:

```
S Chassis(su-config)->interface vlan 50
S Chassis(su-config-intf-vlan.0.50)->ipv6 nd prefix ba10:1100:aa11/48
S Chassis(su-config-intf-vlan.0.50)->
```

ipv6 nd ra hoplimit suppress

Use this command to configure neighbor discovery to suppress IPv6 router advertisement transmissions on an interface.

Syntax

ipv6 nd ra hoplimit suppress

no ipv6 nd ra hoplimit suppress

Parameters

None.

Defaults

None.

Mode

Interface configuration.

Usage

The router advertisement hoplimit suppress feature suppresses IPv6 router advertisement transmissions on an interface by setting the router advertisement hoplimit to 0.

The **no ipv6 ra hoplimit suppress** command disables the suppression of IPv6 router advertisements on the interface.

Example

This example enables router advertisement hoplimit suppression for VLAN 50:

```
S Chassis(su-config)->interface vlan 50
S Chassis(su-config-intf-vlan.0.50)->ipv6 ra hoplimit suppress
S Chassis(su-config-intf-vlan.0.50)->
```

ipv6 nd ra interval

Use this command to set the maximum and minimum router advertisement interval for the IPv6 interface.

Syntax

ipv6 nd ra interval {*maxinterval* | **msec** *maxinterval*} [*mininterval*]

no ipv6 nd ra interval {*maxinterval* | **msec** *maxinterval*} [*mininterval*]

Parameters

maxinterval	Specifies the maximum router advertisement interval in seconds. Valid values are **4** - **1800**. The default value is **600** seconds.
msec *maxinterval*	Specifies the maximum router advertisement interval in milli-seconds. Valid values are **4000** - **1800000**. The default value is **600000** ms.
mininterval	(Optional) Specifies the minimum router advertisement interval in seconds. Valid values are **4** - **1800**. The default value is **198** seconds or .33 of the configured maximum router advertisement value.

Defaults

If mininterval is not specified, the minimum router advertisement interval is set to **.33** times the current maximum router advertisement interval.

Mode

Interface configuration.

Usage

The **no ipv6 nd ra interval** command resets the maximum and router advertisement interval to the default value of **600** seconds. The minimum router advertisement interval always defaults to **.33** times the maximum router advertisement interval, unless you optionally specify a minimum value, in which case, the minimum value will be the specified value.

Example

This example sets the maximum router advertisement interval to 650 seconds and the minimum router advertisement value to .33 times 650 (214) for VLAN 50:

```
S Chassis(su-config)->interface vlan 50
S Chassis(su-config-intf-vlan.0.50)->ipv6 nd ra interval 650
S Chassis(su-config-intf-vlan.0.50)->
```

ipv6 nd ra lifetime

Use this command to set the router lifetime value in seconds for router advertisements on the IPv6 interface.

Syntax

ipv6 nd ra lifetime *value*

no ipv6 nd ra lifetime *value*

Parameters

value	Specifies the lifetime value for router advertisements on the IPv6 interface. Valid values are **0** or from the configured maximum router advertisement interval to **9000** seconds. The default value is **1800** seconds.

Defaults

None.

Mode

Interface configuration**.**

Usage

The lifetime parameter specifies the usefulness of the router as a default router on this IPv6 interface. Configuring the lifetime to **0** specifies that the router should not be considered a default router for this interface. If the lifetime is set to a nonzero value, it can not be less than the configured maximum router advertisement interval.

The **no ipv6 nd ra lifetime** command resets the router lifetime value to the default value of **1800** seconds.

Example

This example sets the router lifetime value to 2200 seconds for VLAN 50:

```
S Chassis(su-config)->interface vlan 50
S Chassis(su-config-intf-vlan.0.50)->ipv6 nd ra lifetime 2200
S Chassis(su-config-intf-vlan.0.50)->
```

ipv6 nd ra mtu

Use this command to set the Maximum Transmission Unit (MTU) value in bytes for router advertisements on the IPv6 interface.

Syntax

ipv6 nd ra mtu *mtu*

no ipv6 nd ra mtu *mtu*

Parameters

mtu	Specifies the MTU value for the IPv6 interface. Valid values are **1280** - **4294967295** bytes. The default value is **1500** bytes.

Defaults

None.

Mode

Interface configuration.

Usage

The **no ipv6 nd ra mtu** command resets the MTU value to the default value of **1500** bytes for the IPv6 interface.

Example

This example sets the MTU value to **12000** bytes for VLAN 50:

```
S Chassis(su-config)->interface vlan 50
S Chassis(su-config-intf-vlan.0.50)->ipv6 nd ra mtu 12000
S Chassis(su-config-intf-vlan.0.50)->
```

ipv6 nd ra suppress

Use this command to stop sending router advertisements on the IPv6 interface.

Syntax

ipv6 nd ra suppress

no ipv6 nd ra suppress

Parameters

None.

Defaults

None.

Mode

Interface configuration.

Usage

By default, router advertisements are sent on the IPv6 interface. The **ipv6 nd ra suppress** command stops the sending of router advertisements on the IPv6 interface.

The **no ipv6 nd ra suppress** command restarts the sending of router advertisements on the IPv6 interface.

Example

This example suppresses the sending of router advertisements on VLAN 50:

```
S Chassis(su-config)->interface vlan 50
S Chassis(su-config-intf-vlan.0.50)->ipv6 nd ra suppress
S Chassis(su-config-intf-vlan.0.50)->
```

ipv6 nd reachable-time

Use this command to set the number of milli-seconds the router is considered to be reachable on this IPv6 interface.

Syntax

ipv6 nd reachable-time *interval*

no ipv6 nd reachable-time *interval*

Parameters

interval	Specifies the number of milli-seconds the router is considered to be reachable on this IPv6 interface. Valid values are **0** - **3600000** (1 hour). The default value is **30000** ms (30 seconds).

Defaults

None.

Mode

Interface configuration**.**

Usage

A neighbor is determined to be reachable if positive confirmation has been received within the reachable interval that the forward path to the neighbor was functioning properly. If no confirmation is received within the reachable interval, it is assumed that the neighbor is unreachable.

The **no ipv6 nd reachable-time** command resets the router reachability value to the default value of **30** seconds for the IPv6 interface.

Example

This example sets the router reachability interval to **120000** ms (120 seconds) for VLAN 50:

```
S Chassis(su-config)->interface vlan 50
S Chassis(su-config-intf-vlan.0.50)->ipv6 nd reachable-time 120000
S Chassis(su-config-intf-vlan.0.50)->
```

56

IP Traffic Routes Commands

This chapter provides details for the IPv4 and IPv6 traffic routes set of commands including: static route configuration and IP route information display. For information about configuring IP traffic routes, refer to the "IP Routing Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show ip route	56-1
show ipv6 route	56-4
ip route	56-5
ipv6 route	56-7
set ip route	56-9
clear ip route	56-10
ip icmp	56-10
ipv6 neighbor	56-11
ipv6 nd delay-time	56-12
ipv6 nd reachable-time	56-12
ipv6 nd retransmit-time	56-13
ipv6 nd stale-time	56-13
show ipv6 neighbors	56-14
show ipv6 general-prefix	56-16
ipv6 general-prefix	56-17

show ip route

Use this command to display information about IP routes.

Syntax

show ip route [**host** {[**connected**] | [*host-address*] | [**dynamic**] | [**static**}] [<*address-or-prefix*> {[<*prefix-mask*> {[longer-prefixes]}] [<*prefix/length*> {[**longer-prefixes**]}][**connected**] | [**ospf**] | [**bgp**] | [**isis**] | [**rip**] | [**static**] | [**summary**] [**topology** <*topology-name*>]

Parameters

host	(Optional) Displays routes configured on the host stack.
address-or-prefix	(Optional) Specifies whether following is destination address or subnet prefix.
dest-address [*prefix-mask*]	(Optional) Converts the specified destination address and optional mask into a prefix and displays any routes that match the prefix.
prefix/prefix-length	(Optional) Displays any routes that match the specified prefix and prefix-length.
longer-prefixes	(Optional) Displays all routes that match the specified prefix and length.
connected	(Optional) Displays directly connected routes.
host-address	(Optional) Displays host interface addresses.
dynamic	(Optional) Displays dynamic routes learned via protocols.
ospf	(Optional) Displays routes configured for the OSPF routing protocol. For details on configuring OSPF, refer to the *Extreme Networks S-Series Configuration Guide*.
bgp	(Optional) Displays routes configured for the BGP routing protocol. For details on configuring BGP, refer to the *Extreme Networks S-Series Configuration Guide*.
isis	(Optional) Displays routes configured for the ISIS routing protocol. For details on configuring ISIS, refer to the *Extreme Networks S-Series Configuration Guide*.
rip	(Optional) Displays routes configured for the RIP routing protocol. For details on configuring RIP, refer to the *Extreme Networks S-Series Configuration Guide*.
static	(Optional) Displays static routes.
summary	(Optional) Displays a summary of the IP routing table.
topology *<topology-name>*	(Optional) Displays routes for the specified topology.

Defaults

- If no parameters are specified, all IP route information is displayed.
- If the optional *prefix-mask* is not specified, routes for the specified destination address are displayed.

Mode

All command modes.

Usage

Routes are managed by the RTM (Route Table Manager), and are contained in the RIB (Route Information Base). This database contains all the active static routes, all the RIP routes, and up to eight best routes to each network as determined by OSPF.

To display entries in an IPv4 multicast topology routing table, use the **show ip route** command with the **topology** option.

The RTM selects up to eight of the best routes to each network and installs these routes in the FIB (Forwarding Information Base). The routes in the FIB are distributed to every module for use by the router's ingress module as frames are received.

Examples

This example shows how to display IP connected route information:

```
S Chassis(rw)->show ip route connected

IP Route Table for VRF default
Codes: C-connected, S-static, R-RIP, B-BGP, O-OSPF, IA-OSPF interarea
       N1-OSPF NSSA external type 1, N2-OSPF NSSA external type 2
       E1-OSPF external type 1, E2-0SPF external type 2

C     1.0.0.0/30        [0/0]   direct  1.0.0.1        loop.0.20         4h47m58s
C     1.1.1.0/25        [0/0]   direct  1.1.1.1        vlan.0.1000       4h47m07s
C     10.1.128.0/17     [0/0]   direct  10.1.130.10     vlan.0.128        4h47m06s
C     20.1.0.0/25       [0/0]   direct  20.1.0.1        vlan.0.20         4h47m03s
C     20.1.0.128/25     [0/0]   direct  20.1.0.129      vlan.0.21         4h47m03s
.
.
.
C     200.0.1.128/26    [0/0]  direct  200.0.1.129     vlan.0.437        4h47m08s
C     200.0.1.192/26    [0/0]  direct  200.0.1.193     vlan.0.837        4h47m08s

Number of routes = 18
S Chassis(rw)->
```

The following command displays routes configured on the host stack:

```
S Chassis(rw)->show ip route host

Host IP Route Table for VRF default
Codes: C-connected, D-dynamic, H-host, S-static
       *-no forwarding interface

S*     0.0.0.0/0               10.21.128.1         vlan.0.1
HS*    10.10.10.5              10.20.10.1          vlan.0.1
C*     10.21.128.0/17          10.21.130.59        vlan.0.1
H      10.21.130.59            10.21.130.59        lo.0.1
H      127.0.0.1               127.0.0.1           lo.0.1
H      127.0.2.1               127.0.2.1           lo.0.1

Number of routes = 6
S Chassis(rw)->
```

show ipv6 route

Use this command to display IPv6 routes.

Syntax

```
show ipv6 route [dest-ipv6-address | [<prefix/length> {[longer-prefixes]}] [bgp]
| [connected] | [host {[connected] | [host-address] | [dynamic] | [static]}]
[isis] | [ospf] | [rip] | [topology <topology>]
```

Parameters

dest-ipv6-address	(Optional) Specifies only information for routes with the specified destination IPv6 address will display.
prefix/prefix-length	(Optional) Displays any routes that match the specified prefix and prefix-length.
longer-prefixes	(Optional) Displays all routes that match the specified prefix and length.
bgp	(Optional) Specifies that only BGP routes will display.
host	(Optional) Specifies that only routes with host destination addresses will display.
connected	(Optional) Specifies that only information for connected routes will display.
static	(Optional) Specifies that only information for static routes will display.
summary	(Optional) Specifies that a summary level of IPv6 route information will display.
ospf	(Optional) Displays routes configured for the OSPF routing protocol. For details on configuring OSPF, refer to the *Extreme Networks S-Series Configuration Guide*.
isis	(Optional) Displays routes configured for the ISIS routing protocol. For details on configuring ISIS, refer to the *Extreme Networks S-Series Configuration Guide*.
rip	(Optional) Displays routes configured for the RIP routing protocol. For details on configuring RIP, refer to the *Extreme Networks S-Series Configuration Guide*.
topology *<topology-name>*	(Optional) Displays routes for the specified topology.

Defaults

If an option is not specified, all IPv6 routes display.

Mode

All command modes.

Usage

To display entries in an IPv6 multicast topology routing table, use the **show ipv6 route** command with the **topology** option.

Examples

The following example shows how to display information about the IPv6 route with the destination IPv6 address **1111:1111:1111::/48**:

```
S Chassis(su)->show ipv6 route 1111:1111:1111::/48

IPv6 Route Table for VRF (global)
Codes: C-connected, S-static, R-RIP, B-BGP, O-OSPF

C        1111:1111:1111::/48 [0/0]
          direct    1111:1111:1111:1111::1111:0  vlan.0.50        1d03h05m42s

Number of routes = 1
S Chassis(su)->
```

The following example shows how to display information for all connected IPv6 routes on the router:

```
S Chassis(su)->show ipv6 route connected

IPv6 Route Table for VRF (global)
Codes: C-connected, S-static, R-RIP, B-BGP, O-OSPF

C        1111:1111:1111::/48 [0/0]
          direct    1111:1111:1111:1111::1111:0  vlan.0.50        1d04h21m00s
C        1111:1111:1111:1111::/64 [0/0]
          direct    1111:1111:1111:1111::1111:1010  vlan.0.50        1d04h21m00s
C        2006:7777::3333:0:0:0:0/64 [0/0]
          direct    2006:7777::3333:0:0:0:1  vlan.0.50        1d04h15m09s
C        ba10:1100:aa11::/48 [0/0]
          direct    ba10:1100:aa11:c171::1111:0  vlan.0.50        1d04h21m00s

Number of routes = 4
S Chassis(su)->
```

ip route

Use this command to add or remove a static IP route.

Syntax

ip route {*prefix mask* | *prefix/prefix-length*} {*ip-address* [**recursive**] | **interface** *interface-name* | **vlan** *vlan-id* | **vrf** *egress-vrf* | **blackhole** | **reject** | **probe** {**default** | *probe-name*}} [*distance*] [**tag** *tag-id*]

no ip route {*prefix mask* | *prefix/prefix-length*} {*ip-address* [**recursive**] | **interface** *interface-name*| **vlan** *vlan-id* | **vrf** *egress-vrf* | **blackhole** | **reject** | **probe** {**default** | *probe-name*}} [*distance*] [**tag** *tag-id*]

Parameters

prefix	Specifies a destination IP address prefix.
mask	Specifies a destination prefix mask.
prefix/prefix-length	Specifies a destination IP address in prefix/prefix-length format.
ip-address	Specifies a next-hop router IP address.
interface *interface-name*	Specifies the next-hop interface.
vlan *vlan-id*	Specifies the next-hop VLAN. Valid values are **1** - **4094**.
vrf *egress-vrf*	Specifies the egress VRF router that will determine the next hop for the route.
blackhole	Specifies that packets destined for this route's subnet are silently dropped. An ICMP network unreachable message is not sent to the packet source.
reject	Specifies that packets destined for this route's subnet are dropped, and an ICMP network unreachable message is sent to the packet source.
recursive	(Optional) Specifies that the next-hop interface is determined by route lookup.
probe default | *probe-name*	Specifies either a default or named probe to be configured for this static route.
distance	(Optional) Specifies an administrative distance metric for this route. Valid values are **1** (default) to **255**. Routes with lower values receive higher preference in route selection.
tag *tag-id*	(Optional) Specifies an OSPF tag ID for this route. Valid values are **1** - **4294967295**.

Defaults

- If *distance* is not specified, the default value of 1 will be applied.
- If an OSPF tag ID is not specified, no OSPF tag is associated with the route.
- If **recursive** is not specified, see usage section below.

Mode

Configuration command mode**.**

Usage

This command is used to configure static routes. The route will forward IP traffic depending upon the IP forwarding setting of the routing interface. Routing interfaces are set for IP forwarding by default. To configure a static route as a non-forwarding IP route, set IP forwarding for the routing interface to non-forwarding using the **no ip forwarding** command in interface configuration mode.

Use the **vrf** *egress-vrf* parameter to point to the egress VRF router that will perform the next-hop lookup for this static route. Using the **vrf** *egress-vrf* parameter is more dynamic than configuring a standard static route, in that it determines the next hop based upon a route table lookup. A standard static route specifies a single next hop. Should that next hop be unavailable, the subnet is no longer reachable. A standard static route can be configured to reach the next hop that is a member of a different VRF using the syntax: **ip route** *destination-prefix/length next-hop-address*

interface *next-hop-interface*. Because the **vrf** *egress-vrf* parameter provides greater flexibility in determining the next hop, it is recommended that you use the **vrf** *egress-vrf* parameter.

The default VRF router is referred to as the **global** router. Named VRF routers within a device configured using the **set router vrf create** command are referred to as non-global VRF routers. Static routes are supported between both the **global** router and any non-global VRF router and between any two non-global VRF routers.

If you only enter the prefix/length and the IP address of the nexthop router and do not specify the optional **recursive** parameter, a search is performed of all configured subnets for a subnet containing the next-hop. If found, the static route will be anchored to that interface, else it will become a recursive route.

When configuring a probe for the static route using the **probe** option, the probe session is created on the nexthop address. When the probe session goes down, the static route is disabled. When the probe session comes up, the static route is enabled.

See "ipv6 route" on page 56-7 for IPv6 static route configuration command information.

The "no" form of this command removes the static IP route.

Examples

This example shows how to set IP address 10.1.2.3 as the next hop gateway to destination address 10.0.0.0.:

```
S Chassis(rw-router-config)->ip route 10.0.0.0 255.0.0.0 10.1.2.3
```

This example shows how to set VLAN 100 as the next hop interface to destination address 10.0.0.0:

```
S Chassis(rw-router-config)->ip route 10.0.0.0 255.0.0.0 vlan 100
```

This example shows how to configure, in the VRF Alpha-Group context, the VRF Internet-Access to perform the next hop lookup to destination address 134.141.95.100/24:

```
S Chassis(su)->router Alpha-Group
S Chassis(su-*ha-Group)->configure
S Chassis(su-*ha-Group-config)->ip route 134.141.95.100/24 vrf Internet-Access
```

ipv6 route

Use this command to add or remove a static IPv6 route.

Syntax

ipv6 route *prefix/length* {*ipv6-address* [**recursive** | **interface** *interface-name*] | **interface** *interface-name* | **vlan** *vlan-id* | **vrf** *egress-vrf* | **blackhole** | **reject** | **probe** {**default** | *probe-name*}} [*distance*] [**tag** *tag-id*]

no ipv6 route *prefix/length* {*ipv6-address* [**recursive**] | **interface** *interface-name* | **vlan** *vlan-id* | **vrf** *egress-vrf* | **blackhole** | **reject** | **probe** {**default** | *probe-name*}} [*distance*] [**tag** *tag-id*]

Parameters

prefix/prefix-length	Specifies a destination IP address in prefix/prefix-length format.
ipv6-address	Specifies a next hop IP address.
interface *interface-name*	Specifies a next hop interface ID. When entered with the next-hop IPv6 address, it specifies the interface ID the IPv6 address is assigned to.
vlan *vlan-id*	Specifies the next hop VLAN. Valid values for VLAN ID: **1** - **4094**.

vrf *egress-vrf*	Specifies the egress VRF router as the next hop.
blackhole	Specifies that packets destined for this route's subnet are silently dropped. An ICMP network unreachable message is not sent to the packet source.
reject	Specifies that packets destined for this route's subnet are dropped, and an ICMP network unreachable message is sent to the packet source.
recursive	(Optional) Specifies that the next hop interface is determined by route lookup.
probe default | *probe-name*	Specifies either a default or named probe to be configured for this static route.
distance	(Optional) Specifies an administrative distance metric for this route. Valid values are **1** (default) to **255**. Routes with lower values receive higher preference in route selection.
tag *tag-id*	(Optional) Specifies an OSPF tag ID for this route. Valid values are **1** - **4294967295**.

Defaults

- If **interface** *interface-name* is not specified when configuring an IPv6 address, a specific interface is not configured for the static route.
- If *distance* is not specified, the default value of 1 will be applied.
- If an OSPF tag ID is not specified, no OSPF tag is associated with the route.
- If **recursive** or **interface** *interface-name* are not specified when configuring an IP address, see usage section below.

Mode

Global configuration**.**

Usage

This command is used to configure static routes that will route transit frames.

Use the **vrf** *egress-vrf* parameter to point to the egress VRF instance that will perform the next hop lookup for this static route.

When specifying an IP address as the next hop, it is recommended that you specify the interface the IP address is assigned to. If only the prefix with mask/length and the IP address of the next hop router are entered, and you do not specify the optional **recursive** or the **interface** *interface-name* parameter, when entering the IP address, all configured subnets are searched for a subnet containing the next hop. If found, the static route will be anchored to that interface, else it will become a recursive route.

When configuring a probe for the static route using the **probe** option, the probe session is created on the nexthop address. When the probe session goes down, the static route is disabled. When the probe session comes up, the static route is enabled.

The **no ipv6 route** command removes the specified static IPv6 route.

Examples

This example shows how to:

- Configure a static route with a prefix and length of **2001:11ac:fd34::/48** and a next hop IPv6 address of **2001:11ac:fd34:3333::4**

- Specify that the next-hop interface should be determined using route lookup
- Assign the OSPF tag **65514** to the route

```
S Chassis(su)->configure
S Chassis(su-config)->ipv6 route 2001:11ac:fd34::/48 2001:11ac:fd34:3333::4
recursive tag 65514
S Chassis(su-config)->
```

set ip route

Use this command to add a non-forwarding management IP route to the switch's IP routing table.

Syntax

set ip route {*destination* | **default**} {*gateway* | *interface*} [*mask*]

Parameters

destination	Specifies the IPv4 or IPv6 address of the network or host to be added.
default	Sets the default gateway.
gateway	Specifies the IPv4 or IPv6 address of the next hop router.
interface	Specifies an IP interface. For example: **vlan.0.1**
mask	(Optional) Specifies a netmask.

Defaults

If no *mask* is specified, the specific gateway or interface is used.

Mode

All command modes.

Usage

The **set ip route** command is used to specify static routes that will not be used to route transit frames. Routed static routes can be configured using "ip route" on page 56-5 in configuration command mode.

If the gateway address is specified, the interface defaults to the host (default) VLAN. If the next-hop resides on a VLAN other than the default VLAN, use the interface option to specify the next hop.

A non-forwarding management route can also be configured using "ip route" on page 56-5 in global configuration command mode, with the underlying routing interface set to non-forwarding using the **no ip forwarding** command in interface configuration command mode. The **ip route** command automatically determines the correct VLAN if not specified.

Use "show ip route" on page 56-1 to display routes added to the route table with this command.

Example

This example shows how to add to the routing table an IP route to 192.122.173.42 setting 192.122.168.38 as the gateway:

```
S Chassis(rw)->set ip route 192.122.173.42 192.122.168.38
```

This example shows how to add to the routing table an IP route to 192.122.173.42 using interface VLAN 50:

```
S Chassis(rw)->set ip route 192.122.173.42 vlan 50
```

This example shows how to set 192.122.168.38 as the default gateway for this device:

```
S Chassis(rw)->set ip route default 192.122.168.38
```

clear ip route

Use this command to delete switch IP routing table entries.

Syntax

clear ip route {*destination* | **default**} {*gateway* | *interface*} [*mask*]

Parameters

destination	Specifies the IPv4 or IPv6 address of the network or host to be cleared.
default	Specifies the default gateway.
gateway	Specifies the IPv4 or IPv6 address of the next hop router.
interface	Specifies an IP interface. For example: **vlan.0.1**
mask	(Optional) Specifies a netmask.

Mode

All command modes.

Usage

The **clear ip route** command is used to remove a static route that is not being used to route transit frames. Use the **no** version of "ip route" on page 56-5 to remove static routes that are used to route transit frames.

Example

This example shows how to clear the default gateway:

```
S Chassis(rw)->clear ip route default
```

ip icmp

Use this command to re-enable the Internet Control Message Protocol (ICMP), allowing a router to reply to IP ping requests.

Syntax

ip icmp {**echo-reply** | **mask-reply** | **unreachable**}

no ip icmp {**echo-reply** | **mask-reply** | **unreachable**}

Parameters

echo-reply	Enables ICMP in echo-reply mode.
mask-reply	Enables ICMP in mask-reply mode.

unreachable	Enables ICMP in unreachable mode.

Defaults

None.

Mode

Interface configuration.

Usage

By default, ICMP messaging is enabled on a routing interface for both echo-reply and mask-reply modes. If, for security reasons, ICMP has been disabled using **no ip icmp**, this command will re-enable it on the routing interface.

The "no" form of this command disables ICMP.

Example

This example shows how to enable ICMP in echo-reply mode on VLAN 1:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip icmp echo-reply
```

ipv6 neighbor

Use this command to configure a static entry in the IPv6 neighbor discovery cache.

Syntax

ipv6 neighbor *ipv6-address hardware-address* **interface** *interface*

no ipv6 neighbor *ipv6-address hardware-address* **interface** *interface*

Parameters

ipv6-address	Specifies the IP address of IPv6 neighbor entry.
hardware-address	Specifies the 48-bit hardware address of IPv6 neighbor entry. The hardware address format is H.H.H.
interface *interface*	Specifies the interface to assign the IPv6 neighbor to.

Defaults

None.

Mode

Global Configuration.

Usage

The **no ipv6 neighbor** command removes the specified static entry from the IPv6 neighbor discovery cache.

Example

The following example configures a static entry for IPv6 address **2001:11ac:fd34:3333:0:0:0:3** on a hardware device with a MAC address of **1111.1111.1111** on interface VLAN 51:

```
S Chassis(su)->configure
S Chassis(su-config)->ipv6 neighbor 2001:11ac:fd34:3333:0:0:0:3 1111.1111.1111
interface vlan.0.51
S Chassis(su-config)->
```

ipv6 nd delay-time

Use this command to set the amount of time a neighbor cache entry remains in the delay state before actively probing.

Syntax

ipv6 nd delay-time *interval*

no ipv6 nd delay-time *interval*

Parameters

interval	Specifies the amount of time that should pass before sending another neighbor solicitation during neighbor discovery. Valid values are **1** - **65535** seconds. The default value is **5** seconds.

Defaults

None.

Mode

Global Configuration**.**

Example

This example sets the amount of time a neighbor cache entry remains in the delay state before actively probing to **8** seconds:

```
S Chassis(su-config)->ipv6 nd delay-time 8
S Chassis(su-config)->
```

ipv6 nd reachable-time

Use this command to set the amount of time a neighbor cache entry is considered reachable.

Syntax

ipv6 nd stale-time *interval*

no ipv6 nd stale-time *interval*

Parameters

interval	Specifies the amount of time a neighbor cache entry is considered reachable. Valid values are **1** - **65535** seconds. The default value is **3600** seconds.

Defaults

None.

Mode

Global Configuration.

Example

This example sets the the amount of time a neighbor cache entry is considered reachable to **3200** seconds:

```
S Chassis(su-config)->ipv6 nd stale-time 3200
S Chassis(su-config)->
```

ipv6 nd retransmit-time

Use this command to set the amount of time that should pass before sending another neighbor solicitation during neighbor discovery.

Syntax

ipv6 nd retransmit-time *interval*

no ipv6 nd retransmit-time *interval*

Parameters

interval	Specifies the amount of time that should pass before sending another neighbor solicitation during neighbor discovery. Valid values are **1** - **65535** seconds. The default value is **1** second.

Defaults

None.

Mode

Global Configuration.

Example

This example sets the amount of time that should pass before sending another neighbor solicitation during neighbor discovery to **5** seconds:

```
S Chassis(su-config)->ipv6 nd retransmit-time 5
S Chassis(su-config)->
```

ipv6 nd stale-time

Use this command to set the amount of time that passes before a neighbor cache entry is considered stale.

Syntax

ipv6 nd stale-time *interval*

no ipv6 nd stale-time *interval*

Parameters

interval	Specifies the amount of time that passes before a neighbor cache entry is considered stale. Valid values are **1** - **65535** seconds. The default value is **1200** seconds.

Defaults

None.

Mode

Global Configuration**.**

Example

This example sets the amount of time that passes before a neighbor cache entry is considered stale to **1400** seconds:

```
S Chassis(su-config)->ipv6 nd stale-time 1400
S Chassis(su-config)->
```

show ipv6 neighbors

Use this command to display configured entries in the IPv6 neighbor discovery cache.

Syntax

show ipv6 neighbors [*ipv6-address*] [**group**] [**interface** *interface*] [**verbose**] [**statistics**]

Parameters

ipv6-address	(Optional) Specifies the IPv6 address to display.
group	(Optional) Displays neighbor entries in groups of 5, delineated by a line-break.
interface *interface*	(Optional) Specifies that only entries for the specified interface should display.
verbose	(Optional) Specifies that additional information should display regardless of terminal column size.
statistics	(Optional) Specifies that various IPv6 neighbor cache statistics should display.

Defaults

If *ipv6-address* is not specified, all IPv6 address entries will display.

If **group** is not specified, all interfaces are displayed without line-breaks.

If **interface** *interface* is not specified, all interfaces will display.

If **verbose** is not specified, the default level of data based upon options specified will display.

If **statistics** is not specified, entry information will display.

Mode

All command modes.

Examples

The following example shows how to display information for all learned IPv6 neighbor entries in the neighbor discovery cache:

```
S Chassis(su)->show ipv6 neighbors
FLAGS:    I = Incomplete     R = Reachable
          S = Stale          D = Delay
          P = Probe          L = Local
          F = Fixed (Static) H = Host Interest
          V = VRRP           2 = Secondary VLAN

Note: Additional information is available by using the 'verbose' option or by
increasing the size of your terminal columns to 111 (use 'set width')

Ipv6 Address                          Hardware Address  Flg Age    Interface
------------------------------------- ----------------- --- ------ ---------------
2013:0:0:0:0:0:0:2                    00-11-88-fd-8e-f0  LR      - vlan.0.11
fe80:0:0:0:211:88ff:fefd:8ef0         00-11-88-fd-8e-f0  LR      - vlan.0.11
------------------------------------- ----------------- --- ------ ---------------
Neighbor Entries Found: 2
S Chassis(su)->
```

Table 56-1 provides an explanation of the command output.

Table 56-1 Show IPv6 Neighbors Output Display

Output...	What it displays...
IPv6 address	An IPv6 address of a neighbor entry.
Hardware Address	The MAC address of an IPv6 neighbor entry.
Flg	Zero or more flags associated with an IPv6 neighbor entry: • **I** – The entry is currently in address resolution • **R** – The entry is reachable • **S** – The entry is stale • **D** – A short random state of delay prior to initiating a probe • **P** – A probe is active for this entry • **L** – This entry is a local entry • **F** – This is a static entry • **H** – Host Interest: The ARP entry has been used for direct communication with the router as opposed to communication between hosts that pass through the router. • **2** – Secondary VLAN Entry: The ARP entry belongs to a host on a Secondary VLAN.
Age	The length of time this entry has existed.
Updated	The length of time since the last update for this entry.
Expire	The length of time before this entry moves from its current state to the next state.
Interface	The interface the ARP entry is assigned to.
Port	The host port for this entry.

The following example shows how to display cache statistics information for all IPv4 and IPv6 neighbors:

```
S Chassis(su)->show ipv6 neighbors statistics
Total Number of Entries (IPv4 and IPv6):                    9
Number of IPv4 Entries:                                     3
Number of IPv6 Entries:                                     6
Number of Static Entries:                                   1
Number of Dynamic Entries:                                  9
Number of Static Entries Loaded While Booting:              0

Total Number of ARP Packets Received:                 3048320 *
Number of Request Packets Received:                   3037009 *
Number of Reply Packets Received:                       11311 *
Number of Gratuitous ARP Packets Received:              11552 *

Number of ARP packets Sent:                               778 *
Number of ARP Entries that Could not be Resolved:           0 *

*This blade only

S Chassis(su)->
```

show ipv6 general-prefix

Use this command to display configured IPv6 general prefix information.

Syntax

show ipv6 general-prefix

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

The following example shows how to display information for all configured general prefixes for this router:

```
S Chassis(su)->show ipv6 general-prefix
  ipv6 general-prefix doc-prefix 2001:11ac:fd34::/48
  ipv6 general-prefix mark-prefix 2006:7777::/48
S Chassis(su)->
```

ipv6 general-prefix

Use this command to define an IPv6 general prefix.

Syntax

ipv6 general-prefix *name prefix/length*

Parameters

name	Specifies the name assigned the general prefix.
prefix/length	Specifies the prefix and length of the IPv6 network assigned to the general prefix.

Defaults

None.

Mode

Global Configuration.

Usage

The general prefix is an ease of use feature that allows an assigned name to represent a network prefix from which longer IPv6 addresses can be configured. Network renumbering is simplified by changing the portion of addresses to which the general prefix is assigned, by redefining the general prefix.

When using general prefix to configure an IPv6 address, you can extend the network prefix by adding to the length specified in the **ipv6 address** command. See "ipv6 address" on page 55-3 for command details.

If you delete the general prefix, any IPv6 addresses based upon the general prefix remain. Use the **no ipv6 address** command to remove the IPv6 address.

The S-Series supports the configuration of up to 64 general prefixes on a system.

Example

The following example creates a general prefix named "Doc-Prefix" with a prefix value of **2001:11ac:fd34::/48** and assigns the IPv6 address **2001:11ac:fd34:50:0:0:abcd:33** to VLAN 51. The general prefix **Doc-Prefix** is followed by **::50:0:0:abcd:33/64**. The subnet length is changed to **/64** adding **:50** to the general prefix to create a network prefix of **2001:11ac:fd34:50/64** for this IPv6 address:

```
S Chassis(su)->configure
S Chassis(su-config)->ipv6 general-prefix Doc-Prefix 2001:11ac:fd34::/48
S Chassis(su-config)->show ipv6 general-prefix
  ipv6 general-prefix Doc-Prefix 2001:11ac:fd34::/48
S Chassis(su-config)->interface vlan 51
S Chassis(su-config-intf-vlan.0.51)->ipv6 address Doc-Prefix ::50:0:0:abcd:33/64
S Chassis(su-config-intf-vlan.0.51)->show ipv6 interface vlan.0.51

 vlan.0.51 is Operationally down, Administratively down
  IPv6 is enabled link-local address is fe80::211:88ff:fe7c:32c1%vlan.0.51
```

```
  Global unicast address(es):
    2001:11ac:fd34:50:0:0:abcd:33, subnet is 2001:11ac:fd34:50::/64
...
S Chassis(su-config-intf-vlan.0.51)->
```

57

Tunnel Configuration Commands

This chapter describes the L3 and L2 tunnel set of commands and how to use them. For information about configuring Layer 3 and Layer 2 tunnels, refer to the "Tunneling Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

The commands in this chapter describe how to:

- Display tunnel information
- Specify the tunnel source and destination addresses
- Configure the tunnel mode
- Configure GRE mode tunnel keepalive, and Type of Service
- Configure a GRE keyword
- Configure a tunnel probe

For information about...	Refer to page...
Reviewing Existing Tunnels	57-1
Configuring Tunnels	57-4

Reviewing Existing Tunnels

This command allows you to display a list of tunnels currently configured on the device including: tunnel mode, delivery interface, end-point addresses and tunnel state.

For information about...	Refer to page...
show tunnel	57-1

show tunnel

Use this command to display information related to one or more tunnels.

Syntax

show tunnel [*tunnel-id*] [**verbose**]

Parameters

tunnel-id	(Optional) Displays information for a specific tunnel using the format **tun.***x*.*y*.

verbose	(Optional) Displays a verbose level of tunnel information including configuration parameter values and state.

Defaults

If no options are specified, a standard level of information related to all tunnel interfaces is displayed.

Mode

All command modes.

Examples

This example shows how to display information for all tunnels:

```
S Chassis(rw)->show tunnel

 Codes: A  = Admin status (E-enabled, D-disabled)
        O  = Tunnel Oper status (U-up, D-down)
        M  = Tunnel is enabled for remote mirroring (Y-yes, N-no)
        W  = Tunnel has L2 port configured (Y-yes, N-no)
       S  = Tunnel point, probe or keepalive status (U-up, D-down, N-not configured P-pending R-recursive
route)
        T  = Tunnel IP Address type (L-local, R-remote, P-Probe, K-Keepalive)
        *  = indicates that a keyword mismatch was detected

                                 Delivery
Interface Mode        Keyword    Interface    A O M W S T Endpoint IP Addresses
--------- ----------- ---------- ----------- - - - - - - ---------------------------------------
tun.0.1   gre         777         vlan.0.50   E U N N U L 99.99.99.1
                                                      U R 88.88.88.1
                                                      U P 88.88.88.1
                                                      U K 88.88.88.1
tun.0.2   gre         *888        vlan.0.50   E D N N U L 2999::1
                                                      U R 2888::1
                                                      U P 2888::1
                                                      D K 2888::1
tun.0.3   gre         999         vlan.0.50   E U N N U L 77.77.77.1
                                                      U R 66.66.66.1
                                                      U P 66.66.66.1
                                                      U K 66.66.66.1
S Chassis(rw)->
```

Note: Note that the "*" in the keyword display for tun.0.2 ("*888") shows that the configured keyword is "888", and tunneled GRE packets (matching the tunnel source/destination) were received, but dropped, because there was a keyword mismatch. This is explained in the verbose display below:

```
S Chassis(rw)->show tunnel verbose tun.0.2
Interface: tun.0.2
 Mode: gre, State: down
 ip address 8.0.0.2 255.0.0.0 primary
 ipv6 address 3020::2/64
```

```
 Tunnel Source: 2999::1, interface loop.0.1, state up
 Tunnel Destination: 2888::1, interface vlan.0.50, state up
 Tunnel Source VRF: global
 Tunnel Destination VRF: global
 Encapsulation Limit: no limit, Hop Limit: 64, TOS value: copied from payload
 Tunnel Keyword 888
 Tunnel Admin enabled, Oper down
 Tunnel Oper Status Down Causes:
   Tunnel keepalive is down
   Please check that the tunnel keywords match on each side of the tunnel
   Keyword mismatch detected. Last keyword received 88
 Tunnel Probe Name icmp-probe
 Tunnel Probe IP 2888::1
 Tunnel Probe Session State Up
 Tunnel Keepalive period is 2
 Tunnel Keepalive retries are 1
 Tunnel Keepalive retries left are 0
```

This example shows how to display a verbose level of information for tunnel 1:

```
S Chassis(rw)->show tunnel tun.0.1 verbose
Interface: tun.0.1
 Mode: gre, State: up
 ip address 7.0.0.2 255.0.0.0 primary
 ipv6 address 3010::2/64
 Tunnel Source: 99.99.99.1, interface loop.0.1, state up
 Tunnel Destination: 88.88.88.1, interface vlan.0.50, state up
 A recursive route to the tunnel destination was last detected on 06-03-13 15:11:35
 Tunnel Source VRF: global
 Tunnel Destination VRF: global
 Encapsulation Limit: no limit, Hop Limit: 64, TOS value: copied from payload
 Tunnel Keyword 777
 Tunnel Admin enabled, Oper up
 Tunnel Probe Name icmp-probe
 Tunnel Probe IP 88.88.88.1
 Tunnel Probe Session State Up
 Tunnel Keepalive is active
 Tunnel Keepalive period is 2
 Tunnel Keepalive retries are 1
 Tunnel Keepalive retries left are 1
S Chassis(rw)->
```

Configuring Tunnels

The commands detailed in this sections are used to configure a tunnel. See "interface" on page 54-2 for details on how to create a tunnel interface. The IP address(es) configured for the tunnel interface are configured within tunnel interface configuration mode. For IPv4 interface address configuration details see "ip address" on page 54-6. For IPv6 interface address configuration details see "ipv6 address" on page 55-3.

For information about...	Refer to page...
tunnel source	57-4
tunnel destination	57-5
tunnel any-remote enable	57-7
tunnel keepalive	57-8
tunnel keyword	57-8
tunnel mode	57-9
tunnel mode gre l2 (Virtual Private Port)	57-10
tunnel mode gre l2 (Virtual Private Ethernet Service)	57-11
tunnel mirror enable	57-12
tunnel mode gre l2 (mirrored tunnel)	57-13
tunnel probe	57-14
tunnel tos	57-15

tunnel source

Use this command to configure the IPv4 or IPv6 source address for this tunnel.

Syntax

tunnel source *ip-address*

no tunnel source

Parameters

ip-address	Specifies the source IPv4 or IPv6 tunnel address for the tunnel.

Defaults

None.

Mode

Tunnel Interface Configuration command mode.

Usage

Each tunnel has a source and destination IP address configured from the perspective of the local router. The source address is the local startpoint of the tunnel. The destination address is the remote endpoint of the tunnel. The tunnel source and destination addresses can be configured on either loopback or VLAN interfaces, but are usually loopback interface IP addresses. The delivery

interface for the tunnel is the underlying interface for the IP address associated with the selected route. The delivery interface, if known, for the tunnel is specified in the **show tunnel** command output.

Use the "no" option for this command to remove the source IP address configuration for the tunnel.

Examples

This example shows how to configure the IPv4 source address to **88.88.88.1** for tunnel **1**:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface tunnel 1
S Chassis(rw-config-intf-tun.0.1)->tunnel source 88.88.88.1
S Chassis(rw-config-intf-tun.0.1)->show tunnel tun.0.1

Codes:A  = Admin status (E-enabled, D-disabled)
      O  = Tunnel Oper status (U-up, D-down)
      P  = Tunnel point or probe status (U-up, D-down, N-not configured or pending)
      T  = Tunnel IP Address type (L-local, R-remote, P-Probe, K-Keepalive)

Delivery
Interface Mode        Interface   A O P T Endpoint IP Addresses
--------- ----------- ----------- - - - - ---------------------------------------
tun.0.1   gre         vlan.0.50   E U U L 88.88.88.1
```

This example shows how to configure the IPv6 source address to **2002:2010::1** for tunnel **10**:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface tunnel 10
S Chassis(rw-config-intf-tun.0.10)->tunnel source 2002:2010::1
S Chassis(rw-config-intf-tun.0.10)->show tunnel tun.0.10

Codes:A  = Admin status (E-enabled, D-disabled)
      O  = Tunnel Oper status (U-up, D-down)
      P  = Tunnel point or probe status (U-up, D-down, N-not configured or pending)
      T  = Tunnel IP Address type (L-local, R-remote, P-Probe, K-Keepalive)

Delivery
Interface Mode        Interface   A O P T Endpoint IP Addresses
--------- ----------- ----------- - - - - ---------------------------------------
tun.0.10  gre         unknown     D D N L 2002:2010::1
```

tunnel destination

Use this command to configure the IPv4 or IPv6 destination address for this tunnel.

Syntax

tunnel destination *ip-address*

no tunnel destination

Parameters

ip-address	Specifies the destination IPv4 or IPv6 tunnel address for the tunnel.

Defaults

None.

Mode

Tunnel Interface Configuration command mode.

Usage

Each tunnel has a source and destination IP address configured from the perspective of the local router. The destination address is the remote endpoint of the tunnel. The destination address can be either a loopback or VLAN interface, but is usually a loopback address.

Use the “no” option for this command to remove the destination IP address configuration for the tunnel.

Examples

This example shows how to configure the IPv4 destination address to **99.99.99.1** for tunnel **1**:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface tunnel 1
S Chassis(rw-config-intf-tun.0.1)->tunnel destination 99.99.99.1
S Chassis(rw-config-intf-tun.0.1)->show tunnel

Codes:A  = Admin status (E-enabled, D-disabled)
      O  = Tunnel Oper status (U-up, D-down)
      P  = Tunnel point or probe status (U-up, D-down, N-not configured or pending)
      T  = Tunnel IP Address type (L-local, R-remote, P-Probe, K-Keepalive)

                     Delivery
Interface Mode       Interface   A O P T Endpoint IP Addresses
--------- ---------- ----------- - - - - ---------------------------------------
tun.0.1   gre        vlan.0.50   E U U L 88.88.88.1
                                     U R 99.99.99.1
```

This example shows how to configure the IPv6 destination address to **2002:2010::5** for tunnel **10**:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface tunnel 10
S Chassis(rw-config-intf-tun.0.10)->tunnel destination 2002:2010::5
S Chassis(rw-config-intf-tun.0.10)->show tunnel tun.0.10

Codes:A  = Admin status (E-enabled, D-disabled)
      O  = Tunnel Oper status (U-up, D-down)
      P  = Tunnel point or probe status (U-up, D-down, N-not configured or pending)
      T  = Tunnel IP Address type (L-local, R-remote, P-Probe, K-Keepalive)

Delivery
Interface Mode       Interface   A O P T Endpoint IP Addresses
--------- ---------- ----------- - - - - ---------------------------------------
tun.0.10  gre        unknown     D D N L 2002:2010::1
                                     U R 2002:2010::5
```

tunnel any-remote enable

Use this command to configure a L2 (Virtual Private Port) tunnel to accept any remote IP as the source IP address, as long as the destination IP address matches this tunnel's source IP.

Syntax

tunnel any-remote enable

no tunnel any-remote enable

Parameters

None.

Defaults

The tunnel any-remote feature is disabled by default.

Mode

Tunnel Interface Configuration command mode.

Usage

This command permits the configuration of a source address only L2 Virtual Private Port tunnel, allowing multiple tunneled port mirrors to use this tunnel source as a destination.

When any-remote is enabled on the L2 tunnel:

- The tunnel accepts any tunneled packet destined to it's tunnel source. It decapsulates the packet and forwards it out the Ethernet port assigned to the tunnel.
- Any packets received on the Ethernet port assigned to the tunnel are switched or routed as normal, and not sent across the Virtual Private Port.
- If a destination address is configured on an any-remote enabled L2 tunnel, it has no practical affect, but it must have a route to the destination for the tunnel to be up.

Use the “no” option for this command to reset tunnel any-remote to the default value of disabled.

Examples

This example shows how to enable tunnel any-remote on tunnel **1** configured for L2 Virtual Private Port on port **ge.1.1**:

```
S Chassis(rw)->configure
S Chassis(rw-config)->Interface tun.0.1
S Chassis(rw-config-intf-tun.0.1)->tunnel mode gre l2 ge.1.1
S Chassis(rw-config-intf-tun.0.1)->tunnel any-remote enable
S Chassis(rw-config-intf-tun.0.1)->tunnel source 10.10.10.1
S Chassis(rw-config-intf-tun.0.1)->no shutdown
S Chassis(rw-config-intf-tun.0.1)->exit
S Chassis(rw-config)->
```

tunnel keepalive

Use this command to set the GRE tunnel keepalive transmit interval and retries.

Syntax

tunnel keepalive *seconds retries*

no tunnel keepalive *seconds retries*

Parameters

seconds	Specifies the tunnel keepalive transmit interval in seconds. Valid Values are **1** - **32767** seconds. The default value is not set.
retries	Specifies the number of keepalive retries before the tunnel is declared down. Valid Values are **1** - **255**. The default value is not set.

Defaults

None.

Mode

Tunnel Interface Configuration command mode.

Usage

The keepalive configuration only affects GRE IPv4 over IPv4 tunnels. Unlike a tunnel probe that is only capable of monitoring the state of the specified IP address, GRE keepalive both monitors the state of the IP address and whether the end-point was able to decapsulate the tunnel packet. A failed keepalive causes the tunnel to transition to the down state.

Use the “no” option for this command to disable keepalive on the tunnel

Example

This example shows how to set the tunnel keepalive interval to **3** seconds and retries to **1**:

```
S Chassis(rw)->tunnel keepalive 3 1
```

tunnel keyword

Use this command to configure a GRE keyword for the tunnel.

Syntax

tunnel keyword *keyword*

no tunnel keyword

Parameters

keyword	Specifies the GRE keyword for the tunnel. Valid values are **0** - **4294967295**.

Defaults

None.

Mode

Tunnel Interface Configuration command mode.

Usage

The GRE keyword, as defined in RFC 2890, is a four octet number inserted by the encapsulator. It may be used by the receiver to authenticate the source of the packet. If a GRE keyword is configured at either end of the tunnel, the keyword configuration must match at both ends of the tunnel. If a mis-match occurs, packets are dropped and an asterisk (*) is displayed to the left of the **show tunnel** command tunnel entry.

The keyword configuration is only used in GRE tunnel mode.

Use the “no” option for this command to remove the GRE keyword for the tunnel.

Example

This example shows how to set the GRE keyword to **123456** for tunnel **1**:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface tunnel 1
S Chassis(rw-config-intf-tun.0.1)->tunnel keyword 123456
S Chassis(rw-config-intf-tun.0.1)->
```

tunnel mode

Use this command to configure the Layer 3 tunnel mode.

Syntax

tunnel mode {**gre** | **ipip** [**ipv6**] | **ipv6ip** [**ipv6**]}

no tunnel mode

Parameters

gre	Specifies the Generic Routing Encapsulation (GRE) Layer 3 tunnel mode as defined by RFC 2784.
ipip	Specifies an IPv4 packet over an IPv4 Layer 3 tunnel as defined by RFC 2003.
ipip ipv6	Specifies an IPv4 packet over an IPv6 Layer 3 tunnel as defined by RFC 2473.
ipv6ip	Specifies an IPv6 packet over an IPv4 Layer 3 tunnel as defined by RFC 2473.
ipv6ip ipv6	Specifies an IPv6 packet over an IPv6 Layer 3 tunnel as defined by RFC 2473.

Defaults

Tunnel mode defaults to GRE.

Mode

Tunnel Interface Configuration command mode.

Usage

The tunnel mode determines the encapsulation method used by the tunnel. The tunnel packet contains two headers based upon the:

- Source and destination IP type of the packet entering the tunnel (inner header)
- Source and destination IP type of the tunnel (outer header)

Before the packet enters the tunnel, there is only a single IP header. When the packet enters the tunnel, this original IP header becomes the tunnel inner header. The inner header IP address type (IPv4 or IPv6) is determined by the source and destination IP address of the packet entering the tunnel. Once the packet enters the tunnel, an outer header is added to it. The IP type of the outer header is determined by the source and destination addresses configured for the tunnel using "tunnel source" on page 57-4 and "tunnel destination" on page 57-5. The tunnel mode is specified as the inner address type over the outer address type. For example, if the original packet is an IPv6 packet and it is entering an IPv4 tunnel, the tunnel type is specified as IPv6 over IPv4 and you would use the keyword **ipv6ip** to specify the tunnel mode.

The GRE tunnel mode type is a generic type defined by FRC 2784. The GRE mode is capable of processing any of the four tunnel types and should be used if you do not want to limit the tunnel to a specific IP header combination. The other four parameter options limit the tunnel to the specified IP header combination.

Note: Disable the tunnel interface using the shutdown command before changing the tunnel mode using this command. After changing the tunnel mode, enable the tunnel interface using the **no shutdown** command. See "no shutdown" on page 54-11 for details on enabling and disabling an interface.

Use the "no" option for this command to reset the tunnel mode to the default value of GRE.

Examples

This example shows how to set the tunnel 1 mode to IPv6 over IPv4:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface tunnel 1
S Chassis(rw-config-intf-tun.0.1)->tunnel mode ipv6ip
S Chassis(rw-config-intf-tun.0.1)->
```

This example shows how to set the tunnel 1 mode to IPv4 over IPv6:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface tunnel 1
S Chassis(rw-config-intf-tun.0.1)->tunnel mode ipip ipv6
S Chassis(rw-config-intf-tun.0.1)->
```

tunnel mode gre l2 (Virtual Private Port)

Use this command to bind a physical port to a Virtual Private Port L2 tunnel.

Syntax

tunnel mode gre l2 *port-name*

no tunnel mode gre l2 *port-name*

Parameters

port-name	Specifies the name of the physical port to bind to this L2 tunnel.

Defaults

None.

Mode

Tunnel Interface Configuration command mode.

Usage

This command configures one end of a Virtual Private Port L2 tunnel. Virtual Private Port L2 tunnels permit the user to extend a virtual wire through an arbitrary routed network using GRE with transparent bridging. The configuration on each end of the tunnel specifies a physical port to be connected to the Virtual Private Port. Once configured in this manner, any packets arriving on that physical port are immediately encapsulated and routed to the other end of the tunnel. When the packet arrives at the remote end of the tunnel, it is immediately de-encapsulated and sent out the configured port on that end of the tunnel. The net effect is to create a direct connection between each end of the tunnel. No switch or router configuration affects the original packet. The packet arriving at the ingress port is tunneled without change to the tunnel's remote end.

Note: Disable the tunnel interface using the shutdown command should you have a need to change the tunnel mode. After changing the tunnel mode, enable the tunnel interface using the **no shutdown** command. See "no shutdown" on page 54-11 for details on enabling and disabling an interface.

Use the "no" option for this command to reset the tunnel mode to the default value of GRE. Refer to "tunnel mode" on page 57-9 for default tunnel mode information.

Examples

This example shows how to set:

- IP address **10.10.10.1** as the GRE L2 tunnel source:
- IP address **10.10.10.2** as the GRE L2 tunnel destination
- Physical port **ge.1.2** as the bound physical port for the GRE L2 tunnel **1**

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface tunnel 1
S Chassis(rw-config-intf-tun.0.1)->tunnel source 10.10.10.1
S Chassis(rw-config-intf-tun.0.1)->tunnel destination 10.10.10.2
S Chassis(rw-config-intf-tun.0.1)->tunnel mode gre l2 ge.1.2
S Chassis(rw-config-intf-tun.0.1)->no shutdown
S Chassis(rw-config-intf-tun.0.1)->
```

tunnel mode gre l2 (Virtual Private Ethernet Service)

Use this command to bind a tunnel bridge port (Virtual Private Ethernet Service) to a L2 tunnel.

Syntax

tunnel mode gre l2 *tb-port-name*

```
no tunnel mode gre l2 tb-port-name
```

Parameters

tb-port-name	Specifies the name of the tunnel bridge port to bind to this L2 tunnel. Tunnel bridge ports are defined as **tbp.0.***x* where *x* is the number of the tunnel bridge port.

Defaults

None.

Mode

Tunnel Interface Configuration command mode.

Usage

This command binds the specified tunnel bridge port to the routing tunnel interface with this L2 tunnel. L2 tunnel mode is specified within the L3 tunnel configuration.

Note: Disable the tunnel interface using the shutdown command should you have a need to change the tunnel mode. After changing the tunnel mode, enable the tunnel interface using the **no shutdown** command. See "no shutdown" on page 54-11 for details on enabling and disabling an interface.

Use the "no" option for this command to reset the tunnel mode to the default value of GRE. Refer to "tunnel mode" on page 57-9 for default tunnel mode information.

Examples

This example shows how to set:

- IP address **10.10.10.1** as the GRE L2 tunnel source:
- IP address **10.10.10.2** as the GRE L2 tunnel destination
- Tunnel bridge port **tbp.0.1** as the bound port for the GRE L2 tunnel **1**

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface tunnel 1
S Chassis(rw-config-intf-tun.0.1)->tunnel source 10.10.10.1
S Chassis(rw-config-intf-tun.0.1)->tunnel destination 10.10.10.2
S Chassis(rw-config-intf-tun.0.1)->tunnel mode gre l2 tbp.0.1
S Chassis(rw-config-intf-tun.0.1)->no shutdown
S Chassis(rw-config-intf-tun.0.1)->
```

tunnel mirror enable

Use this command to enable a remote mirror using Layer 2 tunneling.

Syntax

```
tunnel mirror enable
no tunnel mirror enable
```

Parameters

None.

Defaults

Remote mirroring using Layer 2 tunnels is disabled by default.

Mode

Tunnel Interface Configuration command mode.

Usage

This command allocates the necessary resources to support mirrored packets. It searches for SMON or policy port mirrors that use the mirror destination port specified in "tunnel mode gre l2 (mirrored tunnel)" on page 57-13. Once the mirrored tunnel is enabled, the specified port is set to loopback mode and Layer 2 traffic will no longer ingress or egress the port, only mirrored traffic from the destination port.

When configuring the L2 tunnel on the remote side, where the remote mirrored port destination resides, do not enable the L2 tunnel using this command.

Use the "no" option for this command to disable the Layer 2 mirrored tunnel.

Examples

This example shows how to enable the L2 mirrored tunnel for the mirror-destination port ge.1.8:

- Tunnel interface 5
- Tunnel destination 99.99.99.1
- Tunnel mode GRE L2 for destination mirrored port ge.1.8
- Tunnel source 88.88.88.1

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface tunnel 5
S Chassis(rw-config-intf-tun.0.5)->tunnel destination 99.99.99.1
S Chassis(rw-config-intf-tun.0.5)->tunnel mode gre l2 ge.1.8
S Chassis(rw-config-intf-tun.0.5)->tunnel source 88.88.88.1
S Chassis(rw-config-intf-tun.0.5)->tunnel mirror enable
S Chassis(rw-config-intf-tun.0.5)->no shutdown
S Chassis(rw-config-intf-tun.0.5)->exit
S Chassis(rw-config)->
```

tunnel mode gre l2 (mirrored tunnel)

Use this command to configure the Layer 2 GRE mirrored tunnel mode.

Syntax

tunnel mode gre l2 *mirrored-port-string*

no tunnel mode

Parameters

mirrored-port-string	Specifies the port string of the mirrored remote destination port for this L2 mirrored tunnel.

Defaults

None.

Mode

Tunnel Interface Configuration command mode.

Usage

The tunnel mode determines the encapsulation method used by the tunnel. This command instructs the tunnel to use L2 GRE encapsulation mode for the remote mirror-destination port specified.

See the "tunnel mirror enable" on page 57-12 for details on enabling the Layer 2 remote mirrored tunnel.

Note: Disable the tunnel interface using the shutdown command before changing the tunnel mode using this command. After changing the tunnel mode, enable the tunnel interface using the **no shutdown** command. See "no shutdown" on page 54-11 for details on enabling and disabling an interface.

Use the "no" option for this command to reset the tunnel mode to the default value of GRE.

Examples

This example shows how to set the tunnel mode GRE Layer 2 for the mirror-destination port ge.1.8 and enable the tunnel for:

- Tunnel interface 5
- Tunnel destination 99.99.99.1
- Tunnel source 88.88.88.1

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface tunnel 5
S Chassis(rw-config-intf-tun.0.5)->tunnel destination 99.99.99.1
S Chassis(rw-config-intf-tun.0.5)->tunnel mode gre l2 ge.1.8
S Chassis(rw-config-intf-tun.0.5)->tunnel source 88.88.88.1
S Chassis(rw-config-intf-tun.0.5)->tunnel mirror enable
S Chassis(rw-config-intf-tun.0.5)->no shutdown
S Chassis(rw-config-intf-tun.0.5)->exit
S Chassis(rw-config)->
```

tunnel probe

Use this command to configure a tunnel probe to monitor the tunnel destination address.

Syntax

tunnel probe probe-name {**default** | *probe-name*}

no tunnel probe

Parameters

probe-name default | *probe-name*	Specifies the default probe (named **$tunnel_default**) or a named probe will be used to monitor the specified IP address.

Defaults

None.

Mode

Tunnel Interface Configuration command mode.

Usage

A tunnel probe is used to monitor a tunnel endpoint IP address. If a probe fails, the associated tunnel is taken down. A default ICMP tunnel probe exists named **$tunnel_default** or a probe can be configured using the tracked object manager probe facility. See Chapter 22, **Tracked Object Manager Commands** for command details for creating and configuring a probe. See the "Tracked Object Manager Configuration" chapter of the *Extreme Networks S-Series Configuration Guide* for default tunnel probe and tunnel probe configuration details.

Use the "no" option for this command to remove the tunnel probe configuration for the tunnel.

Example

This example shows how to monitor the tunnel destination address for tunnel **1** using the default tunnel probe (you could also specify the default tunnel probe name: **$tunnel_default** instead of the **default** keyword):

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface tunnel 1
S Chassis(rw-config-intf-tun.0.1)->tunnel probe probe-name default
S Chassis(rw-config-intf-tun.0.1)->
```

tunnel tos

Use this command to configure a Type of Service (ToS) for the tunnel.

Syntax

tunnel tos *tos*

no tunnel tos

Parameters

tos	Specifies the ToS applied to packets over the tunnel. Valid Values are 0 - 63. Default value is copied from the packet payload.

Defaults

None.

Mode

Tunnel Interface Configuration command mode.

Usage

ToS configuration using this command only affects the ToS value of the outer tunnel header. Any ToS value configured for the inner header remains unchanged.

Use the “no” option for this command to reset the ToS applied to packets for the tunnel to the default value of copied from the packet payload.

Example

This example shows how to set the ToS applied to packets over tunnel **1** to **33**:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface tunnel 1
S Chassis(rw-config-intf-tun.0.1)->tunnel tos 33
S Chassis(rw-config-intf-tun.0.1)->
```

58

L3 VPN Commands

This chapter describes the Layer 3 (L3) VPN set of commands and how to use them. For information about configuring L3 VPN, refer to the "L3 VPN Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
VRF L3 VPN Commands	58-1
BGP L3 VPN Commands	58-17

VRF L3 VPN Commands

For information about...	Refer to page...
mpls ip	58-2
mpls ipv6	58-2
mpls ldp-lsr-id	58-3
mpls label-protocol-ldp	58-4
mpls ldp-label-allocate	58-5
mpls ldp-label-retention-mode	58-6
mpls ip propagate-ttl	58-7
mpls label mode	58-7
rd	58-8
route-target	58-10
vpn id	58-11
show mpls interface	58-12
show mpls forwarding-table	58-13
show mpls ldp-parameters	58-14
show mpls ip-bindings	58-15
show mpls ldp-neighbor	58-16

mpls ip

Use this command to enable or disable MPLS encapsulation for IPv4 routing.

Syntax

mpls ip

no mpls ip

Parameters

None.

Defaults

IPv4 routing MPLS encapsulation is disabled by default.

If an exclude next hop address is not specified, MPLS includes all next hops.

Mode

Global router or interface configuration mode.

Usage

MPLS encapsulation must be enabled on all routers on the Label Switched Path (LSP) between Label Edge Routers (LER). When MPLS encapsulation is enabled, an MPLS label stack follows the Ethernet header and contains an outer label path to the egress VPN router and an inner label identifying the VPN. The outer label egress VPN router path is assigned to the MPLS router by the Label Distribution Protocol (LDP) and is used by the receiving Label Switch Router (LSR) to determine the next hop on the LSP. The LSR removes the MPLS label from the header and replaces it with a new label before the packet is forwarded to the next LSR in the LSP.

In interface configuration mode, this command enables MPLS encapsulation for IPv4 on the interface. MPLS IPv4 interface configuration requires that MPLS encapsulation also be configured in global router command mode.

The “no” form of this command disables IPv4 routing MPLS encapsulation for the command mode context.

Examples

This example shows how to enable IPv4 MPLS encapsulation:

```
S Chassis(su)->configure
S Chassis(su-config)->mpls ip
S Chassis(su-config)->
```

mpls ipv6

Use this command to enable or disable MPLS encapsulation for IPv6 routing.

Syntax

mpls ipv6 *transport-address*

no mpls ipv6 *transport-address*

Parameters

transport-address	Specifies the MPLS IPv6 transport address in IPv6 format.

Defaults

IPv6 routing MPLS encapsulation is disabled by default.

Mode

Global router configuration mode.

Usage

MPLS encapsulation must be enabled on all routers on the Label Switched Path (LSP) between Label Edge Routers (LER). When MPLS encapsulation is enabled, an MPLS label stack follows the Ethernet header and contains an outer label path to the egress VPN router and an inner label identifying the VPN. The outer label egress VPN router path is assigned to the MPLS router by the Label Distribution Protocol (LDP) and is used by the receiving Label Switch Router (LSR) to determine the next hop on the LSP. The LSR removes the MPLS label from the header and replaces it with a new label before the packet is forwarded to the next LSR in the LSP.

In interface configuration mode, this command enables MPLS encapsulation for IPv6 on the interface. MPLS IPv6 interface configuration requires that MPLS encapsulation also be configured in global router command mode.

The "no" form of this command disables IPv6 routing MPLS encapsulation for the command mode context.

Examples

This example shows how to enable IPv6 MPLS encapsulation with a transport address of **2001::5**:

```
S Chassis(su)->configure
S Chassis(su-config)->mpls ipv6 2001::5
S Chassis(su-config)->
```

mpls ldp-lsr-id

Use this command to configure a unique LDP Label Switch Router (LSR) ID for the router.

Syntax

mpls ldp-lsr-id *lsr-id*

no mpls ldp-lsr-id *lsr-id*

Parameters

lsr-id	Specifies the unique LSR ID for the router in the format A.B.C.D.

Defaults

In an IPv4 system, the LSR ID defaults to the highest IPv4 address associated with a router interface. Loopback interfaces have precedence over VLAN interfaces. In an IPv6 system, the LSR ID is explicitly configured when enabling MPLS using "mpls ipv6" on page 58-2.

Mode

Global router configuration mode.

Usage

This command configures a network wide unique LSR ID for the router. In an IPv4 network, the specified or default LSR ID can also be used as the LDP transport address for LDP peer discovery. In an IPv6 network, the LSR ID must be explicitly configured using this command and the configured LSR ID can not be used as the LDP transport address. In an IPv6 network, the LDP transport address is configured when enabling IPv6 MPLS encapsulation using "mpls ipv6" on page 58-2.

The "no" form of this command deletes the explicit LSR ID for the router.

Examples

This example shows how to configure 110.10.10.5 as the LSR ID and LDP transport address for the global router:

```
S Chassis(su)->configure
S Chassis(su-config)->mpls ldp-lsr-id 110.10.10.5
S Chassis(su-config)->
```

This example shows how to configure 110.10.10.10 as the LSR ID for the global router:

```
S Chassis(su)->configure
S Chassis(su-config)->mpls ldp-lsr-id 110.10.10.10
S Chassis(su-config)->
```

mpls label-protocol-ldp

Use this command to enable LDP as the label distribution protocol.

Syntax

```
mpls label-protocol-ldp {ipv4 | ipv6}
no mpls label-protocol-ldp {ipv4 | ipv6}
```

Parameters

ipv4	Specifies IPv4 as the network address type.
ipv6	Specifies IPv6 as the network address type.

Defaults

The MPLS label distribution protocol is disabled by default.

Mode

Global router or named VRF global configuration mode.

Usage

Specify the IPv4 address type if LDP will be used in an IPv4 network. In an IPv4 network, the related LSR ID is automatically set to the default value. To explicitly set an LSR ID for an IPv4 network use "mpls ldp-lsr-id" on page 58-3. Specify the IPv6 address type if LDP will be used in

an IPv6 network. In an IPv6 network, the related LSR ID must be explicitly set using "mpls ldp-lsr-id" on page 58-3.

The "no" form of this command disables the LDP MPLS label distribution protocol.

Examples

This example shows how to enable LDP MPLS label distribution for an IPv4 network on the VRF **vpnA**:

```
S Chassis(rw)->router vpnA
S Chassis(su-vpnA)->configure
S Chassis(su-vpnA-config)->mpls label-protocol-ldp ipv4
S Chassis(su-vpnA-config)->
```

mpls ldp-label-allocate

Use this command to configure LDP label allocation filtering.

Syntax

mpls ldp-label-allocate {**bgp-routes** | **host-routes**}

no mpls ldp-label-allocate {**bgp-routes** | **host-routes**}

Parameters

bgp-routes	Specifies that LDP will allocate labels for BGP routes.
host-routes	Specifies that LDP will allocate labels for host routes only.

Defaults

The MPLS LDP allocates labels for all routes except BGP.

Mode

Global router or named VRF global configuration mode.

Usage

The "no" form of this command to set LDP label allocation to the default of all routes except BGP.

For a modification of the LDP label allocation configuration to take affect, the MPLS/LDP session must be reset. Use the **no mpls ip** command followed by the **mpls ip** command to reset the MPLS session. Use the **mpls label-protocol-ldp** command to re-enable the LDP session.

Examples

This example shows how to set the MPLS LDP label allocation filter to include BGP routes for VRF **vpnA**:

```
S Chassis(rw)->router vpnA
S Chassis(su-vpnA)->configure
S Chassis(su-vpnA-config)->mpls ldp-label-allocation bgp-routes
S Chassis(su-vpnA-config)->
```

This example shows how to disable MPLS LDP label allocation filter for VRF **vpnA** and reset the MPLS/LDP session:

```
S Chassis(rw)->router vpnA
S Chassis(su-vpnA)->configure
S Chassis(su-vpnA-config)->no mpls ldp-label-allocation
S Chassis(su-vpnA-config)->no mpls ip
S Chassis(su-vpnA-config)->mpls ip
S Chassis(su-vpnA-config)->mpls label-protocol-ldp ipv4
S Chassis(su-config)->
```

mpls ldp-label-retention-mode

Use this command to set the LDP label retention scheme.

Syntax

mpls ldp-label-retention-mode {**liberal** | **conservative**}

no mpls ldp-label-retention-mode {**liberal** | **conservative**}

Parameters

liberal	Specifies that all label mappings advertised by any peer will be kept, regardless of whether the originator is a next-hop peer or not.
conservatived	Specifies that label mappings are only retained if they will be used to explicitly forward packets to their next hop.

Defaults

The MPLS LDP label retention scheme default is liberal.

Mode

Global router or named VRF global configuration mode.

Usage

The “no” form of this command resets the MPLS LDP label retention scheme to the default value of liberal.

Examples

This example shows how to set the MPLS LDP label retention scheme to conservative for VRF **vpnA**:

```
S Chassis(rw)->router vpnA
S Chassis(su-vpnA)->configure
S Chassis(su-vpnA-config)->mpls ldp-label-retention-mode conservative
S Chassis(su-vpnA-config)->
```

mpls ip propagate-ttl

Use this command to enable the propagation of TTL from IPv4 and IPv6 headers to the MPLS label.

Syntax

```
mpls ip propagate-ttl [forwarded | local]
no mpls ip propagate-ttl [forwarded | local]
```

Parameters

propagate-ttl	(Optional) Specifies that TTL from IP/IPv6 header to MPLS label should be propagated.
forwarded	(Optional) Specifies that TTL should be propagated only for forwarded packets.
local	(Optional) Specifies that TTL should be propagated only for local packets.

Defaults

TTL from the IPv4 and IPv6 headers is propagated to the MPLS label.

Mode

Global router or named VRF global configuration mode configuration mode.

Usage

The “no” form of this command disables propagation of TTL from the IPv4 and IPv6 headers to the MPLS label.

A change in the MPLS TTL configuration requires a reset of the MPLS/LDP session. Use the **no mpls ip** command followed by the **mpls ip** command to reset the MPLS session. Use the **mpls label-protocol-ldp** command to re-enable the LDP session.

Examples

This example shows how to disable propagation of the IPv4 and IPv6 header TTL to the MPLS label and reset the MPLS/LDP session:

```
S Chassis(rw)->configure
S Chassis(su-config)->no mpls ip propagate-ttl
S Chassis(su-config)->no mpls ip
S Chassis(su-config)->mpls ip
S Chassis(su-config)->mpls label-protocol-ldp ipv4
S Chassis(su-config)->
```

mpls label mode

Use this command to configure how MPLS labels are assigned.

Syntax

```
mpls label mode {per-prefix | per-vrf}
```

```
no mpls label mode {per-prefix | per-vrf}
```

Parameters

per-prefix	Specifies that MPLS allocates a unique label for each prefix route in the routing table.
per-vrf	Specifies that MPLS allocates a single label for the named VRF (default).

Defaults

MPLS allocates a single label for the VRF.

Mode

A named VRF global configuration mode.

Usage

The per-prefix option is not supported when the core network is GRE.

When the MPLS label mode is set to per-vrf, all prefix routes within the routing table for the VRF context use the same label.

The “no” form of this command resets the MPLS label mode to a single label for each VRF.

Examples

This example shows how to set the MPLS label mode to per-prefix for VRF vpnA:

```
S Chassis(rw)->router vpnA
S Chassis(su-vpnA)->configure
S Chassis(su-vpnA-config)->mpls label mode per-prefix
S Chassis(su-vpnA-config)->
```

This example shows how to set the MPLS label mode so that all prefix routes within the routing table for VRF vpnA use the same label:

```
S Chassis(rw)->router vpnA
S Chassis(su-vpnA)->configure
S Chassis(su-vpnA-config)->mpls label mode per-VRF
S Chassis(su-vpnA-config)->
```

rd

Use this command to assign a route distinguisher (RD) to a VRF.

Syntax

rd {*asn*:*num* | *ipv4Addr*:*num*}

Parameters

asn:*num*	Specifies a Type 0 or Type 2 route distinguisher. Valid values are **1** - **65535**:**1** - **4294967295**.
ipv4Addr:*num*	Specifies a Type 1 route distinguisher. Valid values are *IPv4_Address*:**1** - **65535**.

Defaults

None.

Mode

A named VRF global configuration mode.

Usage

The route distinguisher is a 64 bit identifier attribute that gets prepended to the user IPv4 or IPv6 address and makes the IP address globally unique across the VPN network and within the BGP routing table. The RD is a required component when defining a L3 VPN, and its significance is local to the device. Assign one RD to each VRF that will use the BGP VPN. The BGP VPN-IPv4 or VPN-IPv6 address families are defined by combining the RD, user IP address, and the MPLS Label (see "mpls label mode" on page 58-7 for label mode configuration).

RDs must be unique for each VRF on a device. The same RD can be used on multiple devices belonging to the VPN. Combining the VRF RD with the user IP address, even when that IP address is an unregistered private address, serves to uniquely identify the user.

Three data fields make up the eight bytes (64-bits) of the RD attribute:

- **RD Type** – A non-configurable two-byte field that identifies the format used by the administrator and assigned fields as the packet transits the network. Valid values are 0, 1, or 2.
- **Administrator Field** – A two- or four-byte field (depending upon the RD type) allowing a network administrator to uniquely identify the VRF as a:
  - Two-byte autonomous system number (RD type 0). Valid values are **1** - **65535**.
  - Four-byte IPv4 address (RD type 1)
  - Four-byte autonomous system number (RD type 2). Valid values are **65536** - **4294967295**.
- **Assigned Number Field** – A two- or four-byte field (depending upon the RD type) assigned by the provider network:
  - Four-byte autonomous system number (RD type 0). Valid values are **1** - **4294967295**.
  - Two-byte autonomous system number (RD types 1 and 2). Valid values are **1** - **65535**.

It is recommended that non-private autonomous system numbers be used when configuring the RD. If the BGP autonomous system number is a private AS between 64512-65534, use RD type 1 specifying an IPv4 address.

Non-private autonomous system numbers are assigned by IANA to service providers. Non-private autonomous system numbers use either a two-byte or four-byte number in the following formats:

- Type 0 – **1** - **65535:1** - **4294967295**
- Type 1 – *IPv4-address*:**1** - **65535**
- Type 2 – **65536** - **4294967295:1** - **65535**

Examples

This example shows how to assign a type 0 route distinguisher **1:52** to VRF **vpnA**:

```
S Chassis(rw)->router vpnA
S Chassis(su-vpnA)->configure
S Chassis(su-vpnA-config)->rd 1:52
S Chassis(su-vpnA-config)->
```

This example shows how to assign a type 1 route distinguisher **10.10.100.1:53** to VRF **vpnB**:

```
S Chassis(rw)->router vpnB
S Chassis(su-vpnB)->configure
S Chassis(su-vpnB-config)->rd 10.10.100.1:53
S Chassis(su-vpnB-config)->
```

route-target

Use this command to identify routes that will be imported and exported by the VPN VRF.

Syntax

route-target {**import** | **export** | **both**} *oui*:*num*

Parameters

import	Specifies that this VRF will import routes tagged with the specified route target identifier.
export	Specifies that this VRF will tag routes that it exports with the specified route target identifier.
both	Specifies that this VRF will import routes tagged with the specified route target and will tag routes that it exports with the specified route target identifier.
oui:*number*	Specifies a route target identifier. The route target identifier supports two formats. Valid values are: • **1** - **65535**:**1** - **4294967295** • *valid_IPv4_Address*:**1** - **65535**

Defaults

None.

Mode

A named VRF global configuration mode.

Usage

The route target determines which routes are inserted into a VRF. A VRF can be configured for one or more route targets for import, export, or both. At least one configured route target for import or export is a required component when defining a L3 VPN VRF. All routes exported by the VRF are tagged with each route target identifier configured for export on the VRF. Only VRFs configured to import routes tagged with the route target identifier will import the route. This allows you to configure one VRF to export multiple route targets and another VRF to be configured to import only a subset of the routes the first VRF exports.

- An **export** route target – BGP advertises VPN-IPv4 and VPN-IPv6 address family prefixes, along with extended community names and tags the advertisement with the route target identifier. A redistribute rule must be created under the appropriate IPv4 or IPv6 address family in the BGP global configuration mode for each routing protocol, static, or connected route to be exported. See "bgp address-family" on page 72-4 for the BGP global configuration mode address family command details

- An **import** route target – Import route targets specify that this VRF will import any BGP advertised routes that are tagged with the specified route target identifier, updating the VRF routing and forwarding tables with the advertised VPN-IPv4 or VPN-IPv6 addresses. When the VRF BGP router receives an update, it examines the extended community names for each set of prefixes. If an update matches a configured import route target for this named VRF, BGP installs the matching set of prefixes into the routing and forwarding tables as BGP learned routes, after removing the 64-bit RD.
- **Both** an import and export route target – This VRF will both import routing updates that match configured import route targets and export VPN address family prefixes tagged with the specified route target(s).

Examples

This example shows how to export VPN address family prefixes and tag them with route target **1:1000**:

```
S Chassis(su)->router vpnA
S Chassis(su-vpnA)->configure
S Chassis(su-vpnA-config)->route-target export 1:1000
S Chassis(su-vpnA-config)->
```

This example shows how to both import BGP VPN updates tagged with the route target **10.10.176.25:1000** and tag any BGP VPN advertisements with the route target **10.10.176.25:1000**:

```
S Chassis(su)->router vpnA
S Chassis(su-vpnA)->configure
S Chassis(su-vpnA-config)->route-target both 10.10.176.25:1000
S Chassis(su-vpnA-config)->
```

vpn id

Use this command to configure the VPN identifier.

Syntax

vpn id *oui*:*vpn-index*

Parameters

oui	Specifies the VPN authority. Valid values are **1** - **16777215**.
vpn-index	Specifies a particular VPN belonging to the VPN authority. Valid values are **1** - **4294967295**.

Defaults

None.

Mode

A named VRF global configuration mode.

Usage

The VPN ID is the virtual private network identifier as defined in RFC 2685. It defines both the owner of the VPN (OUI), referred to as the VPN authority, and the specific VPN owned by the VPN authority (VPN Index). These two values are separated by a colon (**:**). The VPN identifier is

used by other network features to identify the VPN to which a client packet flow belongs to. For example, a VPN ID can be sent by a DHCP relay agent to a DHCP server as part of the relay agent information options used by the server to assign the correct lease to a DHCP client.

Examples

This example shows how to configure the VPN ID for VPN **1** belonging to the **1001** VPN authority:

```
S Chassis(su)->router vpnA
S Chassis(su-vpnA)->configure
S Chassis(su-vpnA-config)->vpn id 1001:1
S Chassis(su-vpnA-config)->
```

show mpls interface

Use this command to display information related to the specified or all MPLS interfaces.

Syntax

show mpls interface [*interface-name*] [**detail**]

Parameters

interface-name	(Optional) Specifies the MPLS interface or a range of MPLS interfaces to display.
detail	(Optional) Displays a detailed level of MPLS interface information.

Defaults

- If *interface-name* is not specified, information for all MPLS interfaces displays.
- If **detail** is not specified, a standard level of information for all MPLS interfaces displays.

Mode

All command modes.

Examples

This example shows how to display a standard level of information for all MPLS interfaces:

```
S Chassis(rw)->show mpls interface

Interface               LDP        Tunnel    Operational
------------            --------   ------    -----------
vlan.0.201              Yes        Yes       No
vlan.0.601              Yes        Yes       Yes
S Chassis(rw)->
```

This example shows how to display a detailed level of information for MPLS interface **vlan.0.201**:

```
S Chassis(rw)->show mpls interface vlan.0.201 detail
 vlan.0.201 is Operationally down, Administratively down
   LDP labeling enabled
   LSP Tunnel labeling enabled
```

```
   BGP labeling enabled
   MPLS operational
S Chassis(rw)->
```

show mpls forwarding-table

Use this command to display the contents of the MPLS Label Forwarding Information Base (LFIB).

Syntax

show mpls forwarding-table [*ip-address/length*] [*interface-name*] [**label** *label*] [**detail**]

Parameters

ip-address/length	(Optional) Specifies the IPv4 or IPv6 address and length of the LFIB entries to display.
interface-name	(Optional) Specifies the outgoing interface of the LFIB entries to display.
label *label*	(Optional) Specify the local or outgoing label to display. Valid values are 1 – 1048576.
detail	(Optional) Specifies that a detailed level of information should display.

Defaults

If no options are specified, a one-line summary level of information displays for each LFIB entry.

Mode

All command modes.

Examples

This example shows how to display a summary level of information for all LFIB entries:

```
S Chassis(rw)->show mpls forwarding-table

Local  Outgoing    Prefix              Outgoing   Next Hop
tag    tag or VC   or Tunnel Id        interface
57     0           173.6.1.1/32
78     77          192.17.170.80/32    vlan.0.46  192.18.170.17
80     53          192.17.170.3/32     vlan.0.36  192.17.170.41
81     51          192.17.170.32/29    vlan.0.36  192.17.170.41
82     45          173.101.173.0/24    vlan.0.610 192.17.170.49
83     48          192.17.170.10/32    vlan.0.610 192.17.170.49
84     30          173.4.1.0/24        vlan.0.36  192.17.170.41
85     31          173.4.2.0/24        vlan.0.36  192.17.170.41
86     32          173.4.3.0/24        vlan.0.36  192.17.170.41
...
171    185         173.7.9.0/24        vlan.0.610 192.17.170.49
171    134         173.7.9.0/24        vlan.0.26  192.17.170.65
173    186         173.7.10.0/24       vlan.0.610 192.17.170.49
```

```
173    135         173.7.10.0/24          vlan.0.26  192.17.170.65
S Chassis(rw)->
```

show mpls ldp-parameters

Use this command to display all MPLS LDP parameter information.

Syntax

show mpls ldp-parameters

Parameters

None.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to display current MPLS LDP parameter information:

```
S Chassis(rw)->show mpls ldp-parameters

Global Settings
 LDP LSR id: 192.17.170.10
 Protocol version: 1
 Max PDU length: 4096
 Label distribution method: Downstream Unsolicited
 Label retention mode: Liberal
 Hello hold timer: 15s
 Label control mode: Ordered

Graceful Restart Settings:
 Adjacency down hold time: 3s
 Restart capable: No
 Local reconnect time: 60s
 Local recovery time: 180s
 Max peer reconnect time: 180s
 Max peer recovery time: 240s
S Chassis(rw)->
```

show mpls ip-bindings

Use this command to display .

Syntax

show mpls ip-bindings [*ip-address*] [**detail**] [**local-label**] [**local**]

Parameters

ip-address	(Optional) Displays IP bindings for the specified address.
detail	(Optional) Displays a detailed level of IP binding information.
local-label	(Optional) Displays match locally assigned label values.
local	(Optional) Displays only locally assigned labels.

Defaults

If no option is specified, a summary level of information is displayed for all MPLS IP bindings.

Mode

All command modes.

Examples

This example shows how to display IP bindings for IP address **172.7.10.0/24**:

```
S Chassis(rw)-> show mpls ip-binding 173.7.10.0/24
  173.7.10.0/24
                in label:               173
                out label:              186           lsr: 192.17.170.3
  173.7.10.0/24
                in label:               173
                out label:              135           lsr: 192.17.170.3

S Chassis(rw)->
```

show mpls ldp-neighbor

Use this command to display .

Syntax

show mpls ldp-neighbor [*ip-address*]

Parameters

ip-address	(Optional) Specifies the neighbor IPv4 or IPv6 address to display.

Defaults

If *ip-address* is not specified, all neighbors display.

Mode

All command modes.

Examples

This example shows how to display information for all MPLS LDP neighbors:

```
S Chassis(rw)->show mpls ldp-neighbor

Peer ID       Peer Transport Addr   Session Role   State
---------     -------------------   ------------   -----
192.17.170.17    192.17.170.17        Active         Up
192.17.170.3     192.17.170.3         Active         Up
192.18.170.4     192.18.170.4         Active         Up
192.17.170.10    192.17.170.10        Active         Up
S Chassis(rw)->
```

BGP L3 VPN Commands

For information about...	Refer to page...
address-family	58-17
enable	58-19
neighbor activate	58-19
show ip bgp vpn	58-20
show ip bgp vpn vrf	58-23
show ipv6 bgp vpn	58-26
show ipv6 bgp vpn vrf	58-28

address-family

Use this command to enter the BGP IPv4 or IPv6 L3 VPN address family configuration mode.

Syntax

```
address-family {vpnv4 | vpnv6}
```

Parameters

vpnv4	Enters the BGP IPv4 L3 VPN address family configuration mode.
vpnv6	Enters the BGP IPv6 L3 VPN address family configuration mode.

Defaults

None.

Mode

BGP Router Configuration.

Usage

Within the IPv4 or IPv6 L3 VPN address family mode, you can enable the L3 VPN address family using "enable" on page 58-19.

IPv4 unicast BGP peers are activated by default in a non-L3 VPN context. BGP peers within either the IPv4 or IPv6 L3 VPN address family must be administratively activated using "neighbor activate" on page 58-19.

BGP routes associated with the neighbor must be redistributed to the customer edge router on the VRF that will use the L3 VPN.

Note: To redistribute routes assoicated with the neighbor, enter the BGP global configuration address family using "bgp address-family" on page 72-4, specifying the VRF option, and use the appropriate **redistribute** command.

Examples

This example shows how to:

- Configure BGP neighbor 159.1.1.50 and set the neighbor source to the BGP router ID

- Enter the L3 VPN IPv4 address family
- Enable the L3 VPN IPv4 address family
- Activate the peer for the IPv4 L3 VPN address family
- Enter the BGP global configuration IPv4 address family for the **vr1** VRF
- Redistribute the IPv4 static routes for VRF vr1

```
S Chassis(rw)->
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->neighbor 159.1.1.50 remote-as 65151
S Chassis(su-config-bgp)->neighbor 159.1.1.50 update-source 159.1.1.9
S Chassis(su-config-bgp)->address-family vpnv4
S Chassis(su-config-bgp-af-vpn)->enable
S Chassis(su-config-bgp-af-vpn)->159.1.1.50 neighbor activate
S Chassis(su-config-bgp-af-vpn)->exit
S Chassis(su-config-bgp)->address-family ipv4 vrf vr1
S Chassis(su-config-bgp-af-vrf)->redistribute static
S Chassis(su-config-bgp-af-vrf)->exit
S Chassis(su-config-bgp)->
```

This example shows how to:

- Configure BGP neighbor 4000:1::5 and set the neighbor source to the BGP router ID
- Enter the L3 VPN IPv6 address family
- Enable the L3 VPN IPv6 address family
- Activate the peer for the IPv6 L3 VPN address family
- Enter the BGP global configuration IPv6 address family for the **vr1** VRF
- Redistribute the IPv6 static routes for VRF vr1

```
S Chassis(rw)->
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 4000:1::a
S Chassis(su-config-bgp)->neighbor 4000:1::5 remote-as 65151
S Chassis(su-config-bgp)->neighbor 4000:1::5 update-source 4000:1::a
S Chassis(su-config-bgp)->address-family vpnv6
S Chassis(su-config-bgp-af-vpn)->enable
S Chassis(su-config-bgp-af-vpn)->4000:1::5 neighbor activate
S Chassis(su-config-bgp-af-vpn)->exit
S Chassis(su-config-bgp)->address-family ipv6 vrf vr1
S Chassis(su-config-bgp-af-vrf)->redistribute static
S Chassis(su-config-bgp-af-vrf)->exit
S Chassis(su-config-bgp)->exit
S Chassis(rw-config)->
```

enable

This command enables the current L3 VPN address family context.

Syntax

enable

Parameters

None.

Defaults

BGP L3 VPN IPv4 and IPv6 address families are disabled by default.

Mode

BGP L3 VPN IPv4 or IPv6 Address Family Configuration

Examples

The following example enables the BGP L3 VPN IPv4 address family:

```
S Chassis(su-config-bgp)->address-family vpnv4
S Chassis(su-config-bgp-af-vpn)->enable
S Chassis(su-config-bgp-af-vpn)->
```

The following example enables the BGP L3 VPN IPv6 address family:

```
S Chassis(su-config-bgp)->address-family vpnv6
S Chassis(su-config-bgp-af-vpn)->enable
S Chassis(su-config-bgp-af-vpn)->
```

neighbor activate

This command activates the specified BGP peer for the current L3 VPN address family context.

Syntax

neighbor *ip-address* **activate**

no neighbor *ip-address* **activate**

Parameters

ip-address	Specifies a BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.

Defaults

None.

Mode

BGP L3 VPN IPv4 or IPv6 Address Family Configuration.

Usage

The **neighbor activate** command must be applied to any IPv6 peers, but does not need to be applied to an IPv4 peer.

The **no neighbor activate** command disables activation of the specified BGP neighbor for the current address family context.

Example

The following example activates neighbor **fe80::21f:45ff:fe3d:21be** within the IPv6 unicast address family context:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->neighbor fe80::21f:45ff:fe3d:21be remote-as 5
S Chassis(su-config-bgp)->address-family ipv6 unicast
S Chassis(su-config-bgp-af)->neighbor fe80::21f:45ff:fe3d:21be activate
```

show ip bgp vpn

This command displays information about IPv4 VPN BGP routes installed in the BGP routing information base (RIB).

Syntax

show ip bgp vpn {**all** | **rd** {*asn*:*num* | *ipv4Addr*:*num*}} [**labels**] [**peer** *ip-addr*] {**received-routes** | **advertised-routes**}] [*prefix/length* [**longer-prefixes**] [**detail**]]

Parameters

all	Display all BGP VPN BGP routing table information.
rd *asn*:*num* | *ipv4Addr*:*num*	Display BGP VPN BGP routing table information for the specified route distinguisher.
labels	(Optional) Displays incoming and outgoing BGP labels for each prefix in the routing table.
peer *ip-addr*	(Optional) Specifies the IPv4 peer for route information display.
received-routes	Displays received routes from the peer *after* import policies are applied matching prefix and mask (local-rib).
advertised-routes	Displays all routes advertised to the peer after export policies have been applied that match a prefix and mask (rib-out).
prefix/length	Displays specified BGP route destination.
longer-prefixes	(Optional) Specifies that only routes exactly matching the specified IP address will display.
detail	(Optional) Displays a detailed level of information including: • Route community attributes • Route Extended Community attributes • Route Target • Route Flap Dampening table name

Defaults

- If the label option is not specified, incoming and outgoing BGP labels are not displayed.
- If a peer IP address, route, or the longer prefix option is not specified, information is displayed for all peers and routes.
- If **detail** is not specified, a standard level of route information displays.

Mode

All command modes.

Usage

To display IPv4 VPN BGP routing table information for a specific VRF see "show ip bgp vpn vrf" on page 58-23.

Example

The following example displays IPv4 BGP VPN information for all BGP VPN routes installed in the BGP RIB.

```
S Chassis(rw)->show ip bgp vpn all
Route status codes: > - active

   Network                Next Hop            Rib MED Local-Pref Origin AS Path
Route Distinguisher: 1:3  (default for vrf vpnC)
>   1.0.0.12/32             1.0.0.1              U   0      100    IGP
>   1.0.0.13/32             1.0.0.1              U   0      100    IGP
>   1.0.0.37/32             1.0.0.33             U   0      100    IGP
>   1.0.0.38/32             1.0.0.33             U   0      100    IGP
>   10.0.0.0/8              1.0.0.1              U   0      100    IGP     2
>   10.1.128.0/17           1.0.0.1              U   0      100    IGP     2
...
Route Distinguisher: 1:4  (default for vrf vpnD)
>   1.0.0.15/32             1.0.0.1              U   0      100    IGP
>   1.0.0.36/32             1.0.0.33             U   0      100    IGP
    52.7.0.0/24             1.0.0.33             U   0      100    IGP     4
...
S Chassis(rw)->
```

The following example displays BGP VPN routes for route distinguisher **1:3**:

```
S Chassis(rw)->show ip bgp vpn rd 1:3
Route status codes: > - active

   Network                Next Hop            Rib MED Local-Pref Origin AS Path
Route Distinguisher: 1:3  (default for vrf vpnC)
>   1.0.0.12/32             1.0.0.1              U   0      100    IGP
>   1.0.0.13/32             1.0.0.1              U   0      100    IGP
>   10.0.0.0/8              1.0.0.1              U   0      100    IGP     2
>   10.1.128.0/17           1.0.0.1              U   0      100    IGP     2
```

```
>   52.5.0.0/24             1.0.0.1               U   0      100    IGP
>   134.141.0.0/16          1.0.0.1               U   0      100    IGP      2
>   172.5.1.0/24            1.0.0.1               U   0      100    IGP      2
>   172.5.4.0/24            1.0.0.1               U   0      100    IGP      2
>   192.168.61.0/24         1.0.0.1               U   0      100    IGP      2
>   199.0.0.0/24            1.0.0.1               U   0      100    IGP      2
S Chassis(rw)->
```

The following example displays a detail level of information for the prefix 172.1.1.0/24 BGP VPN route for route distinguisher **1:55**:

```
S Chassis(rw)->show ip bgp vpn rd 1:55 172.1.1.0/24 detail
Route status codes: > - active

   Network                Next Hop            Rib MED Local-Pref Origin AS Path
Route Distinguisher: 1:55  (default for vrf vpnB)
>   172.1.1.0/24             1.0.0.1               U   0      100    IGP

Community attributes in route:

Extended Community attributes in route:
Route Target: 1:55 (0x0002000100000037)
Route Target: 2:10 (0x000200020000000A)

Route Flap Dampening configuration file name: None
```

Table 58-1 table describes the fields that appear in the **show ip bgp vpn** query.

Table 58-1 show ip bgp vpn Output Details

Output...	What it displays...
Route status codes	A greater than symbol “>” specifies the active or used route. If no symbol displays, the route is not being used for the displayed context.
Network	Specifies the network this route is on.
Next Hop	Specifies the IP address of the nearest gateway used to reach the EBGP peer
Rib	Specifies whether the route is installed in the unicast or multicast RIB
MED	Specifies the MED value for the route.
Local-Pref	Specifies the Local Preference value for the route.
Origin	Specifies whether the origin of the route is an internal or external protocol.
AS Path	Specifies the route’s AS Path.
Route Distinguisher	Specifies the route distinguisher associated with the next series of routes.
Community attributes in route	Specifies any BGP community attributes for the specified route.

Table 58-1 show ip bgp vpn Output Details

Output...	What it displays...
Extended Community attributes in route	Specifies any BGP extended community attributes for the specified route.
Route Flap Dampening configuration file name	Specifies if there is a route flap dampening configuration file associated with the specified route.

show ip bgp vpn vrf

This command displays information about IPv4 VPN BGP routes installed in the BGP routing information base (RIB) for the specified VRF.

Syntax

```
show ip bgp vpn vrf vrf-name [labels] [peer ip-addr {received-routes |
advertised-routes}] [prefix/length [longer-prefixes] [detail]]
```

Parameters

vrf-name	Displays the named VRF.
labels	(Optional) Displays incoming and outgoing BGP labels for each prefix in the routing table.
peer *ip-addr*	(Optional) Specifies the IPv4 peer route information to display.
received-routes	Displays received routes from the peer *after* import policies are applied matching prefix and mask (local-rib).
advertised-routes	Displays all routes advertised to the peer after export policies have been applied that match a prefix and mask (rib-out).
prefix/length	Displays specified BGP route destination.
longer-prefixes	(Optional) Specifies that only routes exactly matching the specified IP address will display.
detail	(Optional) Displays a detailed level of information including: • Route community attributes • Route Extended Community attributes • Route Target • Route Flap Dampening table name
ip-prefix/mask	(Optional) Specifies an IP prefix and mask for BGP route display.
longer-prefixes	(Optional) Specifies that only routes matching the specified IP address or IP prefix/length will display.
detail	(Optional) Displays a detailed level of information including: • Route community attributes • Route Extended Community attributes • Route Target • Route Flap Dampening table name • Flap related counters

Defaults

- If the label option is not specified, incoming and outgoing BGP labels are not displayed.
- If a peer IP address, route, or the longer prefix option is not specified, information is displayed for all peers and routes.
- If **detail** is not specified, a standard level of route information displays.

Mode

All command modes.

Example

The following example displays all BGP VPN routes for VRF **Nike**.

```
S Chassis(rw)->show ip bgp vpn vrf Nike
Route status codes: > - active

   Network              Next Hop           Rib MED Local-Pref Origin Weight
AS Path
Route Distinguisher: 192.16.168.12:1  (default for vrf Nike)
>   140.128.12.0/24         192.17.170.10        U   2     100     IGP    0
>   140.128.13.0/27         192.17.170.10        U   12    100     IGP    0
>   140.128.13.32/27        192.17.170.10        U   12    100     IGP    0
>   140.128.13.64/27        192.17.170.10        U   12    100     IGP    0
>   140.128.13.96/27        192.17.170.10        U   12    100     IGP    0
>   140.128.13.128/27       192.17.170.10        U   2     100     IGP    0
>   140.128.13.160/27       192.17.170.10        U   2     100     IGP    0
>   140.128.13.192/27       192.17.170.10        U   2     100     IGP    0
>   140.128.13.224/27       192.17.170.10        U   2     100     IGP    0
>   192.16.168.13/32        192.17.170.10        U   21    100     IGP    0
>    192.16.168.112/29        192.17.170.10         U   11     100     IGP    0
S Chassis(rw)->
```

The following example displays BGP VPN route labels for VRF vpnA:

```
S Chassis(rw)->show ip bgp vpn vrf vpnA labels
Route status codes: > - active

    Network                  Next Hop              In Label/Out Label
Route Distinguisher: 1:52  (default for vrf vpnA)
>   1.0.0.3/32               1.0.0.1                16/No Label
>   1.0.0.5/32               1.0.0.1                16/No Label
>   10.0.0.0/8               1.0.0.1                16/No Label
>   52.1.0.0/24              1.0.0.1                16/No Label
>   53.2.1.0/24              1.0.0.1                16/No Label
>   134.141.0.0/16           1.0.0.1                16/No Label
>   172.1.1.0/24             1.0.0.1                16/No Label
>   172.1.2.0/24             1.0.0.1                16/No Label
>   172.1.3.0/24             1.0.0.1                16/No Label
```

```
...
S Chassis(rw)->
```

The following example displays a detailed level of information for IPv4 BGP VPN VRF **vpnA** route **53.2.1.0/24**:

```
S Chassis(rw)->show ip bgp vpn vrf vpnA 53.2.1.0/24 detail
Route status codes: > - active

    Network                 Next Hop             Rib MED Local-Pref Origin AS Path
Route Distinguisher: 1:52  (default for vrf vpnA)
>   53.2.1.0/24              1.0.0.1               U   0      100    IGP

Community attributes in route:

Extended Community attributes in route:
Route Target: 1:52 (0x0002000100000034)
Route Target: 2:52 (0x0002000200000034)

Route Flap Dampening configuration file name: None
S Chassis(rw)->
```

Table 58-2 table describes the fields that appear in the **show ip bgp vpn vrf** query.

Table 58-2 show ip bgp vpn vrf Output Details

Output...	What it displays...
Route status codes	A greater than symbol “>” specifies the active or used route. If no symbol displays, the route is not being used for the displayed context.
Network	Specifies the network this route is on.
Next Hop	Specifies the IP address of the nearest gateway used to reach the EBGP peer.
Rib	Specifies whether the route is installed in the unicast or multicast RIB.
MED	Specifies the MED value for the route.
Local-Pref	Specifies the Local Preference value for the route.
Origin	Specifies whether the origin of the route is an internal or external protocol.
AS Path	Specifies the route’s AS Path.
Route Distinguisher	Specifies the route distinguisher associated with the next series of routes.
In Label/Out Label	Incoming and outgoing BGP labels for the specified network and next hop.
Community attributes in route	Specifies any community attributes for this route.
Extended Community attributes in route	Specifies any extended community attributes for this route.

Table 58-2 show ip bgp vpn vrf Output Details

Output...	What it displays...
Route Flap Dampening configuration file name	Specifies the name of the route flap dampening configuration file or “None” if no file exists.

show ipv6 bgp vpn

This command displays information about IPv6 VPN BGP routes installed in the BGP routing information base (RIB).

Syntax

```
show ipv6 bgp vpn {all | rd {asn:num | ipv4Addr:num}} [labels] [peer ip-addr
{received-routes | advertised-routes}] [prefix/length [longer-prefixes] [detail]]
```

Parameters

all	Display all IPv6 BGP VPN BGP routing table information.
rd *asn*:*num* | *ipv4Addr*:*num*	Display IPv6 BGP VPN BGP routing table information for the specified route distinguisher.
labels	(Optional) Displays incoming and outgoing BGP labels for each NLRI prefix.
peer *ip-addr*	(Optional) Specifies the IPv6 peer to display route information for.
received-routes	Displays received routes from the peer *after* import policies are applied matching prefix and mask (local-rib).
advertised-routes	Displays all routes advertised to the peer after export policies have been applied that match a prefix and mask (rib-out).
prefix/length	Displays specified BGP route destination.
longer-prefixes	(Optional) Specifies that only routes exactly matching the specified IP address will display.
detail	(Optional) Displays a detailed level of information including: • Route community attributes • Route Extended Community attributes • Route Target • Route Flap Dampening table name

Defaults

- If the label option is not specified, incoming and outgoing BGP labels are not displayed.
- If a peer IP address, route, or the longer prefix option is not specified, information is displayed for all peers and routes.
- If **detail** is not specified, a standard level of route information displays.

Mode

All command modes.

Usage

To display BGP routing table information for a specific VRF see “show ipv6 bgp vpn vrf” on page 58-28.

Example

The following example displays BGP VPN information for all IPv6 BGP VPN routes installed in the BGP RIB for route distinguisher **1:3**.

```
S Chassis(rw)->show ipv6 bgp vpn rd 1:3
Route status codes: > - active

Route Distinguisher: 1:3  (default for vrf vpnC)

Network: > 172:16:1::/64
Nexthop:        2000::33
Rib MED Local-Pref Origin AS Path
U   0      100    IGP     2

Network: > 525::/64
Nexthop:        ::ffff:1.0.0.1
Rib MED Local-Pref Origin AS Path
U   0      100    IGP

Network: > 1725:1::/64
Nexthop:        ::ffff:1.0.0.1
Rib MED Local-Pref Origin AS Path
U   0      100    IGP     2

...
```

The following example displays a detailed level of IPv6 BGP VPN information for VRF vpnA prefix **172:16:1::/64**.

```
S Chassis(rw)->show ipv6 bgp vpn vrf vpnA 193:166:1::/64 detail
Route status codes: > - active

Route Distinguisher: 1:52  (default for vrf vpnA)

Network: > 193:166:1::/64
Nexthop:        ::ffff:1.0.0.1
Rib MED Local-Pref Origin AS Path
U   0      100    IGP

Community attributes in route:

Extended Community attributes in route:
Route Target: 1:52 (0x0002000100000034)
```

```
Route Target: 2:52 (0x0002000200000034)

Route Flap Dampening configuration file name: None
```

Table 58-1 table describes the fields that appear in the **show ipv6 bgp vpn vrf** query.

Table 58-3 show ipv6 bgp vpn vrf Output Details

Output...	What it displays...
Route status codes	A greater than symbol “>” specifies the active or used route. If no symbol displays, the route is not being used for the displayed context.
Route Distinguisher	Specifies the route distinguisher for the specified VRF.
Network	Specifies the network this route is on.
Next Hop	Specifies the IP address of the nearest gateway used to reach the EBGP peer.
Rib	Specifies whether the route is installed in the unicast or multicast RIB.
MED	Specifies the MED value for the route.
Local-Pref	Specifies the Local Preference value for the route.
Origin	Specifies whether the origin of the route is an internal or external protocol.
AS Path	Specifies the route’s AS Path.
Community attributes in route	Specifies any community attributes for this route.
Extended Community attributes in route	Specifies any extended community attributes for this route.
Route Flap Dampening configuration file name	Specifies the name of the route flap dampening configuration file or “None” if no file exists.

show ipv6 bgp vpn vrf

This command displays information about IPv6 VPN BGP routes installed in the BGP routing information base (RIB) for the specified VRF.

Syntax

```
show ipv6 bgp vpn vrf vrf-name [labels] [peer ip-addr {received-routes | advertised-routes}] [prefix/length [longer-prefixes] [detail]]
```

Parameters

vrf-name	Displays the named VRF.
labels	(Optional) Displays incoming and outgoing BGP labels for each NLRI prefix.
peer *ip-addr*	(Optional) Specifies the IPv6 peer for route information to display.
received-routes	Displays received routes from the peer *after* import policies are applied matching prefix and mask (local-rib).

advertised-routes	Displays all routes advertised to the peer after export policies have been applied that match a prefix and mask (rib-out).
prefix/length	Displays specified BGP route destination.
longer-prefixes	(Optional) Specifies that only routes exactly matching the specified IP address will display.
detail	(Optional) Displays a detailed level of information including: • Route community attributes • Route Extended Community attributes • Route Target • Route Flap Dampening table name

Defaults

- If the label option is not specified, incoming and outgoing BGP labels are not displayed.
- If a peer IP address, route, or the longer prefix option is not specified, information is displayed for all peers and routes.
- If **detail** is not specified, a standard level of route information displays.

Mode

All command modes.

Example

The following example displays all IPv6 BGP VPN routes for VRF **vpnA**.

```
S Chassis(rw)->show ipv6 bgp vpn vrf vpnA
Route status codes: > - active

Route Distinguisher: 1:52  (default for vrf vpnA)

Network: > ::/0
Nexthop:        ::ffff:1.0.0.1
Rib MED Local-Pref Origin AS Path
U   0      100    IGP

Network: > 53:2:1::/64
Nexthop:        ::ffff:1.0.0.1
Rib MED Local-Pref Origin AS Path
U   0      100    IGP
...
S Chassis(rw)->
```

The following example displays BGP VPN IPv6 route labels for VRF vpnA:

```
S Chassis(rw)->show ipv6 bgp vpn vrf vpnA labels
Route status codes: > - active

Route Distinguisher: 1:52  (default for vrf vpnA)
```

```
Network: > ::/0
Nexthop:        ::ffff:1.0.0.1
In Label/Out Label:      16/No Label


S Chassis(rw)->
```

The following example displays a detailed level of information for BGP VPN IPv6 VRF **vpnA** route **192:166:1::/64**:

```
S Chassis(rw)->show ipv6 bgp vpn vrf vpnA 192:166:1::/64 detail
Route status codes: > - active

Route Distinguisher: 1:52  (default for vrf vpnA)

Network: > 192:166:1::/64
Nexthop:        ::ffff:1.0.0.1
Rib MED Local-Pref Origin AS Path
U   0      100    IGP

Community attributes in route:

Extended Community attributes in route:
Route Target: 1:52 (0x0002000100000034)
Route Target: 2:52 (0x0002000200000034)

Route Flap Dampening configuration file name: None
```

Table 58-4 table describes the fields that appear in the **show ipv6 bgp vpn vrf** query.

Table 58-4 show ipv6 bgp vpn vrf Output Details

Output...	What it displays...
Route status codes	A greater than symbol “>” specifies the active or used route. If no symbol displays, the route is not being used for the displayed context.
Network	Specifies the network this route is on.
Next Hop	Specifies the IP address of the nearest gateway used to reach the EBGP peer.
Rib	Specifies whether the route is installed in the unicast or multicast RIB.
MED	Specifies the MED value for the route.
Local-Pref	Specifies the Local Preference value for the route.
Origin	Specifies whether the origin of the route is an internal or external protocol.
AS Path	Specifies the route’s AS Path.
Route Distinguisher	Specifies the route distinguisher associated with the next series of routes.

Table 58-4 show ipv6 bgp vpn vrf Output Details

Output...	What it displays...
In Label/Out Label	Incoming and outgoing BGP labels for the specified network and next hop.
Community attributes in route	Specifies any community attributes for this route.
Extended Community attributes in route	Specifies any extended community attributes for this route.
Route Flap Dampening configuration file name	Specifies the name of the route flap dampening configuration file or “None” if no file exists.

59

ARP Table Commands

This chapter describes the ARP table set of commands and how to use them. For information about configuring ARP, refer to the "IP Routing Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show arp	59-1
set arp	59-3
clear arp	59-4
arp	59-4
arp timeout	59-5
arp retransmit-time	59-6
arp stale-entry-timeout	59-7
arp-nd-proxy-all	59-7
ip gratuitous-arp	59-8
ip gratuitous-arp-learning	59-8
ip proxy-arp	59-9
ip mac-address	59-10
ip multicast-arp-learning	59-11
clear arp-cache	59-11

show arp

Use this command to display the switch's ARP table.

Syntax

show arp [*ip-address*] [**interface** *interface*]

Parameters

ip-address	(Optional) Displays ARP entries associated with the specified IP address.
interface *interface*	(Optional) Display ARP entries associated with the specified interface.

Defaults

If the IP address or interface are not specified, all entries in the ARP cache are displayed.

Mode

All command modes.

Example

This example shows how to display the ARP table:

```
S Chassis(rw)->show arp
FLAGS:    U = Unresolved     S = Static
          L = Local          V = VRRP
          * = Stale          B = Best Guess Interface
          H = Host Interest  2 = Secondary VLAN Entry

IP Address      Hardware Address  Flg Age        Updated Interface      Port
--------------- ----------------- --- ---------- ------- -------------- -------------
10.51.64.1      00-00-5e-00-01-02         23h15m     13m vlan.0.4000    ge.1.1
10.51.64.201    00-11-88-fd-8e-f0   L     23h28m       - vlan.0.4000    host.0.1
134.141.79.190  00-00-5e-00-01-02   H     23h27m     25m vlan.0.4000    ge.1.1
134.141.79.192  00-00-5e-00-01-02   H     23h27m     25m vlan.0.4000    ge.1.1
--------------- ----------------- --- ---------- ------- ------------ -------------
ARP Entries Found: 4
```

Table 59-1 provides an explanation of the command output.

Table 59-1 show arp Output Details

Output...	What it displays...
IP Address	IP address mapped to MAC address.
Hardware Address	MAC address mapped to IP address.
Flags	Route status. Possible values and their definitions include: **U** – The router is currently attempting to resolve an ARP entry. An ARP resolution packet has been sent but a response has not been received. If a response is not received within three (3) seconds the Unresolved entry will be removed from the ARP table. **L** – The IP address and hardware address of this entry is the IP address and hardware address assigned to a directly connected interface. **V** – This is an ARP entry for an interface which is running VRRP. ***** – The ARP entry is stale (timed out). The entry will remain in the database and will be used by the router for “stale-entry-timeout” seconds. See stale-entry-timeout for more information. **S** – A permanent (static) entry manually configured. **B** – Interface was not specified when the static ARP was defined, router will make a best guess. **H** – Host Interest: The ARP entry has been used for direct communication with the router as opposed to communication between hosts that pass through the router. **2** – Secondary VLAN Entry: The ARP entry belongs to a host on a Secondary VLAN.

Table 59-1 show arp Output Details (continued)

Output...	What it displays...
Age	Specifies the amount of time the ARP entry has been in the table.
Updated	Specifies the amount of time that has elapsed since this entry was updated.
Interface	The VLAN interface for this entry.
Port	The port name for this entry.

set arp

Use this command to add mapping entries to the switch's ARP table.

Syntax

set arp *ip-address mac-address* [**interface** *interface*] [**temp**]

Parameters

ip-address	Specifies the IP address to map to the MAC address and add to the ARP table.
mac-address	Specifies the MAC address to map to the IP address and add to the ARP table. The supported MAC address formats are: • HH-HH-HH-HH-HH-HH • HH:HH:HH:HH:HH:HH • HHHH.HHHH.HHHH
interface *interface*	(Optional) Specifies the interface this ARP entry is associated with.
temp	(Optional) Sets the ARP entry as not permanent. This allows the entry to time out.

Defaults

- If **temp** is not specified, the ARP entry will be added as a permanent entry.
- If *interface* is not specified, the router makes a best guess as to the interface the ARP entry is associated with, based upon the best route at the time the ARP entry is used or displayed.

Mode

All command modes.

Usage

The interface option is optional, but if not specified, it defaults to a value of 0. This causes the entry to be marked as a "best guess" entry. Best guess entries are resolved by the ARP subsystem. The interface will be determined based on the best route at the time the ARP entry is used or displayed. If an interface is specified, the entry is anchored to that interface, even if the interface is deleted.

The **set arp** command optionally provides for entering a temporary static ARP entry into the ARP table. Static entries configured using the **arp** command are always entered as permanent static ARP entries in the ARP table. There are no other differences between these two commands.

Because they are not permanent, entries using the **temp** option do not display as static (S), when using the **show arp** command.

Example

This example shows how to map IP address 198.133.219.232 to MAC address 00-00-0c-40-0f-bc and VLAN interface 20:

```
S Chassis(rw)->set arp 198.133.219.232 00-00-0c-40-0f-bc interface vlan.0.20
```

clear arp

Use this command to delete a specific entry or all entries from the switch's ARP table.

Syntax

clear arp {*ipaddress* | **all**}

Parameters

ipaddress | **all**	Specifies the IP address in the ARP table to be cleared, or clears all ARP entries.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to delete entry 10.1.10.10 from the ARP table:

```
S Chassis(rw)->clear arp 10.1.10.10
```

This example shows how to delete all entries from the ARP table:

```
S Chassis(rw)->clear arp all
```

arp

Use this command to add or remove permanent (static) ARP table entries.

Syntax

arp *ip-address mac-address* [**interface** *interface*]

no arp *ip-address*

Parameters

ip-address	Specifies the IP address of a device on the network. Valid values are IP addresses in dotted decimal notation.
mac-address	Specifies the 48-bit hardware address corresponding to the hardware MAC address expressed in hexadecimal notation. The supported MAC address formats are: • HH-HH-HH-HH-HH-HH • HH:HH:HH:HH:HH:HH • HHHH.HHHH.HHHH
interface *interface*	(optional) Specifies the interface this ARP entry is associated with.

Defaults

None.

Mode

Configuration command mode.

Usage

If the interface is not specified, the router will do its best to guess which interface the ARP entry is associated with, based on the best route at the time the entry is used or displayed.

The **set arp** command optionally provides for entering a temporary static ARP entry into the ARP table. Static entries configured using the **arp** command are always entered as permanent static ARP entries in the ARP table. There are no other differences between these two commands.

The "no" form of this command removes the specified permanent ARP entry.

Example

This example shows how to add a permanent ARP entry for the IP address 130.2.3.1, MAC address 0003.4712.7a99, and interface VLAN 20:

```
S Chassis(rw-config)->arp 130.2.3.1 0003.4712.7a99 interface vlan.0.20
```

arp timeout

Use this command to set the duration (in seconds) for entries to stay in the ARP table before expiring.

Syntax

arp timeout *seconds*

no arp timeout *seconds*

Parameters

seconds	Specifies the time in seconds that an entry remains in the ARP cache. Valid values are **0** - **65535**. A value of 0 specifies that ARP entries will never be aged out. Default value: **3600** seconds.

Defaults

None.

Mode

Configuration command mode.

Usage

The **arp timeout 20** command is explicitly added to the configuration at boot time overriding the default value of 3600 seconds with a value of 20 seconds.

The "no" form of this command restores the default value of 3600 seconds.

Example

This example shows how to set the ARP timeout to 7200 seconds:

```
S Chassis(rw-config)->arp timeout 7200
```

arp retransmit-time

Use this command to set the duration (in seconds) to wait before retransmitting ARP requests when trying to resolve ARP entries.

Syntax

arp retransmit-time *seconds*

no arp retransmit-time

Parameters

seconds	Specifies the time in seconds to wait before retransmitting ARP requests when trying to resolve ARP entries. Valid values are **1** - **60**. Default value: **1** second.

Defaults

None.

Mode

Configuration command mode.

Usage

The "no" form of this command restores the default value of 1 second.

Example

This example shows how to set the ARP retransmit-time to 2 seconds:

```
S Chassis(rw-config)->arp retransmit-time 2
```

arp stale-entry-timeout

Use this command to set the number of seconds an ARP entry will remain in the stale state before the entry is removed from the ARP table.

Syntax

arp stale-entry-timeout *seconds*

no arp stale-entry-timeout *seconds*

Parameters

seconds	Specifies the time in seconds that a stale entry remains in the ARP cache. Valid values are **1** - **65535**. Default value: **1200** seconds.

Defaults

None.

Mode

Configuration command mode.

Usage

The “no” form of this command restores the default value of 1200 seconds.

Example

This example shows how to set the ARP stale-entry-timeout to 900 seconds:

```
S Chassis(rw-config)->arp stale-entry-timeout 900
```

arp-nd-proxy-all

Use this command to configure the router to respond to all ARP and Neighbor Discovery requests.

Syntax

arp-nd-proxy-all

no arp-nd-proxy-all

Parameters

None.

Defaults

ARP/ND proxy all is disabled on all interfaces by default.

Mode

Configuration command, Interface configuration command mode.

Example

This example shows how to enable ARP/ND proxy all on VLAN 1:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->arp-nd-proxy-all
```

ip gratuitous-arp

Use this command to override the normal ARP updating process, that occurs by default.

Syntax

```
ip gratuitous-arp {ignore | reply | request}
no ip gratuitous-arp
```

Parameters

ignore	Ignore all gratuitous ARP frames, no updates will occur. This option will also prevent any new learning from gratuitous ARPs, if the command **ip gratuitous-arp-learning** was used. (See "ip gratuitous-arp-learning" on page 59-8 for command details).
reply	Update from gratuitous ARP replies only.
request	Update from gratuitous ARP requests only.

Defaults

ARPs are updated from Gratuitous ARP requests and replies.

Mode

Configuration command, Interface configuration command mode.

Example

This example shows how to enable ARP updating from gratuitous ARP requests on VLAN 1:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip gratuitous-arp request
```

ip gratuitous-arp-learning

Use this command to allow an interface to learn new ARP bindings using gratuitous ARP.

Syntax

```
ip gratuitous-arp-learning {both | reply | request}
no ip gratuitous-arp-learning
```

Parameters

both	Allows learning from both the gratuitous ARP reply and request.
reply	Allows learning from the gratuitous ARP reply.
request	Allows learning from the gratuitous ARP request.

Defaults

None.

Mode

Configuration command, Interface configuration command mode.

Usage

This command will not be in effect if the i**p gratuitous-arp ignore** command (“ip gratuitous-arp” on page 59-8) is used. There will be no learning from gratuitous ARP frames, even with the **ip gratuitous-arp-learning** command enabled.

Gratuitious ARP learning is disabled by default.

The “no” form of this command disables gratuitous ARP learning.

Example

This example shows how to enable gratuitous ARP learning for both requests and replies on VLAN 1:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip gratuitous-arp-learning both
```

ip proxy-arp

Use this command to enable proxy ARP on an interface.

Syntax

```
ip proxy-arp [default-route] [local]
no ip proxy-arp
```

Parameters

default-route	(Optional) Sets the router to respond to ARP requests for hosts that are only reachable using the default route. Typically, proxy arp is only used to reply to requests for hosts that are reachable via a non-default route.
local	(Optional) Allows the router to respond to ARP requests that are received on the interface to which this command is applied if the target IP address of the request is reachable on the interface that received the request.

Defaults

- If **default-route** is not specified, the router responds to ARP requests for hosts that are reachable using any route other than the default route.
- If **local** is not specified, the router responds only to ARP requests that are destined to routes reachable via an interface that is not the interface that received the ARP.

Mode

Configuration command, Interface configuration command mode.

Usage

This variation of the ARP protocol allows the routing module to send an ARP response on behalf of an end node to the requesting host. Proxy ARP can lessen bandwidth use on slow-speed WAN links. It is enabled by default without the default route or local options set.

The "no" form of this command disables proxy ARP

Example

This example shows how to enable proxy ARP:

```
S Chassis(rw-config)->interface vlan 1 on VLAN 1:
S Chassis(rw-config-intf-vlan.0.1)->ip proxy-arp
```

ip mac-address

Use this command to set a MAC address on an interface.

Syntax

ip mac-address *address*

no ip mac-address

Parameters

address	Specifies a 48-bit MAC address in hexadecimal format: HHHH.HHHH.HHHH.

Defaults

None.

Mode

Configuration command, Interface configuration command mode.

Usage

By default, every routing interface uses the same MAC address. If you need interfaces to use different MAC addresses, this command will allow it. It is your responsibility to select a MAC address that will not conflict with other devices on the VLAN, since the Extreme Networks S-Series device will not automatically detect this conflict.

The "no" form of this command clears the MAC address.

Example

This example shows how to set an IP MAC address of 000A.000A.000B on VLAN 1:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip mac-address 000A.000A.000B
```

ip multicast-arp-learning

Use this command to remove the multicast ARP learning restriction on an interface.

Syntax

```
ip multicast-arp-learning
no ip multicast-arp-learning
```

Parameters

None.

Defaults

None.

Mode

Configuration command, Interface configuration command mode.

Usage

As specified in RFC 1812, by default the router must not believe any ARP packet that claims the packet MAC address is broadcast or multicast. Use this command to remove the multicast restriction. The broadcast restriction remains unchanged.

The “no” form of this command reinstates the multicast restriction for ARP packets.

Example

This example shows how to remove the multicast restriction for ARP packets:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip multicast-arp-learning
```

clear arp-cache

Use this command to delete all nonstatic (dynamic) entries from the ARP table.

Syntax

clear arp-cache [*ip-address*] [**interface** *interface*]

Parameters

ip-address	(Optional) Specifies the IP address of the ARP cache entry to clear.
interface *interface*	(Optional) Specifies the interface of the ARP cache entry to clear.

Defaults

If the IP address or the interface is not specified, all ARP cache entries will be cleared.

Mode

All command modes.

Example

This example shows how to delete dynamic ARP cache entry 10.1.10.10 on interface VLAN 10 from the ARP table:

```
S Chassis(rw)->clear arp-cache 10.1.10.10 interface vlan.0.10
```

60

Broadcast Configuration Commands

This chapter describes the broadcast configuration set of commands and how to use them. For information about configuring broadcast commands, refer to the "IP Routing Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
ip directed-broadcast	60-1
ip forward-protocol	60-2
ip dhcp relay information option	60-3
ip dhcp relay information option vpn	60-4
ip dhcp relay information option server-override	60-5
ip dhcp relay information option remote-id	60-6
ip dhcp relay information option circuit-id	60-7
ip dhcp relay information option link-selection	60-8
ip dhcp relay source-interface	60-9
ip helper-address	60-11

ip directed-broadcast

Use this command to enable or disable IP directed broadcasts on an interface.

Syntax

ip directed-broadcast [**access-list** *acl-name*] [**copy-to** *interface*]

no ip directed-broadcast [**access-list** *acl-name*] [**copy-to** *interface*]

Parameters

access-list *acl-name*	(Optional) Specifies a standard or extended access list to apply to this directed broadcast.
copy-to *interface*	(Optional) Specifies an interface to which all directed broadcasts should be copied.

Defaults

If **access-list** *acl-name* is not specified, no ACL is applied to this directed broadcast.

Mode

Configuration command, Interface configuration**.**

Usage

The “no” form of this command disables IP directed broadcast for that interface and removes any access list applied to the command. The “no” form of this command with an access list specified will remove the access list from the command but keep the IP directed broadcast command enabled for that interface.

Examples

This example shows how to enable IP directed broadcasts on VLAN 1 applying ACL **db1**:

```
S Chassis(rw-config)->interface vlan.0.1
S Chassis(rw-config-intf-vlan.0.1)->ip directed-broadcast access-list db1
```

This example shows how to set VLAN 100 as the MAC non-authenticated interface that magic packet directed broadcasts are copied to:

```
S Chassis(rw-config)->interface vlan.0.1
S Chassis(rw-config-intf-vlan.0.1)->ip directed-broadcast copy-to vlan.0.100
```

ip forward-protocol

Use this command to enable UDP broadcast forwarding and specify which protocols will be forwarded.

Syntax

ip forward-protocol {**udp** [*port* | *startport endport*]}

no ip forward-protocol {**udp** [*port* | *startport endport*]}

Parameters

udp	Specifies UDP as the IP forwarding protocol.
port | *startport endport*	(Optional) Specifies a destination port or range of destination ports that control which UDP services are forwarded. If not specified, the forwarding protocols are forwarded on the default ports. The following keywords can be used in place of the standard default port value as specified in the keyword description: • **bootps** - Specifies the Bootstrap Protocol server (67) port. • **domain** - Specifies the Domain Name Service (53) port. • **nameserver** - Specifies the IEN116 name service (42) port.
	• **netbios-dgm** - Specifies the NetBIOS datagram service (138) port. • **netbios-ns** - Specifies the NetBIOS name service (137) port. • **tacacs** - Specifies the Terminal Access Controller Access Control System (49) port. • **tftp** - Specifies the Trivial File Transfer Protocol (69) port. • **time** - Specifies the Time (37) port.

Defaults

If *port* is not specified, default forwarding services will be performed as listed above.

Mode

Configuration command, Global configuration**.**

Usage

If a certain service exists inside the node, and there is no need to forward the request to remote networks, the "no" form of this command should be used to disable the forwarding for the specific port. Such requests will not be automatically blocked from being forwarded just because a service for them exists in the node.

The "no" form of this command removes a UDP port or protocol, disabling forwarding.

Examples

This example shows how to enable forwarding of Domain Naming System UDP datagrams (port 53):

```
S Chassis(rw-config)->ip forward-protocol udp 53
```

This example shows how to enable forwarding of Domain Naming System UDP datagrams (port 53) by naming the protocol:

```
S Chassis(rw-config)->ip forward-protocol udp domain
```

ip dhcp relay information option

Use this command to insert the **circuit-id** (1) and **remote-id** (2) sub-options of the Relay Agent Information option (82) into the relay agent DHCP packet.

Syntax

ip dhcp relay information option

no ip dhcp relay information option

Parameters

None.

Defaults

None.

Mode

Configuration command, Global configuration**.**

Configuration command, Interface configuration.

Usage

When forwarding DHCP requests from a local client to a remote DHCP server, the DHCP relay agent needs to include information about itself in order for the DHCP server to determine which pool of client addresses to pull the lease from. Including Option 82 in the DHCP relay information provides the required DHCP relay information.

Refer to RFC 3046 for descriptions of these sub-options:

The default **circuit-id** sub-option value inserted into the relay agent DHCP packet is the interface name of the interface receiving the request from the client, in the form of vlan.0.x where x is the VLAN id between 1 and 4094. This default value can be over-ridden at the interface level by using the **ip dhcp relay information option circuit-id** command in interface configuration mode.

The **remote-id** sub-option is used to identify the remote host end of the circuit. The default value inserted into the relay agent DHCP packet is the MAC address of the chassis. This default value can be over-ridden by using the **ip dhcp relay information option remote-id** command in global configuration mode or interface configuration mode.

The "no" form of this command removes the sending of these sub-options of Option 82 in the DHCP relay information.

Example

This example enables sending the **circuit-id** and **remote-id** sub-options in the relay agent DHCP packet.

```
S Chassis(su)->configure
S Chassis(su-config)->ip dhcp relay information option
```

ip dhcp relay information option vpn

Use this command to insert the Relay Agent Information option **virtual subnet selection** (151), **link selection** (5), and **server identifier override** (11) option 82 sub-options into the relay agent DHCP packet.

Syntax

```
ip dhcp relay information option vpn
no ip dhcp relay information option vpn
```

Parameters

None.

Defaults

None.

Mode

Configuration command, Global configuration.

Configuration command, Interface configuration**.**

Usage

When forwarding the local UDP broadcasts from a VRF to a destination address on a different VRF, the DHCP relay agent needs to include information about itself in order for the DHCP server to determine which pool of client addresses to pull the lease from. Including Option 82 sub-options in the DHCP relay information provides the required DHCP relay information.

The **virtual subnet selection** (VSS) options/sub-options are described in RFC 6607. They are used to pass VSS information about a VPN to the DHCP server to assist in determining the subnet on which to select an address. You can set the VPN id for a VRF with the **vpn id** command. If a VPN id is not configured for the VRF, the virtual subnet selection sub-option will contain the VRF name.

The **link selection** sub-option is described in RFC 3527. The link-selection sub-option is used by any DHCP relay agent that desires to specify a subnet/link for a DHCP client request that it is relaying but needs the subnet/link specification to be different from the IP address the DHCP server should use when communicating with the relay agent. By default, the link selection sub-option contains the primary IP address of the inbound interface to which the client is connected. This default value can be changed with the **ip dhcp relay information option link-selection** command.

The **server identifier override** sub-option is described in RFC 5107. This sub-option allows the DHCP relay agent to specify a new value for the server ID option, which is inserted by the DHCP server in the reply packet. This allows the DHCP relay agent to act as the actual DHCP server so that subsequent requests from the client will come to the relay agent rather than to the DHCP server directly. The server identifier override sub-option contains the IP address of the inbound interface to which the client is connected, which is the IP address on the relay agent that is accessible from the client. Using this information, the DHCP client sends all renew and release requests to the relay agent. The relay agent adds all of the appropriate sub-options and then forwards the request packets to the original DHCP server.

The "no" form of this command removes the sending of these options/sub-options in the DHCP relay information.

Example

The following example:

- Enables IP forwarding for the UPD protocol on VRF Alpha-Group.
- Enables DHCP/BOOTP relay on VLAN 10 of VRF Alpha-Group and sets the new destination address to 134.141.95.105 on VRF Internet-Access.
- Configures inclusion of DHCP relay agent information sub-options **virtual subnet selection, link selection**, and **server identifier override** in the packet sent to the DHCP server by the relay agent.

```
S Chassis(su)->router Alpha-Group
S Chassis(su-*ha-Group)->configure
S Chassis(su-*ha-Group-config)->ip forward-protocol udp
S Chassis(su-*ha-Group-config)->interface vlan.0.10
S Chassis(su-*ha-Group-config-intf-vlan.0.10)->ip helper-address 134.141.95.105
vrf Internet-Access
S Chassis(su-*ha-Group-config-intf-vlan.0.10)->ip dhcp relay information option
vpn
S Chassis(su-*ha-Group-config-intf-vlan.0.10)->exit
S Chassis(su-*ha-Group-config)->
```

ip dhcp relay information option server-override

Use this command to insert the Relay Agent Information option 82 sub-options **link selection** (5) and **server identifier override** (11) into the relay agent DHCP packet.

Syntax

ip dhcp relay information option server-override

no ip dhcp relay information option server-override

Parameters

None.

Defaults

None.

Mode

Configuration command, Global configuration.

Configuration command, Interface configuration**.**

Usage

When forwarding DHCP requests from a local client to a remote DHCP server, the DHCP relay agent needs to include information about itself in order for the DHCP server to determine which pool of client addresses to pull the lease from. Including Option 82 sub-options in the DHCP relay information provides the required DHCP relay information.

The **link selection** sub-option is described in RFC 3527. The link-selection sub-option is used by any DHCP relay agent that desires to specify a subnet/link for a DHCP client request that it is relaying but needs the subnet/link specification to be different from the IP address the DHCP server should use when communicating with the relay agent. By default, the link selection sub-option contains the subnet of the inbound interface to which the client is connected. This default value can be changed with the **ip dhcp relay information option link-selection** command.

The **server identifier override** sub-option is described in RFC 5107. This sub-option allows the DHCP relay agent to specify a new value for the server ID option, which is inserted by the DHCP server in the reply packet. This allows the DHCP relay agent to act as the actual DHCP server so that subsequent requests from the client will come to the relay agent rather than to the DHCP server directly. The server identifier override sub-option contains the IP address on the relay agent that is accessible from the client. Using this information, the DHCP client sends all renew and release requests to the relay agent. The relay agent adds all of the appropriate sub-options and then forwards the request packets to the original DHCP server.

The “no” form of this command removes the sending of these options/sub-options in the DHCP relay information.

Example

This example configures inclusion of DHCP relay agent information sub-options **link selection** and **server identifier override** in the packet sent to the DHCP server by the client

```
S Chassis(su)->configure
S Chassis(su-config)->ip dhcp relay information option server-override
```

ip dhcp relay information option remote-id

Use this command to modify the value of the **remote-id** (2) sub-option sent in the Relay Agent Information option 82.

Syntax

ip dhcp relay information option remote-id *remote-id*

no ip dhcp relay information option remote-id [*remote-id*]

Parameters

remote-id	Specifies the value of the remote-id sub-option as an ASCII string.

Defaults

None.

Mode

Configuration command, Global configuration.

Configuration command, Interface configuration**.**

Usage

If the **ip dhcp relay information option** command has been executed, the **remote-id** sub-option is included in the DHCP Relay Agent packet sent to the server, using a default value of the MAC address of the chassis.

Use this command to change the value of the **remote-id** sub-option.

Example

This example configures sending the **circuit-id** (1) and **remote-id** (2) sub-options of the Relay Agent Information option (82) in the relay agent DHCP packet, then changes the value of the remote-id option to remoteid_blue.

```
S Chassis(su)->configure
S Chassis(su-config)->ip dhcp relay information option
S Chassis(su-config)->ip dhcp relay information option remote-id remoteid_blue
```

ip dhcp relay information option circuit-id

Use this command to modify the value of the **circuit-id** (1) sub-option sent in the Relay Agent Information option.

Syntax

ip dhcp relay information option circuit-id *circuit-id*

no ip dhcp relay information option circuit-id [*circuit-id*]

Parameters

circuit-id	Specifies the value of the circuit-id sub-option as an ASCII string.

Defaults

None.

Mode

Configuration command, Interface configuration**.**

Usage

If the **ip dhcp relay information option** command has been executed, the **circuit-id** sub-option is included in the DHCP Relay Agent packet sent to the server, using as the default value the

interface name of the interface receiving the request from the client, in the form of vlan.0.x where x is the VLAN id between 1 and 4094.

Use this command to change the value of the **circuit-id** sub-option.

Example

This example configures sending the **circuit-id** (1) and **remote-id** (2) sub-options of the Relay Agent Information option (82) in the relay agent DHCP packet, then changes the value of the circuit-id option to vlan_red for VLAN 10.

```
S Chassis(su)->configure
S Chassis(su-config)->ip dhcp relay information option
S Chassis(su-config)->interface vlan.0.10
S Chassis(su-config-intf-vlan.0.10)->ip dhcp relay information option circuit-id
vlan_red
```

ip dhcp relay information option link-selection

Use this command to insert the **link selection** (5) sub-option into the Relay Agent Information packet.

Syntax

ip dhcp relay information option link-selection *IP-subnet* {**vendor-id** *vendor-id*| **mac** *mac-addr*}

no ip dhcp relay information option link-selection [*IP-subnet* {**vendor-id** *vendor-id*| **mac** *mac-addr*}]

Parameters

IP-subnet	Specifies the IP subnet that should be included in the link selection sub-option.
vendor-id *vendor-id*	Specifies the vendor-id (DHCP option 60) to be included in the link selection sub-option.
mac *mac-addr*	Specifies the MAC address of the client hardware. This value can be a partial or full match, in hex format. For example, 01dead or 000203040506.

Defaults

None

Mode

Configuration command, Interface configuration**.**

Usage

The **link selection** sub-option is described in RFC 3527.

You can use this command to specify that the link selection sub-option should be included in the Relay Agent Information and to specify a different subnet from the primary IP address on the relay agent's interface. With this command, you can select a secondary IP address on the interface to be used to help in DHCP pool selection on the server. The subnet selection can be based on the DHCP client's vendor id (option 60) or the hardware MAC address.

When both the MAC address and vendor-id are configured for a specific subnet and the DHCP client can match on both values, the vendor-id link selection is used.

Within a VLAN, a maximum of 20 link selection subnet/vendor or MAC value combinations can be configured.

Example

This example shows how you would use the link selection option to tell the DHCP server to assign leases from different sub-networks, depending on information received in the DHCP client request. For example, when the relay agent receives a DHCP client request from a host with MAC address 002654AF123B, the relay agent sets the DHCP relay agent information link selection option value to 10.180.2.0. If the MAC address were 00301E44AC12, the option value would be set to 10.180.3.0.

```
S Chassis(su)->configure
S Chassis(su-config)->interface vlan.0.10
S Chassis(su-config-intf-vlan.0.10)->ip address 10.180.1.8 255.255.255.0 primary
S Chassis(su-config-intf-vlan.0.10)->ip address 10.180.2.8 255.255.255.0
secondary
S Chassis(su-config-intf-vlan.0.10)->ip address 10.180.3.8 255.255.255.0
secondary
S Chassis(su-config-intf-vlan.0.10)->ip address 10.180.4.8 255.255.255.0
secondary
S Chassis(su-config-intf-vlan.0.10)->ip directed-broadcast
S Chassis(su-config-intf-vlan.0.10)->ip helper-address 11.5.255.255 global
S Chassis(su-config-intf-vlan.0.10)->ip dhcp relay information option
S Chassis(su-config-intf-vlan.0.10)->ip dhcp relay information option vpn
S Chassis(su-config-intf-vlan.0.10)->ip dhcp relay information option remote-id
Shrewsbury
S Chassis(su-config-intf-vlan.0.10)->ip dhcp relay information option circuit-id
engineering
S Chassis(su-config-intf-vlan.0.10)->ip dhcp relay information option
link-selection 10.180.2.0 mac 002654AF123B
S Chassis(su-config-intf-vlan.0.10)->ip dhcp relay information option
link-selection 10.180.2.0 vendor-id "MSFT 5.0"
S Chassis(su-config-intf-vlan.0.10)->ip dhcp relay information option
link-selection 10.180.3.0 mac 00301E44AC12
S Chassis(su-config-intf-vlan.0.10)->ip dhcp relay information option
link-selection 10.180.4.0 mac 001CC504BC34
S Chassis(su-config-intf-vlan.0.10)->exit
S Chassis(su-config)->
```

ip dhcp relay source-interface

Use this command to specify the source interface to be used in the Relay Agent packets sent to the DHCP server or other relay agent.

Syntax

ip dhcp relay source-interface *interface*

no ip dhcp relay source-interface [*interface*]

Parameters

interface	Specifies the interface to be used as the source address in Relay Agent packets sent to the DHCP server. The interface can be a VLAN or loopback interface.

Defaults

If a source interface is not specified with this command, the default is the primary IP address of the VLAN interface that the DHCP client is connected to.

Mode

Configuration command, Global configuration.

Configuration command, Interface configuration**.**

Usage

This command allows you to specify the source IP address to be used used in the Relay Agent packets sent to the DHCP server or other relay agent. This feature should be used in conjunction with the **ip dhcp relay information option server-override** or **ip dhcp relay information option vpn** commands, which cause the **server identifier override** (11) sub-option to be added to the Relay Agent DHCP packets sent to the DHCP server.

Note: The source interface specified with this command must belong to the same VRF specified with the ip helper-address command described below.

Example

The following example:

- Enables IP forwarding for the UPD protocol on VRF Alpha-Group
- Enables DHCP/BOOTP relay on VLAN 10 of VRF Alpha-Group and sets the new destination address to 134.141.95.105 on VRF Internet-Access
- Configures the inclusion of DHCP relay agent information options **virtual subnet selection** (151), **link selection** (5), and **server identifier override** (11) sub-options into the relay agent DHCP packet sent to the server or other relay agent with the **ip dhcp relay information option vpn** command.
- Configures the source interface (VLAN 20) to be used in the server identifier override sub-option.

```
S Chassis(su)->router Alpha-Group
S Chassis(su-*ha-Group)->configure
S Chassis(su-*ha-Group-config)->ip forward-protocol udp
S Chassis(su-*ha-Group-config)->interface vlan.0.10
S Chassis(su-*ha-Group-config-intf-vlan.0.10)->ip helper-address 134.141.95.105
vrf Internet-Access
S Chassis(su-*ha-Group-config-intf-vlan.0.10)->ip dhcp relay information option
vpn
S Chassis(su-*ha-Group-config-intf-vlan.0.10)->ip dhcp relay source-interface
vlan.0.20
S Chassis(su-*ha-Group-config-intf-vlan.0.10)->exit
```

ip helper-address

Use this command to enable DHCP/BOOTP relay and the forwarding of local UDP broadcasts specifying a new destination address.

Syntax

ip helper-address *address* [**global** | **vrf** *vrf-name*] [**access** *acl-name*]

no ip helper-address *address*

Parameters

address	Specifies a destination address used by forwarded local UDP broadcasts.
global	(Optional) Specifies that the default global forwarding table will be used for route lookup.
vrf *vrf-name*	(Optional) Specifies that the routing table of the specified VRF will be used for route lookup.
access-list *acl-name*	(Optional) Specifies the standard or extended IP access list to be applied to inbound UDP frames.

Defaults

None.

Mode

Configuration command, Interface configuration**.**

Usage

This command works in conjunction with the **ip forward-protocol** command, which defines the forward protocol and port number. You can use this command to add more than one helper address per interface.

When enabling DHCP/BOOTP relay and forwarding local UDP broadcasts to a new destination address that is located on a different VRF or the global router, the destination VRF router must be specified in the **ip helper-address** command. Use the **vrf** *vrf-name* parameter to specify a destination VRF or the **global** parameter to specify the global router as the destination.

When forwarding the local UDP broadcasts from a VRF to a destination address on a different VRF, the DHCP relay agent needs to include information about itself in order for the DHCP server to determine which pool of client addresses to pull the lease from. Including Option 82 in the DHCP relay information provides the required DHCP relay information.

Use the **ip dhcp relay information option server-override** or **ip dhcp relay information option vpn** commands described in this chapter to include DHCP relay agent information in the packet sent to the server by the DHCP relay agent.

The “no” form of this command disables the forwarding of UDP datagrams to the specified address

Examples

This example shows how to permit UDP broadcasts from hosts on networks 191.168.1.255 and 192.24.1.255 to reach servers on other networks:

```
S Chassis(rw)->configure
S Chassis(rw-config)->ip forward-protocol udp
S Chassis(rw-config)->interface vlan.0.5
S Chassis(rw-config-intf-vlan.0.5)->ip helper-address 192.168.1.255
S Chassis(rw-config-intf-vlan.0.5)->exit
S Chassis(rw-config)->interface vlan.0.2
S Chassis(rw-config-intf-vlan.0.2)->ip helper-address 192.24.1.255
```

The following example:

- Enables IP forwarding for the UPD protocol on VRF Alpha-Group
- Enables DHCP/BOOTP relay on VLAN 10 of VRF Alpha-Group and sets the new destination address to 134.141.95.105 on VRF Internet-Access
- Configures the inclusion of DHCP relay agent information in the packet sent from the client to the DHCP server

```
S Chassis(su)->router Alpha-Group
S Chassis(su-*ha-Group)->configure
S Chassis(su-*ha-Group-config)->ip forward-protocol udp
S Chassis(su-*ha-Group-config)->interface vlan.0.10
S Chassis(su-*ha-Group-config-intf-vlan.0.10)->ip helper-address 134.141.95.105
vrf Internet-Access
S Chassis(su-*ha-Group-config-intf-vlan.0.10)->exit
S Chassis(su-*ha-Group-config)->ip dhcp relay information option vpn
S Chassis(su-*ha-Group-config)->
```

61

IP Debug

This chapter describes the IP debug set of commands and how to use them. For information about configuring IP debug, refer to the "IP Routing Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
debug ip bgp	61-1
debug ip ospf	61-2
debug packet restart	61-3
debug packet show-statistics	61-3
debug packet clear-statistics	61-4
debug packet filter	61-5
debug packet control	61-6
show debugging	61-7
debug ip vrrp	61-9
debug ip vrrp show	61-9

debug ip bgp

Use this command to enable the debug IP BGP utility for monitoring BGP timers, messages and routes.

Syntax

debug ip bgp {**keepalive** | **notification** | **open** | **route-refresh** | **route-add** | **route-ineligible** | **route-remove** | **update** | **dampen** | **timer**}

no debug ip bgp {**keepalive** | **notification** | **open** | **route-refresh** | **route-add** | **route-ineligible** | **route-remove** | **update** | **dampen** | **timer**}

Parameters

keepalive	Specifies the monitoring of BGP keepalive messages.
notification	Specifies the monitoring of BGP notification messages.
open	Specifies the monitoring of BGP open messages.
route-refresh	Specifies the monitoring of BGP route-refresh messages.
route-add	Specifies the monitoring of BGP routes added to the local rib.

route-ineligible	Specifies the monitoring of BGP rib-in routes deemed ineligible for decision process.
route-remove	Specifies the monitoring of BGP routes removed from the local rib.
update	Specifies the monitoring of BGP update messages.
dampen	Specifies the monitoring of BGP route flap dampening events.
timer	Specifies the monitoring of BGP keepalive and hold timer events.

Defaults

None.

Mode

Configuration command mode.

Usage

The "no" form for this command disables BGP debugging for the specified option.

Example

This example shows how to set the debug IP BGP utility to monitor route refresh messages:

```
S Chassis(rw-config)->debug ip bgp route-refresh
S Chassis(rw-config)->
```

debug ip ospf

Use this command to enable the debug IP OSPF utility for monitoring OSPF adjacencies, LSA generation, packets, and retransmissions.

Syntax

debug ip ospf {**adj** | **lsa-generation** | **packet** | **retransmission** | **trace-interface** *interface*}

no debug ip ospf {**adj** | **lsa-generation** | **packet** | **retransmission** | **trace-interface** *interface*}

Parameters

adj	Specifies the monitoring of OSPF adjacency events.
lsa-generation	Specifies the monitoring of OSPF LSA generation events.
packet	Specifies the monitoring of OSPF packets.
retransmission	Specifies the monitoring of OSPF retransmissions.
trace-interface *interface*	Specifies the monitoring of the specified interface.

Defaults

None.

Mode

Configuration command mode.

Usage

The “no” form for this command disables OSPF debugging for the specified option.

Example

This example shows how to set the debug IP OSPF utility to monitor OSPF adjacency events:

```
S Chassis(rw-config)->debug ip ospf adj
S Chassis(rw-config)->
```

debug packet restart

Use this command to restart the debug IP packet utility.

Syntax

debug packet restart

Parameters

None.

Defaults

None.

Mode

Configuration command.

Usage

By default, 10 debug messages will be display and then the packet monitor will stop. To collect another 10 messages, use this command.

Example

This example shows how to restart the debug IP packet utility:

```
S Chassis(rw-config)->debug packet restart
```

debug packet show-statistics

Use this command to display debug statistics for packet and host counters, and IPv4 and IPv6 exceptions.

Syntax

debug packet show [**packet-counters**] [**ipv4-exceptions**] [**ipv6-exceptions**] [**host-counters**] [*slot*]

Parameters

packet-counters	(Optional) Displays packet counters.
ipv4-exceptions	(Optional) Displays IPv4 exceptions counters.

ipv6-exceptions	(Optional) Displays IPv6 exceptions counters.
host-counters	(Optional) Displays host counters.
slot	(Optional) Displays counters for the specified slot number only.

Defaults

If no options are specified, all packet counters are displayed for all slots in the device.

Mode

Configuration command.

Example

This example shows how to display packet counters for slot 1:

```
S Chassis(rw-config)->debug packet show-statistics packet-counters 1

          Router Statistics for Slot 1 - last cleared 1d 4h 5m 44s ago
                      (repeat command to refresh counters)
-------------------------------------------------------------------------------
   type                                              count     hi-count-blade
-------------------------------------------------------------------------------
                                  Packet Counts
   Total Packets in:                                 27639                  2
   IPv4 Packets in:                                  27474                  2
   Non-Unicast Packets in:                           21068                  2
   Non-Unicast Packets Drop:                             0                  2
   IPv6 Unicast Packets in:                             76                  2
   IPv6 Multicast Packets  in:                           0                  2
   Non Vlan Packets in:                                  0
   ARP Packets in:                                      89                  1
   ARP/ND Defer Packets :                                3                  2
   ARP/ND Pending Packets :                              0
   ACL Deny In Packets :                                 0
   ACL Deny Out Packets :                                0
   ACL Service Packets :                                 0
   IPv4 Forwarded Packets:                            6406                  2
   IPv6 Forwarded Packets:                              52                  2
   Flooded Packets:                                      0
S Chassis(rw-config)->
```

debug packet clear-statistics

Use this command to clear the router packet debug statistics.

Syntax

debug packet clear-statistics

Parameters

None.

Defaults

None.

Mode

Configuration command.

Example

This example shows how to clear all router debug packet statistics:

```
S Chassis(rw-config)->debug packet clear-statistics
S Chassis(rw-config)->
```

debug packet filter

Use this command to filter debug messages based upon the specified criteria.

Syntax

debug packet filter {[**vlan-in-list** *vlan-list*] [**vlan-out-list** *vlan-list*] [**port-in-list** *port-list*] [**port-out-list** *port-list*] [**src-mac** *mac-address*] [**dest-mac** *mac-address*] [**etype** *value*] [**access-list** *access-list*] [**arp** {*ip-address netmask* | *ip-address/length*}]}

no debug packet

Parameters

vlan-in-list *vlan-list*	(Optional) Filters packet debug messages based upon an inbound VLAN ID or range of IDs. Valid values are **1** - **4094**.
vlan-out-list *vlan-list*	(Optional) Filters packet debug messages based upon an outbound VLAN ID or range of IDs. Valid values are **1** - **4094**.
port-in-list *port-list*	(Optional) Filters packet debug messages based upon an inbound port or range of ports in a *media.slot.port* format.
port-out-list *port-list*	(Optional) Filters packet debug messages based upon an outbound port or range of ports in a *media.slot.port* format.
src-mac *mac-address*	(Optional) Filters packet debug messages based upon a 48-bit MAC hardware source address.
dest-mac *mac-address*	(Optional) Filters packet debug messages based upon a 48-bit MAC hardware destination address.

etype *value*	(Optional) Filters packet debug messages based upon an IEEE Ethernet type number or keyword: • *value* – a hex value IEEE Ethernet type number • **LLC_IP** – 0606: IP over EEE 802.2 Logical Link Control/SNAP • **IP** – 0800: IP ethernet version 2 • **ARP** – 0806: Address Resolution Protocol • **REVARP** – 8035: Reverse Address Resolution Protocol • **VLAN** – 8100: IEEE 802.1Q VLAN tagging • **IPV6** – 86dd: IPv6
access-list *access-list*	(Optional) Filters packet debug messages based upon the contents of an IPv4 or IPv6 access list.
arp *ip-address netmask* | *ip-address/length*	(Optional) Filters packet debug messages based upon an ARP IP network address.

Defaults

At least one option must be specified. Filtering does not take place for unspecified options.

Mode

Configuration command.

Usage

Packet debug messages only display for the specified options. At least one option must be specified.

This command overwrites any preexisting debug filter configuration.

Use the **no debug packet** command to reset all packet debug parameters to the default value or behavior. In the case of packet debug filtering, all packet debug messages display.

Use the **show debugging packet** command to display packet debug settings, including the current debug packet filter settings.

Example

This example shows how to filter packet debug such that only packets that meet the criteria specified in access-list **doctest** display:

```
S Chassis(rw-config)->debug packet filter access-list doctest
S Chassis(rw-config)->
```

debug packet control

Use this command to set debug utility control features.

Syntax

debug packet control {[**throttle** *throttle*] [**limit** *limit*] [**verbose** | **brief**]}

no debug packet

Parameters

throttle *throttle*	(Optional) Sets the maximum number of debug packets per second to display. Valid values are **2** - **100**. Default value is **10**.
limit *limit*	(Optional) Sets the maximum number debug packets to display per board per run. Valid values are **0** - **1000**. **0** = no limit. Default value is **10**.
verbose	(Optional) Displays the maximum amount of information available per debug packet. **verbose** is the default level of information displayed by the debug utility.
brief	(Optional) Displays the minimum amount of information available per debug packet.

Defaults

At least one option must be specified. Any option not specified remains unchanged.

Mode

Configuration command.

Usage

If a control limit other than 0 is specified, when the number of debug messages displayed reaches the limit, no further messages display until the debug utility is restarted using "debug packet restart" on page 61-3.

Example

This example shows how to set the debug control throttle setting to 15 messages per second:

```
S Chassis(rw-config)->debug packet control throttle 15
S Chassis(rw-config)->
```

show debugging

Use this command to display the IP debug utility settings.

Syntax

```
show debugging [ospf | bgp | packet | vrrp]
```

Parameters

ospf	Specifies that only OSPF debug settings will display.
bgp	Specifies that only BGP debug settings will display.
packet	Specifies that only IP packet debug settings will display.
vrrp	Specifies that only VRRP debug settings will display.

Defaults

If no option is displayed, all debug settings are shown.

Mode

Configuration command.

Example

This example shows how to display the IP debug utility settings:

```
S Chassis(rw)->show debugging

OSPF settings
 Version           : OSPFV2
 Vrf               : global
 Adjacency         : no
 Lsa Generation    : no
 Packets           : no
 Retransmission    : no
 Trace Interface   : all vlans
 Trace Packet Type : all packets

Packet filter settings
 Status            : disabled - no filter specified
 Throttle          : 10
 Limit             : 10
 Verbose           : yes

VRRP Trace settings
 Advertisements    : no
 Critical IP       : no
 Trace Interface   : all vlans
 Trace VRID        : all vrids

BGP settings
 Vrf               : global
 dampen            : no
 keepalive         : no
 notification      : no
 open              : no
 route-refresh     : no
 route-add         : no
 route-remove      : no
 route-ineligible  : no
 timers            : no
 update            : no
S Chassis(rw)->
```

debug ip vrrp

Use this command to enable the debug IP VRRP utility for monitoring VRRP advertisements, critical IP interfaces, a VRRP interface or a VRRP virtual router.

Syntax

debug ip vrrp {**advertisements** | **critical-ip** | **trace-interface** *interface* | **trace-vrid** *vrid*}

no debug ip vrrp {**advertisements** | **critical-ip** | **trace-interface** *interface* | **trace-vrid** *vrid*}

Parameters

advertisements	Specifies the monitoring of VRRP advertisements.
critical-ip	Specifies the monitoring of critical IP interfaces.
trace-interface *interface*	Specifies the monitoring of a specified VRRP interface.
trace-vrid *vrid*	Specifies the monitoring of a specified VRRP virtual router.

Defaults

None.

Mode

Configuration command mode.

Usage

The “no” form for this command disables VRRP debugging for the specified option.

Example

This example shows how to set the debug IP VRRP utility to monitor advertisement events:

```
S Chassis(rw-config)->debug ip vrrp advertisement
S Chassis(rw-config)->
```

debug ip vrrp show

Use this command to display IP VRRP debug settings.

Syntax

debug ip vrrp show

Parameters

None.

Defaults

None.

Mode

Configuration command mode.

Example

This example shows how to display IP VRRP debug settings:

```
S Chassis(rw-config)->debug ip vrrp show

VRRP Trace settings
 Advertisements    : no
 Critical IP       : no
 Trace Interface   : all vlans
 Trace VRID        : all vrids

S Chassis(rw-config)->
```

62

IGMP Commands

This chapter describes the IGMP configuration set of commands and how to use them. For information about configuring IGMP, refer to the "Multicast Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
Enabling / Disabling IGMP	62-1
Configuring IGMP	62-3

Enabling / Disabling IGMP

This section describes the display of IGMP information and the enabling and disabling of IGMP snooping on the device.

For information about...	Refer to page...
show igmp enable	62-1
set igmp enable	62-2
set igmp disable	62-2

show igmp enable

Use this command to display the status of IGMP on one or more VLAN(s).

Syntax

show igmp enable [*vlan-list*]

Parameters

vlan-list	(Optional) Specifies the VLAN(s) for which to display IGMP status.

Defaults

If *vlan-list* is not specified, the output displays IGMP status for all VLANs.

Mode

All command modes.

Example

This example shows how to display the IGMP status for all VLANs:

```
S Chassis(rw)->show igmp enable
IGMP Vlans Enabled : 13,23,1010,1020,1030,1040
```

set igmp enable

Use this command to enable IGMP on one or more VLANs.

Syntax

set igmp enable *vlan-list*

Parameters

vlan-list	Specifies the VLAN(s) on which to enable IGMP.

Defaults

None.

Mode

All command modes.

Usage

On VLANs where IGMP snooping is enabled, any received multicast stream will be flooded to the VLAN until such time as the IGMP database is populated, then stream forwarding will revert to ports with group membership only.

Example

This example shows how to enable IGMP on VLAN 104:

```
S Chassis(rw)->set igmp enable 104
```

set igmp disable

Use this command to disable IGMP on one or more VLANs.

Syntax

set igmp disable *vlan-list*

Parameters

vlan-list	Specifies the VLAN(s) on which to enable IGMP.

Defaults

None.

Mode

All command modes.

Example

This example shows how to disable IGMP on VLAN 104:

```
S Chassis(rw)->set igmp disable 104
```

Configuring IGMP

This section describes how to display and set IGMP configuration parameters, including query interval and response time settings, and to create and configure static IGMP entries.

For information about...	Refer to page...
show igmp config	62-4
set igmp config	62-5
show igmp counters	62-7
clear igmp counters	62-7
set igmp delete	62-8
show igmp flows	62-8
show igmp flow-full-action	62-10
set igmp flow-full-action	62-10
show igmp groups	62-11
set igmp input-filter	62-13
show igmp input-filter	62-14
clear igmp input-filter	62-14
show igmp number-flows	62-15
set igmp portFastLeave	62-16
clear igmp portFastLeave	62-16
show igmp protocols	62-17
set igmp protocols	62-18
clear igmp protocols	62-18
show igmp query	62-19
set igmp query-enable	62-20
set igmp query-disable	62-20
show igmp reporters	62-21
show igmp static	62-22
set igmp static	62-22
clear igmp static	62-23
set igmp unknown-input-action	62-25
show igmp unknown-input-action	62-25
show igmp vlan	62-26

show igmp config

Use this command to display IGMP configuration information for one or more VLANs.

Syntax

show igmp config *vlan-list*

Parameters

vlan-list	Specifies the VLAN(s) for which to display IGMP configuration information.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display IGMP configuration information for VLAN 1:

```
S Chassis(su)->show igmp config 1

IGMP config for vlan 1
----------------------------------
QueryInterval(sec.)          - 125
Status                       - Active
Version                      - 2
QueryMaxResponseTime(sec.)   - 10
Robustness                   - 2
LastMemberQueryIntvl         - 10
FastLeaveState               - Disabled
RouterAlert Required         - True
QuerierUpTime                - 0 D  0 H  0 M  0 S
QuerierExpiryTime            - 0 D  0 H  0 M  0 S
QuerierIP                    - 0.0.0.0
```

Table 62-1 shows a detailed explanation of command output. For details on using the **set igmp config** command to set these parameters, refer to "set igmp config" on page 62-5.

Table 62-1 show igmp config Output Details

Output...	What it displays...
QueryInterval(sec.)	Frequency (in seconds) of host-query frame transmissions.
Status	Whether VLAN configuration is **Active** or **Not in Service**.
Version	IGMP version (**1** or **2**).
QueryMaxResponseTime(sec.)	Maximum query response time.

Table 62-1 show igmp config Output Details (continued)

Output...	What it displays...
Robustness	Robustness value.
LastMemberQueryIntvl	Last member query interval (in tenths of a second). This is the maximum response time inserted into group-specific queries which are sent in response to Leave Group messages. It is also the amount of time between group-specific query messages.
FastLeaveState	Whether fast leave is enabled or disabled on the VLAN.
RouterAlert Required	Whether routing alert checking is required.
QuerierUpTime	Time (in days, hours, minutes, and seconds) the IGMP querier has been active.
QuerierExpiryTime	Time (in days, hours, minutes, and seconds) before the IGMP querier expires.
QuerierIP	IP address of the IGMP querier.

set igmp config

Use this command to configure IGMP settings on one or more VLANs.

Syntax

set igmp config *vlan-list* {[**query-interva**l *query-interval*] [**igmp-version** *igmp-version*] [**max-resp-time** *max-resp-time*] [**robustness** *robustness*] [**last-mem-int** *last-mem-int*] [**fast-leave** *fast-leave*] [**rtr-alert-checking** *rtr-alert-checking*] [**filter-id** *filter-id*] [**filter-status** {enable | disable}]}

Parameters

vlan-list	Specifies the VLAN(s) on which to configure IGMP.
query-interval *query-interval*	(Optional) Specifies the frequency of host-query frame transmissions. Valid values are from **1–31744** seconds. This value works together with *max-resp-time* to remove ports from an IGMP group.
igmp-version *igmp-version*	(Optional) Specifies the IGMP version. Valid values are: • **1** — IGMP V1 • **2** — IGMP V2 • **3** — IGMP V3
max-resp-time *max-resp-time*	(Optional) Specifies the maximum query response time. Valid values for IGMP V1 and V2 are 1–25 seconds; IGMP V3 are 0– 3174 seconds. This value works together with *query-interval* to remove ports from an IGMP group.
robustness *robustness*	(Optional) Specifies the robustness value. This can be increased to tune for expected packet loss on a subnet. Valid values are **2–255.**
last-mem-int *last-mem-int*	(Optional) Specifies the Last Member Query Interval. This is the maximum response time inserted into group-specific queries which are sent in response to Leave Group messages. It is also the amount of time between group-specific query messages. Valid values are 1**–255** tenths of a second.

fast-leave *fast-leave*	(Optional) Set the VLAN's fast leave state. • **1** — Enable • **2** — Disable The fast leave setting is applied to both IGMP and MLD regardless of which protocol it is set in.
rtr-alert-checking *rtr-alert-checking*	(Optional) Specifies whether router alert checking is required. • **1** — Force (true) • **2** — Don't force (false)
filter-id *filter-id*	(Optional) Assigns an input filter to the VLAN. Specify the filter ID of the input filter. You can apply only one input filter to a VLAN. You can, however, apply an input filter to more than one VLAN.
filter-status	If you assign an input filter to the VLAN, you must enable the input filter for the filter to take effect. • enable — Enable the input filter assigned to the VLAN • disable — Disable the input filter assigned to the VLAN

Defaults

You must specify at least one optional parameter.

- **query-interval** = 125
- **igmp-version** = 2
- **max-resp-time** = 10
- **robustness** = 2
- **last-mem-int** = 10
- **fast-leave** = 2 (disabled)
- **rtr-alert-checking** = 1 (true)
- **filter-status** = disable

Mode

All command modes.

Examples

This example shows how to set the IGMP query interval time to 250 seconds on VLAN 1:

```
S Chassis(rw)->set igmp config 1 query-interval 250
```

This example shows how to assign input filter 1 and enable it on VLAN 10:

```
S Chassis(rw)->set igmp config 10 filter-id 1 filter-status enable
```

show igmp counters

Use this command to display IGMP counter information.

Syntax

show igmp counters

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the IGMP counters:

```
S Chassis(su)->show igmp counters
IGMP Counters:
 Group Table is Full                 : false
 Version 1 Queries Tx                : 0
 Version 2 Queries Tx                : 0
 Version 3 Queries Tx                : 0
 Group Specific Queries Tx           : 0
 Group and Source Specific Queries Tx: 0
 Version 1 Queries Rx                : 0
 Version 2 Queries Rx                : 0
 Version 3 Queries Rx                : 0
 Version 1 Joins Rx                  : 0
 Version 2 Joins Rx                  : 0
 Version 3 Joins Rx                  : 0
 Leave Groups Rx                     : 0
 Bad Frames Rx                       : 0
```

clear igmp counters

Use this command to clear IGMP counter information.

Syntax

clear igmp counters

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear the IGMP counters:

```
S Chassis(rw)->clear igmp counters
```

set igmp delete

Use this command to remove all IGMP configuration settings for one or more VLANs.

Syntax

set igmp delete *vlan-list*

Parameters

vlan-list	Specifies the VLAN(s) on which all IGMP configuration settings will be cleared.

Defaults

None.

Mode

All command modes.

Example

This example shows how to remove IGMP configuration settings from VLANs 13, 23, and 999:

```
S Chassis(su)->set igmp delete 13,23,999
```

show igmp flows

Use this command to display IGMP flow information.

Syntax

show igmp flows [**portlist** *portlist*] [**group** *group*] [**vlan-list** *vlan-list*] [**sip** *sip*]

Parameters

portlist *portlist*	(Optional) Port or range of ports.
group *group*	(Optional) Group IP address (none means show all groups)
vlan-list *vlan-list*	(Optional) VLAN ID or range of IDs (1-4094)
sip *sip*	(Optional) Source IP address (none means show all sips)

Defaults

If no parameters are specified, information for all IGMP flows is displayed.

Mode

All command modes.

Example

This example shows how to display all the IGMP flow information:

```
S Chassis(rw)->show igmp flows
 Multicast Flows
--------------------------------------------------------------------------------
Port = ge.1.1
Multicast Group Address = 224.1.1.1
Vlan Id                 = 1010
Source IP Address       = 192.168.101.10

Port = ge.1.2
Multicast Group Address = 224.1.1.1
Vlan Id                 = 1020
Source IP Address       = 192.168.102.10

Port = ge.1.21
Multicast Group Address = 224.1.1.1
Vlan Id                 = 13
Source IP Address       = 20.1.1.10

Port = ge.1.21
Multicast Group Address = 224.1.1.1
Vlan Id                 = 13
Source IP Address       = 30.1.1.10

Port = ge.1.21
Multicast Group Address = 224.1.1.1
Vlan Id                 = 13
Source IP Address       = 40.1.1.10

Port = ge.1.21
Multicast Group Address = 224.1.1.1
Vlan Id                 = 13
Source IP Address       = 110.1.1.10
```

show igmp flow-full-action

Use this command to show what action to take with multicast frames when the number of unique multicast flows exceeds the number of supported flows.

Syntax

```
show igmp flow-full-action
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the action taken for multicast frames when the number of supported multicast flows is exceeded:

```
S Chassis(rw)->show igmp flow-full-action
Flow Table Full Action: Flood to Vlan
```

set igmp flow-full-action

Use this command to determine what action to take when the number of unique multicast flows exceeds the number of supported flows.

Syntax

set igmp flow-full-action *action*

Parameters

action	Specifies the action to take when the multicast group table is full. The options are: • **1** — Send multicast frames to Routers • **2** — Flood multicast frames to the VLAN

Defaults

Flood multicast frames to the VLAN.

Mode

All command modes.

Usage

This command specifies one of two supported actions to take when the multicast group table is full. If **1** is specified, the firmware forwards multicast frames to routers. If **2** is specified, the firmware floods multicast frames to the VLAN.

The group table full frame action feature setting is applied to both IGMP and MLD regardless of which protocol it is set in.

Example

This example shows how to flood multicast frames to the VLAN when the multicast flow table is full:

```
S Chassis(rw)->set igmp flow-full-action 2
```

show igmp groups

Use this command to display information about IGMP groups known to one or more VLANs.

Syntax

show igmp groups [**group** *group*] [**vlan-list** *vlan-list*] [**sip** *sip*] [**-verbose**]

Parameters

group *group*	(Optional) Group IP address. Entering no IP address shows all groups.
vlan-list *vlan-list*	(Optional) Specifies the VLAN(s) for which to display IGMP group information.
sip *sip*	(Optional) Specifies the source IP address. Entering no source IP address.
-verbose	(Optional) Show verbose display.

Defaults

If you do not specify an optional parameter, the output displays information for all IGMP groups.

Mode

All command modes.

Example

This example shows how to display IGMP group information for group IP address **224.1.1.1**, source IP address **192.168.201.10**:

```
S Chassis(su)->show igmp groups groups
================================================================
Group IP Address     224.11.1.1
VLAN                 20

   Ports In Filter Mode Exclude   none.
   Ports In Filter Mode Include   none.

   0.   Source IP Address         Any
```

```
        Forwarding Ports          none.
        Non-Forwarding Ports      none.
   ----------------------------------------------------------------
   1.   Source IP Address         20.1.2.81
        Source Port               fe.3.48
        Forwarding Ports          none.
        Non-Forwarding Ports      none.
   ----------------------------------------------------------------
==================================================================
Group IP Address     224.12.1.1
VLAN                 20

   Ports In Filter Mode Exclude   none.
   Ports In Filter Mode Include   none.

   0.   Source IP Address         Any
        Forwarding Ports          none.
        Non-Forwarding Ports      none.
   ----------------------------------------------------------------
   1.   Source IP Address         20.1.2.5
        Source Port               fe.1.48
        Forwarding Ports          none.
        Non-Forwarding Ports      none.
   ----------------------------------------------------------------
==================================================================
Group IP Address     224.14.1.1
VLAN                 20

   Ports In Filter Mode Exclude   none.
   Ports In Filter Mode Include   none.

   0.   Source IP Address         Any
        Forwarding Ports          none.
        Non-Forwarding Ports      none.
   ----------------------------------------------------------------
   1.   Source IP Address         20.1.2.7
        Source Port               lag.0.4
        Forwarding Ports          none.
        Non-Forwarding Ports      none.
   ----------------------------------------------------------------
.
.
.
14 entries displayed (9 S,G, 5 *,G)
```

set igmp input-filter

Use this command to create an input filter to apply to the VLAN.

Syntax

```
set igmp input-filter filter-id rule-id start-ip ip-address end-ip ip-address
protocol-action {deny | allow} flow-action {drop | flood | allow}
```

Parameters

filter-id	The ID of the filter. You can create up to 16 IGMP input filters. Each filter must have a unique ID. Possible values are 1–16.
rule-id	The ID of a rule associated with the input filter. The rule ID sets the order in which multiple rules check incoming packets. You can create up to eight rules for each input filter. Each rule must have a unique ID. Possible values are 1–8.
start-ip *ip-address*	The starting IP address of the rule's IP address range
end-ip *ip-address*	The ending IP address of the rule's IP address range
protocol-action	The response to protocols in packets that match a rule's IP address range: • deny — Deny packets matching this rule • allow — Allow packets matching this rule
flow-action	The response to flows in packets that match a rule's IP address range: • drop — Drop packets matching this rule • flood — Flood packets matching this rule • allow — Allow packets matching this rule

Defaults

None.

Mode

All command modes.

Usage

IGMP will check all incoming packets received from the range of IP addresses specified in the filter's rules. The protocol action and flow action occur when an incoming packet matches an IP address range. If an incoming packet matches a rule's address range, the other rules in the filter are not checked.

To activate the filter, you must assign the filter to a VLAN and enable the filter. For more information, see "set igmp config" on page 62-5.

Example

This example shows how to create a filter that will block all multicast flows received by 239.255.255.250.

```
S Chassis(su)->set igmp input-filter 1 1 start-ip 239.255.255.250 end-ip
239.255.255.250 protocol-action allow flow-action drop
```

show igmp input-filter

Use this command to display configuration information for input filters.

Syntax

show igmp input-filter [*filter-id*] [*rule-id*]

Parameters

filter-id	The ID of the filter that you want to display. Possible values are 1–16.
rule-id	The ID of the rule that you want to display. Possible values are 1–8.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to display configuration information for all input filters:

```
S Chassis(su)->show igmp input-filter
Filter  Rule              StartIP               EndIP     ProtocolAction    FlowAction    HitCounter
  1     1               224.10.1.1              224.10.1.2     Allow            Allow            0
  1     2               224.10.1.5              224.10.1.7      Deny             Drop            0
```

This example shows how to display the configuration information for input filter 1 rule 1:

```
S Chassis(su)->show igmp input-filter 1 1
Igmp Input Filter
------------------------
Filter Id      :  1
Rule Id        :  1
Start IP       :  224.10.1.1
End IP         :  224.10.1.2
Protocol Action:  Allow
Flow Action    :  Allow
Hit Counter    :  0
```

clear igmp input-filter

Use this command to clear an input filter.

Syntax

```
clear igmp input-filter filter-id [rule-id]
```

Parameters

filter-id	The ID of the filter that you want to clear. Possible values are 1–16.
rule-id	The ID of the rule that you want to clear. Possible values are 1–8.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear input filter 1 rule 1.

```
S Chassis(su)->clear igmp input-filter 1 1
```

show igmp number-flows

Use this command to display the number of multicast groups supported by the S-Series device.

Syntax

show igmp number-flows

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

The command displays the number of active multicast groups supported by the device.

Example

This example shows how to display the number of multicast groups supported by the device:

```
S Chassis(su)->show igmp number-flows
IGMP current number of flows(default) = 16331
S Chassis(su)->
```

show igmp portFastLeave

Use this command to show the IGMP fast leave state for one or more ports.

Syntax

show igmp portFastLeave *port-list*

Parameters

port-list	Specifies the ports for which to display fast leave state.

Defaults

None

Mode

All command modes.

Example

This example shows how to display fast leave information for ports ge.1.1 and ge.1.2:

```
S Chassis(su)->show igmp portFastLeave ge.1.1-2
Port Fast Leave Table

Port Number      Fast Leave State
-------------------------
ge.1.1           Disabled
ge.1.2           Disabled
```

set igmp portFastLeave

Use this command to enable fast leave on one or more ports.

Syntax

set igmp portFastLeave *port-list*

Parameters

port-list	Specifies the ports on which to enable fast leave.

Defaults

Fast leave is disabled by default.

Mode

All command modes.

Example

This example shows how to enable fast leave on ports ge.1.1 and ge.1.2:

```
S Chassis(rw)->set igmp portFastLeave ge.1.1-2
```

clear igmp portFastLeave

Use this command to disable fast leave on one or more ports.

Syntax

clear igmp portFastLeave *port-list*

Parameters

port-list	Specifies the ports on which to disable fast leave.

Defaults

None

Mode

All command modes.

Example

This example shows how to disable fast leave on ports ge.1.1 and ge.1.2:

```
S Chassis(rw)->clear igmp portFastLeave ge.1.1-2
```

show igmp protocols

Use this command to display the binding of IP protocol id to IGMP classification.

Syntax

show igmp protocols

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the binding of IP protocol id to IGMP classification:

```
S Chassis(rw)->show igmp protocols
Protocol Classifications

Protocol Ids set to Mcast Data
17

Protocol Ids set to routing Protocol
3,7-9,42-43,45,47-48,85-86,88-89,91-92,100,103,112

Protocol Ids set to Ignore
0,4-6,10-16,18-41,44,46,49-84,87,90,93-99,101-102,104-111,113-255
```

set igmp protocols

Use this command to change how IGMP handles received IP frames for a particular protocol.

Syntax

set igmp protocols {**classification** *classification}* {**protocol-id** *protocol-id}* [**modify**]

Parameters

classification *classification*	Specifies the classification. Options are: **1** — Multicast data. IGMP forwards these protocol frames to IGMP joined clients. **2** — Routing protocol. IGMP treats these protocol frames as routing protocols. **3** — Ignore. IGMP ignores these frames.
protocol-id *protocol-id*	The IP protocol ID or range of IDs to change (3–57,59–255).
modify	(Optional) Add to existing classifications. If not used, protocols will be overwritten.

Defaults

If **modify** is not specified, protocols will be overwritten.

Mode

All command modes.

Usage

The protocol feature setting is applied to both IGMP and MLD regardless of which protocol it is set in.

Example

This example shows how to classify TCP frames, identified by protocol ID 6, as multicast data:

```
S Chassis(rw)->set igmp protocols classification 1 protocol-id 6 modify
```

clear igmp protocols

Use this command to clear the current IGMP classification setting of an IP protocol ID and return the IP protocol to its default IGMP classification.

Syntax

clear igmp protocols {**protocol-id** *protocol-id}*

Parameters

protocol-id *protocol-id*	The IP protocol ID or range of IDs to change (3–57,59–255).

Defaults

None.

Mode

All command modes.

Usage

This command clears the IGMP classification setting of a specified IP protocol or all IP protocols and returns the IP protocol to its default IGMP classification as follows:

- Multicast data is the default IGMP classification for IP protocol **17**.
- Routing protocol is the default IGMP classification for IP protocols **3**, **7** - **9**, **42** - **43**, **45**, **47** - **48**, **85** - **86**, **88** - **89**, **91** - **92**, **100**, **103**, **112**.
- Ignore is the default IGMP classification for IP protocols **4** - **6**, **10** - **16**, **18** - **41**, **44**, **46**, **49** - **57**, **59** - **84**, **87**, **90**, **93** - **99**, **101** - **102**, **104** - **111**, **113** - **255**.

Example

This example shows how to return TCP frames, identified by protocol ID 6, to their default IGMP classification (ignore):

```
S Chassis(rw)->clear igmp protocols protocol-id 6 modify
```

show igmp query

Use this command to display the IGMP query status of one or more VLANs.

Syntax

show igmp query *vlan-list*

Parameters

vlan-list	Specifies the VLAN(s) for which to display IGMP query state.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the IGMP query state for VLAN 1:

```
S Chassis(rw)->show igmp query 1
IGMP Vlans Query Enabled : 1
```

set igmp query-enable

Use this command to enable IGMP querying on one or more VLANs.

Syntax

set igmp query-enable *vlan-list*

Parameters

vlan-list	Specifies the VLAN(s) on which to enable IGMP querying.

Defaults

None.

Mode

All command modes.

Example

This example shows how to enable IGMP querying on VLAN 104:

```
S Chassis(rw)->set igmp query-enable 104
```

set igmp query-disable

Use this command to disable IGMP querying on one or more VLANs.

Syntax

set igmp query-disable *vlan-list*

Parameters

vlan-list	Specifies the VLAN(s) on which to disable IGMP querying.

Defaults

None.

Mode

All command modes.

Example

This example shows how to disable IGMP querying on VLAN 104:

```
S Chassis(rw)->set igmp query-disable 104
```

show igmp reporters

Use this command to display IGMP reporter information.

Syntax

show igmp reporters [**portlist** *portlist*] [**group** *group*] [**vlan-list** *vlan-list*] [**sip** *sip*]

Parameters

portlist *portlist*	(Optional) Port or range of ports.
group *group*	(Optional) Group IP address (none means show all groups)
vlan-list *vlan-list*	(Optional) VLAN ID or range of IDs (1-4094)
sip *sip*	(Optional) Source IP address (none means show all sips)

Defaults

If no parameters are specified, all IGMP reporter information is displayed.

Mode

All command modes.

Example

This example shows how to display the all IGMP reporter information:

```
S Chassis(rw)->show igmp reporters
IGMP Reporters
--------------------------------------------------------------------------------
Port = ge.1.1
Multicast Group Address = 224.1.1.1
Vlan Id                 = 2501
Source IP Address       = Any
Expire Time(Sec)        = 258
Port Mode               = Exclude

Port = ge.1.1
Multicast Group Address = 239.1.1.1
Vlan Id                 = 2501
Source IP Address       = Any
Expire Time(Sec)        = 258
Port Mode               = Exclude

2 entries displayed
S Chassis(rw)->
```

show igmp static

Use this command to display all static IGMP entries or static IGMP entries for the specified IGMP group.

Syntax

show igmp static [**group** *group*] [**vlan-list** *vlan-list*]

Parameters

group *group*	(Optional) Specifies a group IP address.
vlan-list *vlan-list*	(Optional) Specifies the VLAN(s) for which to display static IGMP information.

Defaults

If not specified, static IGMP information will be displayed for all groups and VLANs.

Mode

All command modes.

Example

This example shows how to display static IGMP information for group **10.10.50.1** and VLAN **100**:

```
S Chassis(rw)->set igmp static 10.10.50.1 100 include-ports tg.1.1-5 exclude-ports
tg.1.6-10
S Chassis(rw)->show igmp static group 10.10.50.1 vlan-list 100
--------------------------------------------------------------------------------
Multicast Group Address = 10.10.50.1
Vlan Id                 = 100
Source IP Address       = Any
Include List            = tg.1.1-5
Exclude List            = tg.1.6-10
S Chassis(rw)->
```

set igmp static

Use this command to create a new static IGMP entry or to add one or more new include or exclude ports to an existing entry.

Syntax

set igmp static *group vlan-list* [**modify**] [**include-ports** *include-ports*] [**exclude-ports** *exclude-ports*]

Parameters

group	Specifies a group IP address for the entry.
vlan-list	Specifies the VLAN or range of VLANs for which to configure the entry.
modify	(Optional) Adds new ports to an existing entry.

include-ports *include-ports*	(Optional) Port or range of ports to include for this static entry.
exclude-ports *exclude-ports*	(Optional) Port or range of ports to exclude from both this static entry and dynamic IGMP.

Defaults

If the **modify** option is not specified, any previous configuration for this group and vlan is overwritten.

If the **include-ports** option is not specified, all ports that are not specifically excluded using the exclude-ports option are included in this entry.

If the **exclude-ports** option is not specified, no ports are excluded for this entry.

Mode

All command modes.

Usage

If the receiving system is not IGMP capable, a static IGMP entry configured with the receiving device's IP address (group address) and VLAN will force the sending of IGMP messages to the device.

If **include-ports** is specified, only ports in the include list will be members of this static IGMP entry.

If **exclude-ports** is specified, both static and dynamic IGMP messages will be blocked for the excluded ports.

Example

This example shows how to create a static IGMP entry for group 10.10.50.1 on VLAN 100 including ports tg.1.1-5 and excluding ports tg.1.6-10:

```
S Chassis(rw)->set igmp static 10.10.50.1 100 include-ports tg.1.1-5 exclude-ports
tg.1.6-10
S Chassis(rw)->show igmp static group 10.10.50.1 vlan-list 100
--------------------------------------------------------------------------------
Multicast Group Address = 10.10.50.1
Vlan Id                 = 100
Source IP Address       = Any
Include List            = tg.1.1-5
Exclude List            = tg.1.6-10
S Chassis(rw)->
```

clear igmp static

Use this command to delete a static IGMP entry, or to remove one or more ports from an existing entry.

Syntax

clear igmp static *group vlan-list* [**modify**] [**include-ports**] [**exclude-ports**]

Parameters

group	Specifies a group IP address for the entry.
vlan-list	Specifies the VLAN(s) on which to configure the entry.
modify	(Optional) Removes ports from an existing entry.
include-ports	(Optional) Port or range of ports in the include-ports list to be removed from this entry.
exclude-ports	(Optional) Port or range of ports in the exclude-ports list to be removed from this entry.

Defaults

If the **modify** option is not specified, all configuration for this entry is removed.

If the **include-ports** option is not specified, all members of the include-ports list are removed for this option.

If the **exclude-ports** option is not specified, all members of the exclude-ports list are removed for this option.

Mode

All command modes.

Usage

You must include the **modify** option when removing a part of the entry configuration using the **include-ports** or **exclude-ports** option.

Examples

This example shows how to remove port tg.1.5 from the IGMP group at 10.10.50.1 (VLAN 100) leaving the remaining configuration unchanged:

```
S Chassis(rw)->show igmp static
--------------------------------------------------------------------------------
Multicast Group Address = 10.10.50.1
Vlan Id                 = 100
Source IP Address       = Any
Include List            = tg.1.1-5
Exclude List            = tg.1.6-10
S Chassis(rw)->clear igmp static 10.10.50.1 100 modify include-ports tg.1.5
S Chassis(rw)->show igmp static
--------------------------------------------------------------------------------
Multicast Group Address = 10.10.50.1
Vlan Id                 = 100
Source IP Address       = Any
Include List            = tg.1.1-4
Exclude List            = tg.1.6-10
S Chassis(rw)->
```

This example shows how to remove the static IGMP entry for IGMP group at 10.10.50.1 on VLAN 100:

```
S Chassis(rw)->clear igmp static group 10.10.50.1 vlan-list 100
```

set igmp unknown-input-action

Use this command to set the action taken when the first few frames of a multicast stream are received (that is, before the stream is added to the IGMP database).

Syntax

```
set igmp unknown-input-action {routers | flood | discard}
```

Parameters

routers	Send the frames of the multicast stream to all known multicast routers
flood	Flood the frames of the multicast stream to the VLAN on which the stream was received. This is the default value.
discard	Discard the frames of the multicast stream.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the unknown input action to discard the frames of multicast streams.

```
S Chassis(su)->set igmp unknown-input-action discard
```

show igmp unknown-input-action

Use this command to display the action taken when the first frames of a multicast stream are received.

Syntax

```
show igmp unknown-input-action
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the currently configured unknown input action.

```
S Chassis(su)->show igmp unknown-input-action
Unknown Input Action: Flood to Vlan
```

show igmp vlan

Use this command to display IGMP information for a specific VLAN.

Syntax

show igmp vlan [*vlan-list*]

Parameters

vlan-list	(Optional) Show IGMP info for the specified VLAN only.

Defaults

If a VLAN is not specified, information for all VLANs are displayed.

Mode

All command modes.

Example

This example shows how to display igmp information for VLAN 12:

```
S Chassis(rw)->show igmp vlan 12
--------------------------------------------------------------------------------
IGMP Vlan 12 Info
Querying                    - Enabled
QueryInterval(sec.)         - 125
Status                      - Active
Version                     - 2
QueryMaxResponseTime(sec.)  - 10
Robustness                  - 2
LastMemberQueryIntvl(sec.)  - 1
FastLeaveState              - Disabled
QuerierUpTime               - 0 D  4 H  42 M  18 S
QuerierExpiryTime           - 0 D  0 H  0 M  0 S
QuerierIP                   - 192.168.104.3
Router(s) seen on ports     - none.
Router Ports Egressing      - none.
```

63

Multicast Listener Discovery (MLD) Commands

This chapter describes Multicast Listener Discovery (MLD) commands and how to configure them. For information about configuring MLD, refer to the Multicast Configuration chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
set mld enable	63-2
show mld enable	63-2
set mld disable	63-3
set mld delete	63-3
set mld config	63-4
show mld config	63-5
show mld counters	63-6
clear mld counters	63-7
set mld query-enable	63-7
set mld query-disable	63-8
show mld query	63-8
set mld flow-full-action	63-9
show mld flow-full-action	63-10
set mld input-filter	63-12
show mld input-filter	63-13
clear mld input-filter	63-14
set mld static	63-14
clear mld static	63-15
set mld protocols	63-15
clear mld protocols	63-16
show mld protocols	63-17
set mld portFastLeave	63-17
clear mld portFastLeave	63-18
show mld portFastLeave	63-19
show mld number-flows	63-19

For information about...	Refer to page...
show mld vlan	63-20
show mld groups	63-20
show mld static	63-23
show mld reporters	63-23
show mld flows	63-24
set mld unknown-input-action	63-25
show mld unknown-input-action	63-26

set mld enable

Use this command to enable MLD on one or more VLANs.

Syntax

set mld enable *vlan-list*

Parameters

vlan-list	Enables MLD on the specified VLAN(s). Valid values are **1 – 4094**.

Defaults

None.

Mode

All command modes.

Usage

Multiple VLANs can be specified delineated by a comma or as a range delineated by a hyphen.

Example

This example shows how to enable MLD on VLAN 104, 106, and 108 through 109:

```
S Chassis(rw)->set mld enable 104,106,108-109
S Chassis(rw)->
```

show mld enable

Use this command to display the status of MLD on one or more VLAN(s).

Syntax

show mld enable [*vlan-list*]

Parameters

vlan-list	(Optional) Displays the MLD status for the specified VLAN or range of IDs. Valid values are **1 – 4094**.

Defaults

If *vlan-list* is not specified, all enabled VLANs display.

Mode

All command modes.

Example

This example displays all MLD enabled VLANs on the device:

```
S Chassis(rw)->show mld enable
MLD Vlans Enabled :2501-2504,3001,3014
S Chassis(rw)->
```

set mld disable

Use this command to disable MLD on one or more VLANs.

Syntax

set mld disable *vlan-list*

Parameters

vlan-list	Disables MLD on the specified VLAN(s). Valid values are **1 – 4094**.

Defaults

None.

Mode

All command modes.

Example

This example shows how to disable MLD on VLAN 104:

```
S Chassis(rw)->set mld enable 104
S Chassis(rw)->
```

set mld delete

Use this command to remove MLD configuration settings for one or more VLANs.

Syntax

set mld delete *vlan-list*

Parameters

vlan-list	Removes the MLD configuration settings from the specified VLAN(s). Valid values are **1 – 4094**.

Defaults

None.

Mode

All command modes.

Example

This example shows how to remove the MLD configuration settings on VLAN 104:

```
S Chassis(rw)->set mld delete 104
S Chassis(rw)->
```

set mld config

Use this command to set VLAN configuration parameters.

Syntax

set mld config *vlan-list* { [**query-interval** *query-interval*] [**mld-version** *mld-version*] [**max-resp-time** *max-resp-time*] [**robustness** *robustness*] [**last-mem-int** *last-mem-int*] [**fast-leave** *fast-leave*] [**filter-id** *filter-id*] [**filter-status** {enable | disable}]}

Parameters

vlan-list	Applies this configuration to the specified VLAN(s). Valid values are **1 – 4094**.
query-interval *query-interval*	(Optional) Specifies the interval between the sending of host query messages by this device. Valid values are **1 – 31744** seconds. The default value is **125** seconds.
mld-version *mld-version*	(Optional) Specifies the MLD version: • **1**— MLDv1 • **2**— MLDv2 (default)
max-resp-time *max-resp-time*	(Optional) Specifies the maximum response time advertised in MLD query messages. Valid values are **1** - **25** seconds for MLDv1 and **1 – 3174** seconds for MLDv2. Default value is **10** seconds.
robustness *robustness*	(Optional) Specifies the robustness value which accounts for expected packet loss on a link. If a link is expected to be lossy, the robustness value may be increased. Valid values are **2 – 255**. Default value is **2**.
last-mem-int *last-mem-int*	(Optional) Specifies the last member interval which is the length of time that must pass before a router decides that there is no longer another router which should be the querier on a link. This value is normally set to the robustness value times the query interval, plus one half of one maximum response time. Valid values are **1** - **255** seconds for MLDv1 and **1 – 3174** seconds for MLDv2. Default value is **10** seconds.

fast-leave *fast-leave*	(Optional) Sets the VLANs fast leave state. Valid values are **1** for enable or **2** for disable. Default value is **2**.
filter-id *filter-id*	(Optional) Assigns an input filter to the VLAN. Specify the filter ID of the input filter. You can apply only one input filter to a VLAN. You can, however, apply an input filter to more than one VLAN.
filter-status	If you assign an input filter to the VLAN, you must enable the input filter for the filter to take effect. • enable — Enable the input filter assigned to the VLAN • disable — Disable the input filter assigned to the VLAN

Defaults

At least one optional parameter must be entered.

If not specified:

- *query-interval* defaults to 125 seconds
- *mld-version* defaults to MLDv2
- *max-resp-time* defaults to 10 seconds
- *robustness* defaults to 2
- *last-mem-int* defaults to 10 seconds
- *fast-leave* defaults to 2 (disabled)
- *filter-status* defaults to disable

Mode

All command modes.

Usage

The maximum response time is used to tune the burstiness of MLD messages on the link. Larger values make the traffic less bursty, as host responses are spread out over a larger interval. The maximum response time must be less than the query interval.

Example

This example shows how to set the query interval on VLAN 104 to 150 seconds:

```
S Chassis(rw)->set mld config 104 query-interval 150
S Chassis(rw)->
```

show mld config

Use this command to show the MLD configuration information for one or more VLANs.

Syntax

show mld config [*vlan-list*]

Parameters

vlan-list	(Optional) Displays the MLD configuration information for the specified VLAN(s). Valid values are **1** – **4094**.

Defaults

If a *vlan-list* is not specified, all MLD configured VLANs display.

Mode

All command modes.

Example

This example displays the MLD configuration settings for VLAN 2501:

```
S Chassis(rw)->show mld config 2501

MLD config for vlan 2501
-----------------------------------
QueryInterval(sec.)         - 125
Status                      - Active
Version                     - 2
QueryMaxResponseTime(sec.)  - 10
Robustness                  - 2
LastMemberQueryIntvl        - 10
FastLeaveState              - Disabled
QuerierUpTime               - 0 D  22 H  31 M  25 S
QuerierExpiryTime           - 0 D  0 H  0 M  0 S
QuerierIP                   - fe80::21f:45ff:fe5b:f5cf
S Chassis(rw)->
```

show mld counters

Use this command to display MLD counters.

Syntax

show mld counters

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

```
S Chassis(rw)->show mld counters
MLD Counters:
 Flow Table is Full                  : false
 Version 1 Queries Tx                : 0
 Version 2 Queries Tx                : 132
 Group Specific Queries Tx           : 0
 Group and Source Specific Queries Tx: 0
 Version 1 Queries Rx                : 0
 Version 2 Queries Rx                : 0
 Wrong Version Queries Rx            : 0
 Version 1 Joins Rx                  : 132
 Version 2 Joins Rx                  : 89
 Leave Groups Rx                     : 0
 Bad Frames Rx                       : 140
S Chassis(rw)->
```

clear mld counters

Use this command to clear MLD display counters.

Syntax

clear mld counters

Parameters

None

Defaults

None.

Mode

All command modes.

Example

```
S Chassis(rw)->clear mld counters
S Chassis(rw)->
```

set mld query-enable

Use this command to enable MLD querying on one or more VLANs.

Syntax

set mld query-enable *vlan-list*

Parameters

vlan-list	Enables MLD querying for the specified VLAN(s). Valid values are **1** – **4094**.

Defaults

None.

Mode

All command modes.

Example

This example shows how to enable MLD querying on VLAN 104 through 107:

```
S Chassis(rw)->set mld query-enable 104-107
```

set mld query-disable

Use this command to disable MLD querying on one or more VLANs.

Syntax

set mld query-disable *vlan-list*

Parameters

vlan-list	Disables MLD querying on the specified VLAN(s). Valid values are **1** – **4094**.

Defaults

None.

Mode

All command modes.

Example

This example shows how to disable MLD querying on VLAN 104 through 107:

```
S Chassis(rw)->set mld query-disable 104-107
```

show mld query

Use this command to show the MLD query status of one or more VLANs.

Syntax

show mld query [*vlan-list*]

Parameters

vlan-list	(Optional) VLAN ID or range of IDs. Valid values are **1 – 4094**.

Defaults

If *vlan-list* is not specified, the command output displays MLD query status for all VLANs.

Mode

All command modes.

Example

This example displays the MLD query status for VLAN 2501:

```
S Chassis(rw)->show mld query 2501
MLD Vlans Query Enabled :2501
S Chassis(rw)->
```

set mld flow-full-action

Use this command to set the frame action if the flow table is full.

Syntax

```
set mld flow-full-action {1 | 2}
```

Parameters

1	Specifies that frames are sent to routers if the flow table is full.
2	Specifies that frames are flooded on VLANs (default) if the flow table is full.

Defaults

None.

Mode

All command modes.

Usage

This command specifies one of two supported actions to take when the multicast flow table is full. If **1** is specified, the firwmare forwards multicast frames to routers. If **2** is specified, the firmware floods multicast frames to the VLAN.

The flow table full frame action setting is applied to both IGMP and MLD regardless of which protocol it is set in.

Example

This example shows how to set the flow full action to send to routers:

```
S Chassis(rw)->set mld flow-full-action 1
```

show mld flow-full-action

Use this command to show what action to take with multicast frames when the multicast flow table is full.

Syntax

show mld flow-full-action

Defaults

None.

Mode

All command modes.

Example

```
S Chassis(su)->show mld flow-full-action
Flow Table Full Action: Flood to Vlan
```

show igmp groups

Use this command to display information about IGMP groups known to one or more VLANs.

Syntax

show igmp groups [**group** *group*] [**vlan-list** *vlan-list*] [**sip** *sip*] [**-verbose**]

Parameters

group *group*	(Optional) Group IP address. Entering no IP address shows all groups.
vlan-list *vlan-list*	(Optional) Specifies the VLAN(s) for which to display IGMP group information.
sip *sip*	(Optional) Specifies the source IP address. Entering no source IP address.
-verbose	(Optional) Show verbose display.

Defaults

If you do not specify an optional parameter, the output displays information for all IGMP groups.

Mode

All command modes.

Example

This example shows how to display IGMP group information for group IP address **224.1.1.1**, source IP address **192.168.201.10**:

```
S Chassis(su)->show igmp groups groups
==========================================================================
Group IP Address     224.11.1.1
VLAN                 20

   Ports In Filter Mode Exclude   none.
   Ports In Filter Mode Include   none.

   0.   Source IP Address         Any
        Forwarding Ports          none.
        Non-Forwarding Ports      none.
   --------------------------------------------------------------
   1.   Source IP Address         20.1.2.81
        Source Port               fe.3.48
        Forwarding Ports          none.
        Non-Forwarding Ports      none.
   --------------------------------------------------------------
==========================================================================
Group IP Address     224.12.1.1
VLAN                 20

   Ports In Filter Mode Exclude   none.
   Ports In Filter Mode Include   none.

   0.   Source IP Address         Any
        Forwarding Ports          none.
        Non-Forwarding Ports      none.
   --------------------------------------------------------------
   1.   Source IP Address         20.1.2.5
        Source Port               fe.1.48
        Forwarding Ports          none.
        Non-Forwarding Ports      none.
   --------------------------------------------------------------
==========================================================================
Group IP Address     224.14.1.1
VLAN                 20

   Ports In Filter Mode Exclude   none.
   Ports In Filter Mode Include   none.

   0.   Source IP Address         Any
```

```
        Forwarding Ports          none.
        Non-Forwarding Ports      none.
   ------------------------------------------------------------
   1.   Source IP Address         20.1.2.7
        Source Port               lag.0.4
        Forwarding Ports          none.
        Non-Forwarding Ports      none.
   ------------------------------------------------------------
.
.
.
14 entries displayed (9 S,G, 5 *,G)
```

set mld input-filter

Use this command to create an input filter to apply to the VLAN.

Syntax

set mld input-filter *filter-id rule-id* **start-ip** *ip-address* **end-ip** *ip-address* **protocol-action** {deny | allow} **flow-action** {drop | flood | allow}

Parameters

filter-id	The ID of the filter. You can create up to 16 MLD input filters. Each filter must have a unique ID. Possible values are 1–16.
rule-id	The ID of a rule associated with the input filter. The rule ID sets the order in which multiple rules check incoming packets. You can create up to eight rules for each input filter. Each rule must have a unique ID. Possible values are 1–8.
start-ip *ip-address*	The starting IP address of the rule's IP address range
end-ip *ip-address*	The ending IP address of the rule's IP address range
protocol-action	The response to protocols in packets that match a rule's IP address range: • deny — Deny packets matching this rule • allow — Allow packets matching this rule
flow-action	The response to flows in packets that match a rule's IP address range: • drop — Drop packets matching this rule • flood — Flood packets matching this rule • allow — Allow packets matching this rule

Defaults

None.

Mode

All command modes.

Usage

MLD will check all incoming packets received from the range of IP addresses specified in the filter's rules. The protocol action and flow action occur when an incoming packet matches an IP address range. If an incoming packet matches a rule's address range, the other rules in the filter are not checked.

To activate the filter, you must assign the filter to a VLAN and enable the filter. For more information, see "set mld config" on page 63-4.

Example

This example shows how to create a filter that will block all multicast flows received by 2001:11ac:fd34:3333:0:0:0:3.

```
S Chassis(su)->set mld input-filter 1 1 start-ip 2001:11ac:fd34:3333:0:0:0:3
end-ip 2001:11ac:fd34:3333:0:0:0:3 protocol-action allow flow-action drop
```

show mld input-filter

Use this command to display configuration information for input filters.

Syntax

show mld input-filter [*filter-id*] [*rule-id*]

Parameters

filter-id	The ID of the filter that you want to display. Possible values are 1–16.
rule-id	The ID of the rule that you want to display. Possible values are 1–8.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the configuration information for input filter 1 rule 1:

```
S Chassis(su)->show mld input-filter 1 1
MLD Input Filter
------------------------
Filter Id      :  1
Rule Id        :  1
Start IP       : 2001:11ac:fd34:3333:0:0:0:3
End IP         : 2001:11ac:fd34:3333:0:0:0:3
Protocol Action:  Allow
Flow Action    :  Allow
Hit Counter    :  0
```

clear mld input-filter

Use this command to clear an input filter.

Syntax

clear mld input-filter *filter-id* [*rule-id*]

Parameters

filter-id	The ID of the filter that you want to clear. Possible values are 1–16.
rule-id	The ID of the rule that you want to clear. Possible values are 1–8.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear input filter 1 rule 1.

```
S Chassis(su)->clear mld input-filter 1 1
```

set mld static

Use this command to add or modify a static MLD entry.

Syntax

set mld static *group-address vlan-list* [**modify** {[**include-ports** *include-ports*] [**exclude-ports** *exclude-ports*]}]

Parameters

group	Adds or modifies a static MDL entry for the specified Group IP address
vlan-list	Adds or modifies a static MDL entry for the specified VLAN ID or range of IDs. Valid values are **1 – 4094**.
modify	(Optional) Appends specified include or exclude ports to an existing MLD group.
include-ports *include-ports*	(Optional) Port or range of include ports to add to this static MLD group configuration.
exclude-ports *exclude-ports*	(Optional) Port or range of exclude ports to add to this static MLD group configuration.

Defaults

- If **modify** is not specified, the static entry will be created and overwrite any existing MLD group configuration for this group address.
- If **include-ports** is not specified, no include ports are added to the MLD group.
- If **exclude-ports** is not specified, no exclude ports are added to the MLD group.

Mode

All command modes, Read-Write.

Example

This example creates a new MLD static group on VLAN **1** with a group address of **ff33:abcd::1** and includes ports **ge.1.5** through **ge.1.8**:

```
S Chassis(rw)->set mld static ff33:abcd::1 1 include-ports ge.1.5-8
```

clear mld static

Use this command to delete a static MLD entry or to remove one or more ports from an existing entry.

Syntax

clear mld static *group-address vlan-list* [**modify** {[**include-ports** *include-ports*] [**exclude-ports** *exclude-ports*]}

Parameters

group	Deletes a static MLD entry for the specified multicast group IP address.
vlan-list	Deletes a static MLD entry for the specified VLAN(s). Valid values are **1 – 4094**.
modify	(Optional) Modifies the existing MLD static entry by removing specified ports.
include-ports *include-ports*	(Optional) Port or range of include ports to remove from this static MLD group configuration.
exclude-ports *exclude-ports*	(Optional) Port or range of exclude ports to remove from this static MLD group configuration.

Defaults

If no option is specified, the static entry will be deleted instead of modified.

Mode

All command modes.

Example

This example removes port ge.1.5 from the MLD static group on VLAN **1** with a group address of **ff33:abcd::1**:

```
S Chassis(rw)->clear mld static ff33:abcd::1 1 modify include-ports ge.1.5
```

set mld protocols

Use this command to set the MLD classification of received IP frames.

Syntax

set mld protocols classification *classification* **protocol-id** *protocol-id* [**modify**]

Parameters

classification	• **1** — Multicast data • **2** — Routing protocol • **3** — Ignore
protocol-id	The protocol IDs to add to the classification (3–57,59–255).
modify	(Optional) Add the specified protocol to the existing classification. If not used, protocols will be overwritten.

Defaults

If **modify** is not specified, existing protocols for the specified classification are overwritten.

Mode

All command modes.

Usage

When entering multiple protocols, delineate individual protocols using a comma (**,**) and a range of protocols using a hyphen (**-**).

Example

This example adds the IPv6 encapsulation (41) and IPv6 route (43) protocols to the MLD routing protocol classification list:

```
S Chassis(rw)->set mld protocols classification 2 protocol-id 41,43 modify
S Chassis(rw)->
```

clear mld protocols

Use this command to clear the binding of an IP protocol ID to MLD classification.

Syntax

clear mld protocols protocol-id *protocol-id*

Parameters

protocol-id *protocol-id*	The IP protocol IDs to clear. Valid values are 3–57,59–255.

Defaults

None.

Mode

All command modes.

Example

This example removes the IPv6 route (43) protocol from the MLD classification list:

```
S Chassis(rw)->clear mld protocols protocol-id 43
S Chassis(rw)->
```

show mld protocols

Use this command to display the binding of IP protocol ID to MLD classification.

Syntax

show mld protocols

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

The protocol setting is applied to both IGMP and MLD regardless of which protocol it is set in.

Example

This example shows how to display the protocol ID to MLD classification bindings for this device:

```
S Chassis(su)->show mld protocols
Protocol Classifications

Protocol Ids set to Mcast Data
17

Protocol Ids set to routing Protocol
3,7-9,42-43,45,47-48,85-86,88-89,91-92,100,103,112

Protocol Ids set to Ignore
4-6,10-16,18-41,44,46,49-57,59-84,87,90,93-99,101-102,104-111,113-255
S Chassis(su)->
```

set mld portFastLeave

Use this command to enable port fast leave on the specified port or range of ports.

Syntax

set mld portFastLeave *port-list*

Parameters

port-list	port ID or a range of port IDs.

Defaults

None.

Mode

All command modes.

Usage

Port fast leave is an MLD mechanism that immediately removes the layer 2 LAN interface from the forwarding table upon receiving an MLD done message for the multicast group without first sending out general queries to the interface. Enable MLD port fast leave only on ports with only one host connected. This prevents the inadvertent dropping of other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group.

The port fast leave setting is applied to both IGMP and MLD regardless of which protocol it is set in.

Example

This example enables the port fast leave feature on ports **ge.1.5-8**:

```
S Chassis(rw)->set mld portFastLeave ge.1.5-8
S Chassis(rw)->
```

clear mld portFastLeave

Use this command to disable port fast leave on the specified port or range of ports.

Syntax

clear mld portFastLeave *port-list*

Parameters

port-list	port ID or a range of port IDs.

Defaults

None.

Mode

All command modes.

Example

This example disables the port fast leave feature on port **ge.1.5**:

```
S Chassis(rw)->clear mld portFastLeave ge.1.5
S Chassis(rw)->
```

show mld portFastLeave

Use this command to show the MLD fast leave state for a specific VLAN.

Syntax

show mld fastleave *port-list*

Parameters

port-list	Specifies the port(s) for the display of MLD fast leave state.

Defaults

None

Mode

All command modes.

Example

This example displays the MLD fast leave state for port **ge.2.1**:

```
S Chassis(su)->show mld portFastLeave ge.2.1
Port Fast Leave Table

Port Number      Fast Leave State
--------------------------
ge.2.1           Disabled
```

show mld number-flows

Use this command to display the number of MLD flows set on the device.

Syntax

show mld number-flows

Parameters

None

Defaults

None.

Mode

All command modes.

Usage

This example displays the number of multicast flows set for the multicast flow table:

```
S Chassis(rw)->show mld number-flows
MLD current number of flows(default) = 8139
```

```
S Chassis(rw)->
```

show mld vlan

Use this command to show MLD information for the specified VLAN(s).

Syntax

show mld vlan [*vlan-list*]

Parameters

vlan-list	(Optional) VLAN ID or range of IDs. Valid values are **1 – 4094**.

Defaults

If *vlan-list* is not displayed, information for all VLANs are displayed.

Mode

All command modes.

Example

This example displays the MLD information for VLAN **2501**:

```
S Chassis(rw)->show mld vlan 2501
--------------------------------------------------------------------------------
MLD Vlan 2501 Info
Querying                    - Enabled
QueryInterval(sec.)         - 125
Status                      - Active
Version                     - 2
QueryMaxResponseTime(sec.)  - 10
Robustness                  - 2
LastMemberQueryIntvl        - 10
FastLeaveState              - Disabled
QuerierUpTime               - 1 D  1 H  17 M  19 S
QuerierExpiryTime           - 0 D  0 H  0 M  0 S
QuerierIP                   - fe80::21f:45ff:fe5b:f5cf
Router(s) seen on ports     - none.
Router Ports Egressing      - none.
```

show mld groups

Use this command to display information about MLD groups known to one or more VLANs.

Syntax

show mld groups [**group** *group*] [**vlan-list** *vlan-list*] [**sip** *sip*] [**-verbose**]

Parameters

group *group*	(Optional) Group address. You can display all groups by not specifying a group address.
vlan-list *vlan-list*	(Optional) VLAN ID or range of IDs. Valid values are **1 – 4094**.
sip *sip*	(Optional) Source IP address. Source IPv6 addresses are link local.
-verbose	(Optional) Show verbose display

Defaults

If no options are specified, a standard level of information displays for all MLD groups.

Mode

All command modes.

Example

This example displays MLD group information for all MLD groups on the device:

```
S Chassis(su)->show mld groups group ff04::1:1:1:1
==========================================================================
Group IP Address     ff04::1:1:1:1
VLAN                 2502

   Ports In Filter Mode Exclude   ge.1.26
   Ports In Filter Mode Include   none.

   0.   Source IP Address         Any
        Forwarding Ports          ge.1.26
        Non-Forwarding Ports      none.
   --------------------------------------------------------------
   1.   Source IP Address         2502::10
        Source Port               ge.1.26
        Forwarding Ports          none.
        Non-Forwarding Ports      none.
   --------------------------------------------------------------
   2.   Source IP Address         2503::10
        Source Interface          vlan.0.2503
        Forwarding Ports          none.
        Non-Forwarding Ports      none.
   --------------------------------------------------------------
   3.   Source IP Address         2504::10
        Source Interface          vlan.0.3001
        Forwarding Ports          none.
        Non-Forwarding Ports      none.
   --------------------------------------------------------------
==========================================================================
Group IP Address     ff04::1:1:1:1
```

```
VLAN                2503

   Ports In Filter Mode Exclude   ge.1.27
   Ports In Filter Mode Include   none.

   0.   Source IP Address         Any
        Forwarding Ports          ge.1.27
        Non-Forwarding Ports      none.
   ------------------------------------------------------------
   1.   Source IP Address         2502::10
        Source Interface          vlan.0.2502
        Forwarding Ports          none.
        Non-Forwarding Ports      none.
   ------------------------------------------------------------
   2.   Source IP Address         2503::10
        Source Port               ge.1.27
        Forwarding Ports          none.
        Non-Forwarding Ports      none.
   ------------------------------------------------------------
   3.   Source IP Address         2504::10
        Source Interface          vlan.0.3001
        Forwarding Ports          none.
        Non-Forwarding Ports      none.
   ------------------------------------------------------------
================================================================
Group IP Address     ff04::1:1:1:1
VLAN                 3001

   Ports In Filter Mode Exclude   none.
   Ports In Filter Mode Include   none.

   0.   Source IP Address         Any
        Forwarding Ports          none.
        Non-Forwarding Ports      none.
   ------------------------------------------------------------
   1.   Source IP Address         2502::10
        Source Interface          vlan.0.2502
        Forwarding Ports          none.
        Non-Forwarding Ports      none.
   ------------------------------------------------------------
   2.   Source IP Address         2503::10
        Source Interface          vlan.0.2503
        Forwarding Ports          none.
        Non-Forwarding Ports      none.
   ------------------------------------------------------------
```

```
   3.   Source IP Address         2504::10
        Source Port               ge.1.40
        Forwarding Ports          none.
        Non-Forwarding Ports      none.
   ------------------------------------------------------------

12 entries displayed (9 S,G, 3 *,G)
```

show mld static

Use this command to show static MLD entries for one or more VLANs or MLD groups.

Syntax

show mld static [**group** *group*] [**vlan-list** *vlan-list*]

Parameters

group *group*	(Optional) Group address. You can display all groups by not specifying a group address.
vlan-list *vlan-list*	(Optional) VLAN ID or range of IDs. Valid values are **1 – 4094**.

Defaults

If not specified, static MLD information will be displayed for all groups.

Mode

All command modes.

Example

This example displays static entries for group **ff3e:1:1:1**:

```
S Chassis(rw)->show mld static group ff3e:1:1:1
--------------------------------------------------------------------------------
Multicast Group Address = ff3e:1:1::1
Vlan Id                 = 77
Source IP Address       = Any
Include List            = ge.1.1
Exclude List            = ge.1.2
1 static entries displayed
S Chassis(rw)->
```

show mld reporters

Use this command to display MLD reporters.

Syntax

show mld reporters [**portlist** *portlist*] [**group** *group*] [**vlan-list** *vlan-list*] [**sip** *sip*]

Parameters

portlist *portlist*	(Optional) Specifies a port or range of ports
group *group*	(Optional) Multicast group IP address.
vlan-list *vlan-list*	(Optional) VLAN ID or range of IDs. Valid values are **1** – **4094**.
sip *sip*	(Optional) Source IP address. Enter **::** to display all source IP addresses.

Defaults

If no parameters are specified, all MLD reporters are displayed.

Mode

All command modes.

Usage

An MLD reporter is a host system that sends out MLD reports.

Example

This example displays MLD reporters for this device:

```
S Chassis(su)->show mld reporters
MLD Reporters
--------------------------------------------------------------------------------
Port = ge.1.26
Multicast Group Address = ff04::1:1:1:1
Vlan Id                 = 2502
Source IP Address       = Any
Expire Time(Sec)        = 194
Port Mode               = Exclude

Port = ge.1.27
Multicast Group Address = ff04::1:1:1:1
Vlan Id                 = 2503
Source IP Address       = Any
Expire Time(Sec)        = 193
Port Mode               = Exclude

2 entries displayed

S Chassis(su)->
```

show mld flows

Use this command to display MLD flow table entries.

Syntax

show mld flows [**port-list** *port-list*] [**group** *group*] [**vlan-list** *vlan-list*] [**sip** *sip*]

Parameters

portlist *portlist*	(Optional) Displays flow table entries by port or range of ports
group *group*	(Optional) Displays flow table entries by multicast group IP address.
vlan-list *vlan-list*	(Optional) Displays flow table entries by VLAN ID or range of VLAN IDs. Valid values are **1 – 4094**.
sip *sip*	(Optional) Source IP address. Use 0.0.0.0 to show all sips.

Defaults

If no parameters are specified, information for all MLD flows is displayed.

Mode

All command modes.

Example

```
S Chassis(su)->show mld flows vlan-list 3001 sip 2504::19
 Multicast Flows
--------------------------------------------------------------------------------
Port = ge.1.40
Multicast Group Address = ff04::1:1:1:1
Vlan Id                 = 3001
Source IP Address       = 2504::19

1 entries displayed
S Chassis(su)->
```

set mld unknown-input-action

Use this command to set the action taken when the first few frames of a multicast stream are received (that is, before the stream is added to the MLD database).

Syntax

set mld unknown-input-action {**routers** | **flood** | **discard**}

Parameters

routers	Send the frames of the multicast stream to all known multicast routers
flood	Flood the frames of the multicast stream to the VLAN on which the stream was received. This is the default value.
discard	Discard the frames of the multicast stream.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the unknown input action to discard the frames of multicast streams.

```
S Chassis(su)->set mld unknown-input-action discard
```

show mld unknown-input-action

Use this command to display the action taken when the first frames of a multicast stream are received.

Syntax

show mld unknown-input-action

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the currently configured unknown input action.

```
S Chassis(su)->show mld unknown-input-action
Unknown Input Action: Flood to Vlan
```

64

IPv4 PIM Commands

This chapter describes the Protocol Independent Multicast (PIM) IPv4 configuration set of commands and how to use them. For information about configuring PIM, refer to the "Multicast Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
ip mroute	64-2
ip pim sparse-mode	64-4
ip pim dense-mode	64-4
ip pim ssm	64-5
ip pim anycast-rp	64-6
ip pim asm-join-filter	64-7
ip pim ssm-join-filter	64-7
ip pim bsr-candidate	64-8
ip pim bsr-border	64-9
ip pim dr-priority	64-9
ip pim graceful-restart	64-10
ip pim multipath	64-11
ip pim neighbor-filter	64-12
ip pim rp-address	64-12
ip pim rp-candidate	64-13
ip pim state-refresh origination-interval	64-14
ip pim static-rp-override	64-15
show ip mroute	64-15
show ip mcache	64-17
show ip pim	64-19
show ip pim anycast-rp	64-20
show ip pim bsr	64-21
show ip pim interface	64-23
show ip pim mrt	64-24
show ip pim mrt type	64-26

For information about...	Refer to page...
show ip pim neighbor	64-28
show ip pim rp	64-30
show ip pim rp-hash	64-32
show ip pim statistics	64-32
clear ip mroute	64-33
clear ip pim statistics	64-34

ip mroute

Use this command to add or remove a static IP multicast route. This command is valid only when an ipv4 multicast topology is configured for this router.

Syntax

ip mroute *<prefix>* {*<prefix-mask>*} | *<prefix/prefix-length>* **vlan** *<vlan-id>* {[*<distance>*] [**tag** *<tag-id>*]} **reject** {[*<distance>*] [**tag** *<tag-id>*]} **blackhole** {[*<distance>*] [**tag** *<tag-id>*]} **interface** *<interface-name>* {[*<distance>*] [**tag** *<tag-id>*]} *<ip-address>* {[**interface** *<interface-name>*] | [**recursive**] [*<distance>*] [**tag** *<tag-id>*] [**probe** {**default** | *<probe-name>*}] **vrf** *<vrf-name>* {[*<distance>*] [tag *<tag-id>*]}

no ip mroute *<prefix>* {*<prefix-mask>*} | *<prefix/prefix-length>*

Parameters

prefix	Specifies a destination IP address prefix.
prefix mask	Specifies a destination prefix mask.
prefix/prefix-length	Specifies a destination IP address in prefix/prefix-length format.
ip-address	Specifies a next-hop router IP address.
interface *interface-name*	Specifies the next-hop interface.
vlan *vlan-id*	Specifies the next-hop VLAN. Valid values are **1** - **4094**.
vrf *vrf-name*	Specifies that the destination is in VRF router with this name.
blackhole	Specifies that packets destined for this route's subnet are silently dropped. An ICMP network unreachable message is not sent to the packet source.
reject	Specifies that packets destined for this route's subnet are dropped, and an ICMP network unreachable message is sent to the packet source.
recursive	(Optional) Specifies that the next-hop interface is determined by route lookup.
distance	(Optional) Specifies an administrative distance metric for this route. Valid values are **1** (default) to **255**. Routes with lower values receive higher preference in route selection.
tag *tag-id*	(Optional) Specifies an OSPF tag ID for this route. Valid values are **1** - **4294967295**.
default	Uses the default static route probe

probe-name	Specifies the name of a probe to use.

Defaults

- If *distance* is not specified, the default value of 1 is applied.
- If an OSPF tag ID is not specified, no OSPF tag is associated with the route.
- If **recursive** is not specified, see usage section below.

Mode

Configuration command mode**.**

Usage

This command is used to configure static multicast routes. The route forwards IP traffic depending upon the IP forwarding setting of the routing interface. Routing interfaces are set for IP forwarding by default. To configure a static multicast route as a non-forwarding IP route, set IP forwarding for the routing interface to non-forwarding using the **no ip forwarding** command in interface configuration mode.

Use the **vrf** *egress-vrf* parameter to point to the egress VRF router that will perform the next-hop lookup for this static route. Using the **vrf** *egress-vrf* parameter is more dynamic than configuring a standard static route, in that it determines the next hop based upon a route table lookup. A standard static route specifies a single next hop. Should that next hop be unavailable, the subnet is no longer reachable. A standard static route can be configured to reach the next hop that is a member of a different VRF using the syntax: **ip route** *destination-prefix/length next-hop-address* **interface** *next-hop-interface*. Because the **vrf** *egress-vrf* parameter provides greater flexibility in determining the next hop, it is recommended that you use the **vrf** *egress-vrf* parameter.

The default VRF router is referred to as the **global** router. Named VRF routers within a device configured using the **set router vrf create** command are referred to as non-global VRF routers. Static routes are supported between both the **global** router and any non-global VRF router and between any two non-global VRF routers.

If you only enter the prefix/length and the IP address of the nexthop router and do not specify the optional **recursive** parameter, a search is performed of all configured subnets for a subnet containing the next-hop. If found, the static route is anchored to that interface, else it becomes a recursive route.

See “ipv6 mroute” on page 65-2 for IPv6 static multicast route configuration command information.

The “no” form of this command removes the static IP multicast route.

Examples

This example shows how to set IP address 10.1.2.3 as the next hop gateway to destination address 10.0.0.0.:

```
S Chassis(rw-router-config)->ip mroute 10.0.0.0 255.0.0.0 10.1.2.3
```

This example shows how to set VLAN 100 as the next hop interface to destination address 10.0.0.0:

```
S Chassis(rw-router-config)->ip mproute 10.0.0.0 255.0.0.0 vlan 100
```

ip pim sparse-mode

Use this command to enable Protocol Independent Multicast (PIM) Sparse Mode (SM) on an IPv4 routing interface.

Syntax

ip pim sparse-mode

no ip pim sparse-mode

Parameters

None.

Defaults

None.

Mode

Interface configuration.

Usage

The “no” form of this command disables PIM on an interface.

You do not have to enable PIM on a loopback interface for use as a BSR or RP.

Example

This example enables PIM sparse mode on VLAN 1:

```
S Chassis(su-config)->interface vlan 1
S Chassis(su-config-intf-vlan.0.1)->ip pim sparse-mode
```

ip pim dense-mode

Use this command to enable Protocol Independent Multicast (PIM) dense mode (DM) on an IPv4 routing interface.

Syntax

ip pim dense-mode

no ip pim dense-mode

Parameters

None.

Defaults

None.

Mode

Interface configuration.

Usage

The “no” form of this command disables PIM dense mode on an interface.

Example

This example enables PIM dense mode on VLAN 1:

```
S Chassis(su-config)->interface vlan 1
S Chassis(su-config-intf-vlan.0.1)->ip pim dense-mode
```

ip pim ssm

Use this command to configure Source Specific Multicast (SSM) mode for the default or a specified multicast group range.

Syntax

ip pim ssm {**default** | *group-address group-mask*}

no ip pim ssm {**default** | *group-address group-mask*}

Parameters

default	Specifies that PIM SSM is enabled with the default address-group. The default address group is 232.0.0.0 255.0.0.0 (232.0.0.0/8).
group-address group-mask	Specifies that PIM SSM is enabled with the specified address range and mask.

Defaults

None.

Mode

Configuration command.

Usage

The “no” form of this command removes PIM SSM configuration.

Example

This example enables PIM SSM for the default group range 232.0.0.0/8 and for a user defined group range of 235.100.10.0/24:

```
S Chassis(su)->configure
S Chassis(su-config)->ip pim ssm default
S Chassis(su-config)->ip pim ssm 235.100.10.0 255.255.255.0
```

ip pim anycast-rp

Use this command to configure an anycast Rendezvous Points (RP) set member for a multicast group.

Syntax

ip pim anycast-rp *anycast-address peer-address*

no ip anycast-rp *anycast-address peer-address*

Parameters

anycast-address	Specifies the IP address of a loopback interface to be configured on each anycast-RP that will be used as the RP address for all members of the anycast-RP set.
peer-address	Specifies the unique peer IP address of a loopback or hardware interface for this anycast RP.

Defaults

None.

Mode

Configuration command.

Usage

The relationship between a source or receiver and the PIM RP router is a one-to-one relationship. The relationship between a source or receiver and an anycast-RP set of routers is a one-to-many relationship, where one of multiple anycast configured RPs is selected by the routing protocol to be the source or receiver RP. The purpose of anycast-RP is to provide a means of fast convergence when a PIM RP router fails.

Anycast-RP provides for the selection of a set of routers to be identified as anycast RPs by configuring:

- A loopback interface with the same IP address for each anycast-RP router in the set
- Either a second loopback interface or another hardware interface to be configured with a unique address for this peer of the anycast-RP set

Each anycast-RP router is configured with the same anycast-RP address and all the peer-addresses of each router in the anycast-RP router set. Each anycast-RP and peer-address combination is configured in its own command line entry using the **ip pim anycast-rp** command.

The routing protocol determines which member of the anycast-RP router set will function as the PIM RP router. Should the PIM RP router fail, the routing protocol determines the next anycast-RP router that will become the new PIM RP router, based upon the routing protocol's routing criteria. Should the failed router return to an operational state, the routing protocol will determine whether a new PIM RP will be selected based upon current conditions.

The "no" form of this command removes a single anycast-RP configuration from the anycast-RP set.

Example

This example configures an anycast RP set with the anycast address of 1.0.0.1 and peer addresses of 10.0.0.1, 20.0.0.1, and 30.0.0.1 on this anycast-RP router:

```
S Chassis(su-config)->ip pim anycast-rp 1.0.0.1 10.0.0.1
S Chassis(su-config)->ip pim anycast-rp 1.0.0.1 20.0.0.1
S Chassis(su-config)->ip pim anycast-rp 1.0.0.1 30.0.0.1
```

ip pim asm-join-filter

Use this command to specify the Any-Source Multicast groups permitted to cross this interface in either an inbound or outbound direction.

Syntax

ip pim asm-join-filter *standard-acl*

no ip pim asm-join-filter *standard-acl*

Parameters

standard-acl	Specifies the standard ACL containing ASM group permit or deny entries.

Defaults

None.

Mode

Interface command mode.

Usage

The ASM join filter applies a standard permit/deny ACL that defines which Any-Source Multicast groups are permitted to cross this interface either inbound our outbound.

The “no” form of this command removes the specified ASM join filter.

Example

This example defines the ASM groups permitted to cross this interface using the **asmFilter1** standard ACL on VLAN 100:

```
S Chassis(su-config)->interface vlan 100
S Chassis(su-config-intf-vlan.0.100)->ip pim asm-join-filter asmFilter1
S Chassis(su-config-intf-vlan.0.1)->
```

ip pim ssm-join-filter

Use this command to specify the Source-Specific Multicast groups permitted to cross this interface in either an inbound or outbound direction.

Syntax

ip pim ssm-join-filter *extended-acl*

no ip pim ssm-join-filter *extended-acl*

Parameters

standard-acl	Specifies the extended ACL containing SSM group permit or deny entries.

Defaults

None.

Mode

Interface command mode.

Usage

The SSM join filter applies an extended permit/deny ACL, specifying the source or destination IP addresses that define which Source Specific Multicast S,G pairs are permitted to cross the interface.

The "no" form of this command removes the specified SSM join filter.

Example

This example defines the SSM groups permitted to cross this interface using the **ssmFilter1** standard ACL on VLAN 100:

```
S Chassis(su-config)->interface vlan 100
S Chassis(su-config-intf-vlan.0.100)->ip pim ssm-join-filter ssmFilter1
S Chassis(su-config-intf-vlan.0.100)->
```

ip pim bsr-candidate

Use this command to enable the router to announce its candidacy as a BootStrap Router (BSR).

Syntax

ip pim bsr-candidate *interface-address* [**priority** *priority*]

no ip bsr-candidate *interface-address*

Parameters

interface-address	Address of the BSR candidate interface. With the exception of a loopback interface, the interface used as the BSR candidate must be enabled with PIM as described in "ip pim sparse-mode" on page 64-4.
priority *priority*	(Optional) Specifies a BSR priority value ranging from **0–255**. Higher values assign higher priority. The BSR with the larger priority is preferred. If priority values are the same, the IP address breaks the tie. The BSR candidate with the higher IP address is preferred. Default value: **0**.

Defaults

If *priority* is not specified, **0** will be applied.

Mode

Configuration command.

Usage

Only one BSR candidate can be configured per router.

The “no” form of this command removes the router as a BSR candidate.

Example

This example sets the BSR priority to 77 on 10.0.0.1:

```
S Chassis(su-config)->ip pim bsr-candidate 10.0.0.1 priority 77
```

ip pim bsr-border

Use this command to configure a BSR border router. A BSR border router prevents the interface from receiving BSR messages outside the PIM domain and from sending BSR messages out.

Syntax

ip pim bsr-border

[no] **ip pim bsr-border**

Parameters

None.

Defaults

None.

Mode

Interface configuration mode.

Usage

This command limits BSR messages in a PIM domain. Without a BSR border, BSR messages from other PIM domains may result in wrong RPs for this domain.

Use the “no” form of this command to remove a BSR border from this domain.

Examples

This example shows how to configure a BSR border for this domain:

```
S Chassis(su-config)->ip pim bsr-border
```

ip pim dr-priority

Use this command to set the priority for which a router will be elected as the designated router (DR).

Syntax

ip pim dr-priority *priority*

no ip dr-priority

Parameters

priority	Specifies a priority value for designated router selection. Valid values are **0–4294967294**. Default is **1**.

Defaults

None.

Mode

Interface configuration.

Usage

The “no” form of this command disables the DR functionality.

Example

This example sets the DR priority to 20 on VLAN 1:

```
S Chassis(su-config)->interface vlan 1
S Chassis(su-config-intf-vlan.0.1)->ip pim dr-priority 20
```

ip pim graceful-restart

Use this command to set the multicast graceful-restart period, which is the period of time in which a restarting router and its neighbors can continue to forward multicast packets during the failover.

Syntax

ip pim graceful-restart [**period** *value*]

no ip pim graceful-restart

Parameters

period *value*	Specifies the maximum amount of time in seconds that this router will remain in multicast graceful-restart mode starting at the time it enters graceful-restart. Possible values are **30–600** seconds. The default value is **120** seconds.

Defaults

The default value is **120** seconds.

Mode

Configuration command.

Usage

Multicast graceful restart requires OSPF graceful restart. Ensure that you have configured and enabled OSPF graceful restart before you enable multicast graceful restart. For more information about configuring and enabling OSPF graceful restart, see Chapter 73, **OSPFv2 Commands** or Chapter 74, **OSPFv3 Commands**.

The “no” form of this command disables the multicast graceful-restart period.

To view the current graceful-restart setting, use the **show running-config pim** command.

Example

This example shows the multicast graceful-restart period set to 180 seconds.

```
S Chassis(su-config)->ip pim graceful-restart period 180
```

ip pim multipath

Use this command to allow PIM multicast to either load share over ECMP paths or have a single deterministic next hop for ECMP paths.

Syntax

ip pim multipath {**hash** | **highest-nexthop**}

no ip pim multipath {**hash** | **highest-nexthop**}

Parameters

hash	Configure multipath to choose a PIM next hop based on a hash of the source (or RP) being queried.
highest-nexthop	Configure multipath to choose the highest address as the PIM next hop.

Defaults

Multipath will use the first nexthop learned for an ECMP route.

Mode

Configuration command.

Usage

Multipath provides the ability to define the mechanism by which PIM chooses the nexthop. By default, PIM uses the first learned next hop. You can change multipath to use the highest next hop or a next hop based on a hash of the source IP address.

For a deterministic next hop, the **highest-nexthop** algorithm chooses the numerically highest next hop. The **hash** algorithm will attempt to spread multicast over all possible next hops.

For the least disruption during network events (including bootup), use the default (first next-hop). The first next hop learned will be the one used regardless of added or removed next hops.

Multipath also allow PIM graceful restart to choose the same next hop after a router failover because the **highest-nexthop** and the **hash** algorithms will choose the same next hop, assuming the set of next hops is consistent after the failover.

The “no” form of this command resets the multipath configuration to the default value (using the first next hop).

To view the current multipath setting, use the **show running-config pim** command.

Example

This example shows setting the multipath configuration to the highest address as the PIM next hop.

```
S Chassis(su-config)->ip pim multipath highest-nexthop
```

ip pim neighbor-filter

Use this command to filter PIM neighbors.

Syntax

ip pim neighbor-filter *neighbor-filter*

no ip pim neighbor-filter *neighbor-filter*

Parameters

neighbor-filter	Specifies the name of a standard access-list containing one of more allowed neighbors.

Defaults

None.

Mode

Interface configuration.

Usage

The “no” form of this command removes the specified neighbor-filter.

Example

This example sets the neighbor-filter to permit only 10.21.5.45 and 10.22.10.1 to participate in the PIM protocol for VLAN 1:

```
S Chassis(su-config)->ip access-list standard pim_nbr_fltr
S Chassis(su-cfg-std-acl-pim_*fltr)->permit host 10.21.5.45
S Chassis(su-cfg-std-acl-pim_*fltr)->permit host 10.22.10.1
S Chassis(su-cfg-std-acl-pim_*fltr)->exit
S Chassis(su-config)->interface vlan 1
S Chassis(su-config-intf-vlan.0.1)->ip pim neighbor-filter pim_nbr_fltr
```

ip pim rp-address

Use this command to set a static Rendezvous Point (RP) for a multicast group.

Syntax

ip pim rp-address *rp-address* {*group-address group-mask* | **group-list** *group-list*}

no ip pim rp-address *rp-address* {*group-address group-mask* | **group-list** *group-list*}

Parameters

rp-address	Specifies the IP address of the PIM RP router.
group-address	Specifies the multicast group address.
group-mask	Specifies the multicast group mask.
group-list *group-list*	Specifies a standard access-list containing one or more multicast groups.

Defaults

None.

Mode

Configuration command.

Usage

For each static RP, groups may be configured either individually or using a group-list. A group-list must exist before it can be used by this command. If a group-list referenced by this command is removed, the configuration will also be removed. Before using a group-list, any groups entered using the group-address and group-mask must be removed.

The "no" form of this command removes the static RP configuration. Groups specified using a group-list may not be removed using the *group-address group-mask* option; they must be removed using the **group-list** option.

Example

This example sets a static RP address at 10.0.0.1 for the multicast group at 235.0.0.0 255.0.0.0:

```
S Chassis(su-config)->ip pim rp-address 10.0.0.1 235.0.0.0. 255.0.0.0
```

ip pim rp-candidate

Use this command to enable the router to advertise itself as a PIM candidate rendezvous point (RP) to the BSR.

Syntax

ip pim rp-candidate *pim-interface-address* {*group-address group-mask* | **priority** *priority* | **group-list** *group-list* [**priority** *priority*]}

no ip pim rp-candidate *pim-interface-address* {*group-address group-mask* | **group-list** *group-list* [**priority** *priority*]}

Parameters

pim-interface-address	Address of the interface to advertise as an RP candidate. With the exception of a loopback interface, the interface used as the RP candidate must be enabled with PIM as described in "ip pim sparse-mode" on page 64-4.
group-address	Specifies the multicast group address.
group-mask	Specifies the multicast group mask.
priority *priority*	Specifies an RP priority value, ranging from **0–255**. Lower values assign higher priority. Default value: **192**.
group-list *group-list*	Specifies a permit only standard access-list containing one or more multicast group addresses. All non-permit multicast groups are ignored.

Defaults

If no priority is specified when assigning a group-address or group-list, the priority defaults to **192**.

Mode

Configuration command.

Usage

At least one group-address or a group list must be specified before this RP will be active. For each candidate RP, groups may be configured either individually or using a group-list. A group-list must exist before it may be used by this command. If a group-list referenced by this command is removed, that configuration will also be removed. Before using a group-list, any groups entered using the group-address and group-mask must be removed.

The "no" form of this command removes the candidate RP configuration for the group-list or group-address specified, but resets the priority to default of **192**, if only the priority is specified. Groups specified using a group-list may not be removed by using the *group-address group-mask* option; they must be removed using the **group-list** option.

Examples

This example enables the PIM interface at address **35.0.0.1** to advertise itself as an RP candidate with a priority of **5**:

```
S Chassis(su-config)->ip pim rp-candidate 35.0.0.1 priority 5
```

This example enables the PIM interface at address **35.0.0.1** to advertise itself as an RP candidate with a priority of **5**, for groups specified in the **pimrp** standard access-list:

```
S Chassis(su-config)->ip pim rp-candidate 35.0.0.1 group-list pimrp priority 5
```

ip pim state-refresh origination-interval

Use this command to set the interval between PIM dense mode state refresh messages.

Syntax

ip pim state-refresh origination-interval *interval*

no ip pim state-refresh origination-interval *interval*

Parameters

interval	Specifies the interval in seconds between the sending of PIM dense mode state refresh messages. Default value: **60** seconds.

Defaults

PIM dense mode state refresh messages are sent at **60** second intervals by default.

Mode

Configuration command.

Usage

PIM dense mode state refresh messages are sent to neighbor routers by the PIM dense mode routers that are connected to a PIM source. State refresh messages convey prune state for the purpose of minimizing overhead to the network.

The "no" form of this command resets the PIM dense mode state refresh message interval to **60** seconds.

Examples

This example sets the PIM dense mode state refresh message interval to **80** seconds:

```
S Chassis(su-config)->ip pim state-refresh origination-interval 80
```

ip pim static-rp-override

Use this command to control whether static RP configurations will override dynamic RP information learned for IPv4 groups.

Syntax

ip pim static-rp-override

no ip pim static-rp-override

Defaults

None.

Defaults

Configuration command.

Usage

The static RP override feature is enabled by default. If both static and dynamic RP configurations exist, by default the static RP configurations take precedence over the dynamic RP configurations. Disabling this command allows dynamic RP configurations to take precedence over static RP configurations.

The “no” form of this command disables the static RP override feature.

Examples

This example disables static RP override for this device, allowing dynamic RP configurations to take precedence over static RP configurations:

```
S Chassis(su-config)->no ip pim static-rp-override
```

show ip mroute

Use this command to display the IP multicast routing table.

Syntax

show ip mroute [**source** *source* | **group** *group* | **interface** *interface*] [**brief**] [**type** {**all** | **s-g** | **star-g**}] [**summary**]

Parameters

source *source*	(Optional) Displays information about a specific unicast source address.
group *group*	(Optional) Displays information about a multicast destination address.
interface *interface*	(Optional) Displays information about a specific interface entered in format vlan.0.*x*.
brief	(Optional) Displays a brief level of information.

type all | **s-g** | **star-g**	(Optional) Displays the specified route entry type: • **all** – displays all route entries (default) • **s-g** – displays S,G entries • **star-g** – displays *,G entries
summary	(Optional) Displays a one line summary for each multicast route based upon the source, group, or interface filter option entered.

Defaults

If no optional parameters are specified, detailed information about all source and destination addresses will be displayed.

Mode

All command modes.

Usage

The output for this command shows how a multicast routing protocol, such as PIM and DVMRP, will forward a multicast packet. Information in the table includes source network/mask and upstream neighbors. For more information on configuring PIM and DVMRP, refer to the *Extreme Networks S-Series Configuration Guide*.

Example

This example shows a portion of the IP multicast routing table display. In this case, it shows there are two source PIM sparse mode (PIM-SM) multicast networks. The first PIM-SM network shows an incoming route at VLAN 13 and outgoing routes at VLAN 1030 and 1040:

```
S Chassis(su)->show ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Source is connected,
       F - Register flag, N - No outgoing interfaces
       Q - Null-Forwarding entry

Timers: Uptime/Expires

  PIMSM (*, 224.1.1.1), 14:02:09/00:00:00, flags: SC
        Incoming interface: vlan.0.13
        Outgoing interface list:
          vlan.0.1030, Forward/Sparse, 14:02:09/00:00:00
          vlan.0.1040, Forward/Sparse, 14:02:09/00:00:00

  PIMSM (30.1.1.11/32, 224.1.1.1), 14:02:09/00:00:00, flags: S
        Incoming interface: vlan.0.13
        Outgoing interface list:
          vlan.0.1030, Forward/Sparse, 14:02:09/00:00:00
          vlan.0.1040, Forward/Sparse, 14:02:09/00:00:00

  PIMSM (110.1.1.11/32, 224.1.1.1), 14:02:09/00:00:00, flags: S
```

```
Incoming interface: vlan.0.13
Outgoing interface list:
  vlan.0.1030, Forward/Sparse, 14:02:09/00:00:00
  vlan.0.1040, Forward/Sparse, 14:02:09/00:00:00
```

show ip mcache

Use this command to display the IP multicast forwarding cache that was used to program the hardware flow.

Syntax

show ip mcache [**group** *group* | **source** *source*] [**interface**] [**verbose** | **brief** | **summary**] [**statistics**] [**-wide**]

Parameters

group *group*	(Optional) Displays information about a specific multicast destination address.
source *source*	(Optional) Displays information about a specific unicast source address.
interface	(Optional) Displays mcache information filtered for the inbound interface.
verbose	(Optional) Displays a detailed level of information.
brief	(Optional) Displays a single line brief level of information.
summary	(Optional) Displays the number of entries currently in the cache.
statistics	(Optional) Displays multicast cache statistics.
-wide	(Optional) Specifies that the display should use up to 132 characters per line if applicable.

Defaults

If no optional parameters are specified, detailed information about all source and destination addresses will be displayed. The statistics verbose option uses a standard 80 column format.

Mode

All command modes.

Usage

An 80 character line can display statistics for up to 4 slots. If your system has more than 4 slots, use the **-wide** option to allow for the display of slots beyond slot 4 on a single line.

The output of this command shows what multicast routes have actually been programmed into the S-Series hardware. Although redundant to the **show ip mroute** display ("show ip mroute" on page 64-15), it is a useful debugging tool if there are discrepancies between the multicast routing table and the multicast forwarding table.

Example

This example shows a portion of the IP multicast forwarding cache display:

```
S Chassis(su)->show ip mcache
```

```
IP Multicast Cache Table
FLAGS: S - L2 flow, M - MFIB entry, N - Null OIF, T - static
       C - CPU Flow (not in HW), A - flow active, X - pending deletion
       F - register

 Group           Source           Interface    Flags       Age
 224.1.1.1       110.1.1.10       vlan.0.13    MA       0d 00h:11m:44s
     Outgoing Interface List:
       vlan.0.1040
 230.1.1.1       20.1.1.10        vlan.0.23    MA       0d 00h:10m:35s
     Outgoing Interface List:
       vlan.0.1040
 239.1.1.1       192.168.101.10   vlan.0.1010  MA       0d 00h:11m:49s
     Outgoing Interface List:
       vlan.0.13
       vlan.0.23
       vlan.0.1040

3 mcache entries displayed
```

This example shows to display IP multicast forwarding cache statistics:

```
S Chassis(rw)->show ip mcache statistics

IP Multicast Cache Statistics
These counters represent IP Multicast packets seen in the soft-path only.

Total IP Multicast packets received        : 634
IPv4 IP Multicast packets received         : 634
IPv6 IP Multicast packets received         : 0
Multicast packets dropped due to TTL       : 0
Multicast packets dropped due to ACL       : 0
Data packets sent up to PIM at DR          : 95
Register packets received at RP            : 653
Decapsulated register packets transmitted  : 1048
S Chassis(rw)->
```

This example shows how to display a verbose level of IP multicast forwarding cache statistics:

```
S Chassis(rw)->show ip mcache statistics verbose

IP Multicast Cache Statistics
These counters represent IP Multicast packets seen in the soft-path only.

Statistic             Totals     Slot  2     Slot  3
-----------------------------------------------------
Packets in      :        634          42         592
v4 Pkts in      :        634          42         592
```

```
v6 Pkts in      :          0           0           0
Drop TTL        :          0           0           0
Drop ACL        :          0           0           0
Sent to PIM     :         95          95           0
Registers recvd :        653         170         483
RP transmits    :       1048        1048           0
S Chassis(rw)->
```

This example shows how to display a brief level of multicast forwarding cache statistics:

```
S Chassis(rw)->show ip mcache statistics brief

IP Multicast Cache Statistics
These counters represent IP Multicast packets seen in the soft-path only.

Total IP Multicast packets received        : 634
IPv4 IP Multicast packets received         : 634
IPv6 IP Multicast packets received         : 0
S Chassis(rw)->
```

show ip pim

Use this command to display summary tables of IPv4 PIM interfaces, neighbors, BSR, and group-to-RP mappings.

Syntax

show ip pim

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

```
S Chassis(su)->show ip pim

[PIM Interfaces]
 Interface    Address          Nbr    Hello  DR         Status  DR-Address
                               Count  Intvl  Priority
 ------------------------------------------------------------------------------
 vlan.0.2334  192.233.4.4      1      30     1          UP      192.233.4.4
 vlan.0.2501  10.51.0.1        0      30     1          UP      10.51.0.1
 vlan.0.2502  10.52.0.1        0      30     1          UP      10.52.0.1
```

```
 vlan.0.2503  10.53.0.1        0      30     1          UP      10.53.0.1
 vlan.0.2504  10.54.0.1        0      30     1          UP      10.54.0.1
 vlan.0.2601  10.61.0.1        0      30     1          UP      10.61.0.1
 vlan.0.3014  192.168.14.4     1      30     1          UP      192.168.14.4
 vlan.0.3024  192.168.24.4     1      30     1          UP      192.168.24.4
 vlan.0.3034  192.168.34.4     1      30     1          UP      192.168.34.4

 9 PIM enabled interfaces

[PIM Neighbors]
 Neighbor Address    Interface      DR Priority    Uptime            Expires
 ------------------------------------------------------------------------------
 192.233.4.3         vlan.0.2334    1              04:47:56          00:01:28
 192.168.14.1        vlan.0.3014    1              04:47:57          00:01:28
 192.168.24.2        vlan.0.3024    1              04:47:47          00:01:38
 192.168.34.3        vlan.0.3034    1              04:47:55          00:01:30

 4 PIM neighbors

[PIM BSR]
 PIMv2 Elected Bootstrap Router Information:
    BSR Address: 172.16.1.1
    BSR Hash Mask Length: 30
    BSR Priority: 100
    BSR Expire: 00:01:20

[PIM Group-To-RP Mappings]
 Group Range           RP Address         Mode  Active  Origin    Anycast
 ------------------------------------------------------------------------
 232.0.0.0/8           0.0.0.0            SSM   Yes     Static    no-info
 224.0.0.0/4           172.16.1.2         ASM   Yes     BSR       no-info
 224.0.0.0/4           172.16.2.2         ASM   No      BSR       no-info
 224.0.0.0/8           172.16.1.1         ASM   Yes     BSR       no-info

 4 PIM Group to RP mappings (1 static, 3 via BSR)
```

show ip pim anycast-rp

Use this command to display RP anycast information for all or a specified RP.

Syntax

show ip pim anycast-rp [**rp-address** *rp-address*]

Parameters

rp-address	(Optional) Specifies the IP address of the PIM RP router to display.

Defaults

If no RP IP-address is specified, information for all RPs is displayed.

Mode

All command modes.

Example

```
S Chassis(su)->show ip pim anycast-rp

PIM Anycast RP Configuration

  Anycast-RP 172.16.1.2
    Peer 192.168.13.1     (local router)
    Peer 192.168.13.3
S Chassis(su)->
```

show ip pim bsr

Use this command to display BootStrap Router (BSR) information.

Syntax

show ip pim bsr [**detail**]

Parameters

detail	(Optional) Displays detailed information about the BSR.

Defaults

If **detail** is not specified, a standard level of information displays about the BSR.

Mode

All command modes.

Examples

This example shows how to display BootStrap Router (BSR) information:

```
S Chassis(su)->show ip pim bsr

 PIMv2 Elected Bootstrap Router Information:
    BSR Address: 192.168.1.1
    BSR Hash Mask Length: 30
    BSR Priority: 100
    BSR Expire: 00:01:43

 This Router is a Candidate Bootstrap Router (CBSR)
    Candidate BSR Address: 192.168.1.3
    Hash Mask Length: 30
```

```
    Priority: 30
```

This example shows how to display detailed BSR information:

```
S Chassis(su)->show ip pim bsr detail

 PIMv2 Elected Bootstrap Router Information:
    BSR Address: 192.168.1.1
    BSR Hash Mask Length: 30
    BSR Priority: 100
    BSR Expire: 00:01:52

This Router is a Candidate Bootstrap Router (CBSR)
    Candidate BSR Address: 172.16.3.1
    Hash Mask Length: 30
    Priority: 40
    Elected BSR: true
    Next BSM: 00:00:29
```

Table 64-1 provides an explanation of the command output.

Table 64-1 show ip pim bsr Output Details

Output...	What it displays...
BSR Address	IP address of the bootstrap router.
BSR Hash Mask Length	Length of a mask that is to be added with the group address before the hash function is called. This value is hard coded to **30**.
BSR Priority	Priority as set by the **ip pim bsr-candidate** command.
BSR Expire	Period in which the next bootstrap message is due from this BSR (in hours:minutes:seconds). After 24 hours, format will change into days:hours and, after a week, will change into weeks:days.
Candidate BSR Address	The (unicast) address that the local router will use to advertise itself as a Candidate-BSR.
Hash Mask Length	The hash mask length (used in the RP hash function) that the local router will advertise in its Bootstrap messages for this zone. This object is hard-coded to 30 if the Candidate BSR Address Type is **ipv4** or **ipv4z**.
Priority	The priority value for the local router as a Candidate-BSR for this zone. Numerically higher values for this object indicate higher priorities.
Elected BSR	Whether the local router is the elected BSR for this zone. If the value is false, the Next BSM timer does not appear in the output.
Next BSM	The time remaining before the local router next originates a Bootstrap message for this zone.

show ip pim interface

Use this command to display information about IPv4 PIM interfaces that are currently up (not shutdown).

Syntax

show ip pim interface [*ifName*] [**brief**] [**detail**] [**statistics**]

Parameters

ifName	(Optional) Displays information about a specific PIM interface.
brief	(Optional) Displays a summary level of information about all PIM interfaces or a specific PIM interface.
detail	(Optional) Displays detailed information about all PIM interfaces or a specific PIM interface.
statistics	(Optional) Displays PIM statistics information for all or the specified interface.

Defaults

If no parameters are specified, information about all PIM interfaces will be displayed.

Mode

All command modes.

Examples

This example shows how to display summary information for all PIM interfaces.

```
S Chassis(su)->>show ip pim interface
 Interface    Address          Nbr    Hello  DR         Status  DR-Address
                               Count  Intvl  Priority
 ---------------------------------------------------------------------------
 vlan.0.3034  192.168.34.4     1      30     1          UP      192.168.34.4
```

This example shows how to display detailed information for a specific PIM interface.

```
S Chassis(su)->show ip pim interface vlan.0.3034 detail
Interface vlan.0.3034
  PIM IP Address is 192.168.34.4
  PIM version: 2, mode: sparse
  PIM DR Primary Address: 192.168.34.4
  PIM Hello Interval: 30
  PIM Triggered Hello Interval: 5
  PIM Join Prune Interval: 60
  PIM Hello Holdtime: 105
  PIM Join Prune Holdtime: 210
  PIM Generation Id Value: 1639319435 (0x61b6078b)
  PIM Neighbor Count: 1
  PIM Propagation Delay: 500
  PIM Override Interval: 2500
```

```
PIM DR Priority: 1
PIM Lan Delay Enabled: true
PIM Effective Propagation Delay: 500
PIM Effective Override Interval: 2500
PIM Suppression Enabled: true
PIM DR Priority Enabled: true
PIM Assert Interval: 177
PIM Assert Holdtime: 180
```

Table 64-2 provides an explanation of the command output.

Table 64-2 show ip pim interface Output Details

Output...	What it displays...
Interface	Specifies the PIM interface for this information.
Address	Specifies the PIM IP address for this information.
Nbr Count	Specifies the number of neighbors for this PIM interface.
Hello Intvl	Specifies the value of the hello interval.
DR Priority	Specifies the priority value of the designated router.
Status	Specifies the status of this PIM interface.
DR-Address	Specifies the IP address of the designated router.

show ip pim mrt

Use this command to display the IPv4 PIM and DVMRP multicast route (*,G and S,G) table.

Syntax

show ip pim mrt [**source** *source* | **group** *group*] [**interface**] [**detail**] [**brief**] [**summary**]

Parameters

source *source*	(Optional) Displays information about a specific unicast source address.
group *group*	(Optional) Display information about a multicast destination address.
interface	(Optional) Displays information for the multicast route table filtered based upon the inbound interface.
detail	(Optional) Displays a detailed level of multicast route table information.
brief	(Optional) Displays a brief level of specified information.
summary	(Optional) Displays the number of entries found.

Defaults

If no optional parameters are specified, a standard level of information about all source and destination addresses is displayed.

Mode

All command modes.

Usage

This command provides insight into PIM specific data for an mroute such as protocol state and timers for purposes of debugging PIM.

Examples

This example displays a standard level of information for the IPv4 PIM multicast route table for source address **192.168.202.10**:

```
S Chassis(su)->show ip pim mrt source 192.168.202.10

PIM Sparse Mode Multicast Routing Table
Timers: Uptime/Expires

  192.168.202.10, 224.1.1.1, up 23:54:44
    RPF interface: vlan.0.2334, SPT true, mode ASM
    Downstream S,G state:
      vlan.0.3014, Forward, 23:54:44/00:03:03
      vlan.0.3024, Forward, 23:54:43/00:03:05
      vlan.0.3034, Forward, 23:54:43/00:03:02

1 mroute entries displayed (1 S,G, 0 *,G)
S Chassis(su)->
```

This example displays a detailed level of IPv4 PIM multicast route table information for source address **192.168.202.10**:

```
S Chassis(su)->show ip pim mrt source 192.168.202.10 detail

PIM Sparse Mode Multicast Routing Table
Timers: Uptime/Expires

  192.168.202.10, 224.1.1.1, up 23:56:51
    RPF interface: vlan.0.2334, SPT true, mode ASM
    Upstream join state joined, timer 00:00:25, neighbor 192.233.4.3
    RPF nexthop 192.233.4.3, route 192.168.202.0/24 [110/20]
    DR register state no-info, timer 00:00:00
    RPT prune state pruned, up 23:56:51, override timer 00:00:00
    Downstream S,G state:
      vlan.0.3014, Forward, 23:56:51/00:02:56
        local S,G membership false
        joinPrune state join
        prunePending timer 00:00:00
        assert state winner
        assert timer 00:00:35
      vlan.0.3024, Forward, 23:56:50/00:02:58
        local S,G membership false
        joinPrune state join
```

```
        prunePending timer 00:00:00
        assert state no-info
      vlan.0.3034, Forward, 23:56:50/00:02:55
        local S,G membership false
        joinPrune state join
        prunePending timer 00:00:00
        assert state no-info

1 mroute entries displayed (1 S,G, 0 *,G)
S Chassis(su)->
```

show ip pim mrt type

Use this command to display the IPv4 PIM multicast route (*,G and S,G) table by type.

Syntax

show ip mcache type {**all** | **s-g** | **star-g**} [**source** *source* | **group** *group*] [**interface**] [**detail**] [**brief**] [**summary**]

Parameters

all	Displays all PIM multicast route table entries.
s-g	Displays only S,G PIM multicast route table entries.
star-g	Displays only *,G entries PIM multicast route table entries.
source *source*	(Optional) Displays information about a specific unicast source address table entry.
group *group*	(Optional) Display information about a multicast destination address table entry.
interface	(Optional) Displays interface information for the multicast route table.
detail	(Optional) Displays a detailed level of the specified information.
brief	(Optional) Displays a brief level of specified information.
summary	(Optional) Displays the number of entries found.

Defaults

If no optional parameters are specified, a standard level of information about all source and destination addresses is displayed.

Mode

All command modes.

Examples

This example displays a standard level of information for the IPv4 PIM multicast route table S,G entries for source address **192.168.101.10**:

```
S Chassis(su)->show ip pim mrt type s-g source 192.168.101.10

PIM Sparse Mode Multicast Routing Table
Timers: Uptime/Expires
```

```
  192.168.101.10, 224.1.1.1, up 12:22:54
    RPF interface: vlan.0.3034, SPT true, mode ASM
    Downstream S,G state:
      vlan.0.2334, Forward, 07:16:36/00:02:34
      vlan.0.2601, Forward, 12:22:54/00:00:00

1 mroute entries displayed (1 S,G, 0 *,G)
S Chassis(su)->
```

This example displays a detailed level of information for the IPv4 PIM multicast route table S,G entries for source address **192.168.101.10**:

```
S Chassis(su)->show ip pim mrt type s-g source 192.168.101.10 detail

PIM Sparse Mode Multicast Routing Table
Timers: Uptime/Expires

  192.168.101.10, 224.1.1.1, up 12:24:49
    RPF interface: vlan.0.3034, SPT true, mode ASM
    Upstream join state joined, timer 00:00:23, neighbor 192.168.34.3
    RPF nexthop 192.168.34.3, route 192.168.101.0/24 [110/20]
    DR register state no-info, timer 00:00:00
    RPT prune state pruned, up 12:24:05, override timer 00:00:00
    Downstream S,G state:
      vlan.0.2334, Forward, 07:18:31/00:02:40
        local S,G membership false
        joinPrune state join
        prunePending timer 00:00:00
        RPT join-prune state pruned, up 06:52:30
        RPT local-receiver-exclude false
        RPT prune-pending-timer 00:00:00, prune-expiry-timer 00:02:38
        assert state no-info
      vlan.0.2601, Forward, 12:24:49/00:00:00
        local S,G membership true
        joinPrune state no-info
        prunePending timer 00:00:00
        RPT join-prune state pruned, up 06:52:30
        RPT local-receiver-exclude false
        RPT prune-pending-timer 00:00:00, prune-expiry-timer 00:02:38
        assert state no-info

1 mroute entries displayed (1 S,G, 0 *,G)
S Chassis(su)->
```

show ip pim neighbor

Use this command to display information about discovered PIM neighbors.

Syntax

show ip pim neighbor [*ifName*] [**brief**] [**detail**] [**statistics**]

Parameters

ifName	(Optional) Displays information about a specific PIM interface. This interface must be enabled with PIM as described in "ip pim sparse-mode" on page 64-4.
brief	(Optional) Displays a summary level of information about all PIM neighbors or a specific PIM neighbor.
detail	(Optional) Displays detailed information about all PIM interfaces or a specific PIM interface.
statistics	(Optional) Displays PIM statistics information for all neighbors.

Defaults

If no options are specified, a standard level of information for all PIM neighbors displays.

Mode

All command modes.

Examples

This example shows how to display PIM neighbor information:

```
S Chassis(su)->show ip pim neighbor

 Neighbor Address    Interface      DR Priority    Uptime            Expires
 ------------------------------------------------------------------------------
 192.168.12.2        vlan.0.12      1              00:07:54          00:01:24
 192.168.13.3        vlan.0.13      1              00:07:48          00:01:27
```

This example shows how to display PIM neighbor information for a specific PIM neighbor:

```
S Chassis(su)->show ip pim neighbor vlan.0.12
Neighbor Address    Interface      DR Priority    Uptime            Expires
 ------------------------------------------------------------------------------
 192.168.12.2        vlan.0.12      1              00:07:54          00:01:24
```

Table 64-3 provides an explanation of the command output.

Table 64-3 show ip pim neighbor Output Details

Output...	What it displays...
PIM Neighbor Address	IP address of the PIM neighbor.
Interface	Specifies the interface for the PIM neighbor.
DR Priority	Specifies the value of the designated router priority from the last PIM Hello message received from this neighbor. This object is always zero if pimNeighborDRPriorityPresent is FALSE.

Table 64-3 show ip pim neighbor Output Details (continued)

Output...	What it displays...
Uptime	Specifies the length of time in hours, minutes, and seconds that this PIM neighbor has been in the PIM neighbor table.
Expires	Specifies the length of time in hours, minutes, and seconds until this PIM neighbor will be removed from the IP multicast routing table.

This example shows how to display detailed PIM neighbor information for a specific PIM neighbor:

```
S Chassis(su)->show ip pim neighbor vlan.0.12 detail
Interface vlan.0.12
  PIM Neighbor Address: 192.168.12.2
  PIM Neighbor Uptime: 00:08:02
  PIM Neighbor Expiry: 00:01:16
  PIM Generation Id : 2682437344 (0x9fe2bee0)
  PIM DR Priority: 1
  PIM Lan Prune Delay Present: true
  PIM Lan Prune Delay Tbit Present: false
  PIM Propagation Delay: 500
  PIM Override Interval: 2500
  PIM Generation Id Present: true
  PIM DR Priority Present: true
```

Table 64-4 provides an explanation of the command output.

Table 64-4 show ip pim neighbor detail Output Details

Output...	What it displays...
PIM Neighbor Address	IP address of the PIM neighbor.
PIM Neighbor Uptime	The time since this PIM neighbor last became a neighbor of the local router.
PIM Neighbor Expiry	The minimum time remaining before this PIM neighbor will be aged out. The value zero indicates that this PIM neighbor will never be aged out.
PIM Generation Id	The value of the Generation ID from the last PIM Hello message received from this neighbor. This object is always zero if pimNeighborGenerationIDPresent is FALSE.
PIM DR Priority	The value of the Designated Router Priority from the last PIM Hello message received from this neighbor. This object is always zero if pimNeighborDRPriorityPresent is FALSE.
PIM Lan Prune Delay Present	Evaluates to TRUE if this neighbor is using the LAN Prune Delay option.
PIM Lan Prune Delay Tbit Present	Evaluates to TRUE if this neighbor is using the LAN Prune Delay Tbit option. Whether the T bit was set in the LAN Prune Delay option received from this neighbor. The T bit specifies the ability of the neighbor to disable join suppression.

Table 64-4 show ip pim neighbor detail Output Details (continued)

Output...	What it displays...
PIM Propagation Delay	The value of the Propagation_Delay field of the LAN Prune Delay option received from this neighbor. This object is always zero if pimNeighborLanPruneDelayPresent is FALSE.
PIM Override Interval	The value of the Override_Interval field of the LAN Prune Delay option received from this neighbor. This object is always zero if pimNeighborLanPruneDelayPresent is FALSE.
PIM Generation ID Present	Evaluates to TRUE if this neighbor is using the Generation ID option.
PIM DR Priority Present	Evaluates to TRUE if this neighbor is using the DR Priority option.

This example shows how to display a summary level of PIM neighbor information for a specific PIM neighbor:

```
S Chassis(su)->show ip pim neighbor vlan.0.12 brief
Interface vlan.0.12
  PIM Neighbor Address: 192.168.12.2
  PIM Neighbor Uptime: 00:08:00
  PIM Neighbor Expiry: 00:01:18
  PIM Generation Id : 2682437344 (0x9fe2bee0)
  PIM DR Priority: 1
```

Table 64-5 provides an explanation of the command output.

Table 64-5 show ip pim neighbor brief Output Details

Output...	What it displays...
Neighbor Address	Specifies the PIM neighbor IP address for this information.
Interface	Specifies the PIM interface for this information.
DR Priority	Specifies the priority value of the designated router.
Uptime	Specifies the amount of time this neighbor has been up.
Expires	The minimum time remaining before this PIM neighbor will be aged out. The value zero indicates that this PIM neighbor will never be aged out.

show ip pim rp

Use this command to display the active rendezvous points (RPs) that are cached with associated multicast routing entries.

Syntax

```
show ip pim rp [mapping]
```

Parameters

mapping	(Optional) Displays all RP mappings.

Defaults

If **mapping** is not specified, RP details for each group will not display.

Mode

All command modes.

Examples

This example shows how to display information about active RPs:

```
S Chassis(su)->show ip pim rp
PIM Group-to-RP mapping for active groups with *,G state:

Group: 224.1.1.1, RP: 172.16.1.1
Group: 232.1.1.1, RP: 172.16.1.1
Group: 239.1.1.1, RP: 172.16.1.2, Anycast RP

PIM Group-to-RP mapping for active groups with only S,G state:
```

This example shows how to display information for PIM groups and their associated RPs:

```
SI-1(su)->show ip pim rp mapping
PIM Group to RP Mapping:

    Group(s): 224.0.0.0/4
        RP: 172.16.1.2, Priority: 10, Expiry: 00:02:22, Anycast RP
        RP: 172.16.2.2, Priority: 20, Expiry: 00:02:24

    Group(s): 224.0.0.0/8
        RP: 172.16.1.1, Priority: 100, Expiry: 00:02:22
```

Table 64-6 provides an explanation of the command output.

Table 64-6 show ip pim rp mapping Output Details

Output...	What it displays...
Group(s)	Address of the multicast group(s) about which to display RP data.
RP	Address of the RP for that group.
Priority	RP priority value.
Expiry	Period (in hours:minutes:seconds) in which the next bootstrap message is due from this BSR.
Anycast RP	The RP is an Anycast RP.

show ip pim rp-hash

Use this command to display the rendezvous point (RP) that is being selected for a specified group.

Syntax

show ip pim rp-hash *group-address*

Parameters

group-address	Displays information for the specified group address.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display RP hash information for group **239.0.0.0**:

```
S Chassis(su)->show ip pim rp-hash 239.0.0.0

 RP  192.168.1.1, via  Bootstrap Router
```

show ip pim statistics

Use this command to display PIM statistics for this device.

Syntax

show ip pim statistics

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

Neighbor level statistics can be found using the **show ip pim neighbor statistics** command. Interface level statistics can be found using the **show ip pim interface stat** command.

Example

This example shows how to display PIM statistics information:

```
S Chassis(su)->show ip pim statistics

Time since the stats counters were last reset: 01:37:45
PIM Candidate-RP-Advertisement messages sent: 0
PIM Register messages sent: 466
PIM Register-Stop messages sent: 0
Valid PIM Candidate-RP-Advertisement messages received: 0
Valid PIM Register messages received: 0
Valid PIM Register-Stop messages received: 460
Erroneous PIM Candidate-RP-Advertisement messages received: 0
Erroneous PIM Register messages received: 0
Erroneous PIM Register-Stop messages received: 0
PIM messages with a known but unsupported PIM message type received: 0
PIM messages with an unknown PIM message type received: 0
PIM messages with an unknown PIM version received: 0
PIM messages with an incorrect PIM checksum received: 0
PIM messages with a length too short received: 0
Groups for which non-interface specific (*,G) and/or (S,G) state is stored: 3
Groups for which non-interface specific (S,G) state is stored: 18
{group, interface} pairs for which  (*,G,I) is stored: 15
{source, group, interface} triplets for which (S,G,I) state is stored: 36
```

clear ip mroute

Use this command to purge all or the specified group PIM-SM route state, requiring PIM to relearn all active state.

Syntax

clear ip mroute [**group** *group-address*]

Parameters

group *group-address*	(Optional) Specifies an address of the multicast group to clear PIM-SM route state.

Defaults

If the **group** parameter is not specified, PIM-SM route state for all groups are cleared.

Mode

All command modes.

Usage

This command should be used as a last-resort debug tool. This command only has any effect on PIM-SM state; it has no affect on DVMRP.

Example

This example shows how to clear all PIM-SM route state for this device:

```
S Chassis(su)->clear ip mroute
```

clear ip pim statistics

Use this command to clear all PIM show command counters.

Syntax

clear ip pim statistics

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example clears all PIM show command statistics for this device:

```
S Chassis(rw)->clear ip pim statistics
```

65

IPv6 PIM Commands

This chapter describes the Protocol Independent Multicast (PIM) IPv6 configuration set of commands and how to use them. For information about configuring PIM, refer to the "Multicast Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
ipv6 mroute	65-2
ipv6 pim sparse mode	65-3
ipv6 pim dense-mode	65-4
ipv6 pim ssm	65-5
ipv6 pim static-rp-override	65-5
ipv6 pim state-refresh origination-interval	65-6
ipv6 pim asm-join-filter	65-7
ipv6 pim ssm-join-filter	65-7
ipv6 pim bsr candidate bsr	65-8
ipv6 pim bsr candidate rp	65-9
ipv6 pim dr-priority	65-10
ipv6 pim rp-address	65-10
ipv6 pim anycast-rp	65-11
ipv6 pim graceful-restart	65-12
ipv6 pim multipath	65-13
ipv6 pim neighbor-filter	65-14
clear ipv6 mroute	65-15
clear ipv6 pim statistics	65-15
show ipv6 mcache	65-16
show ipv6 mroute	65-17
show ipv6 pim	65-19
show ipv6 pim anycast-rp	65-20
show ipv6 pim bsr	65-20
show ipv6 pim interface	65-22
show ipv6 pim mrt	65-24

For information about...	Refer to page...
show ipv6 pim mrt type	65-26
show ipv6 pim neighbor	65-27
show ipv6 pim rp	65-29
show ipv6 pim rp-hash	65-30
show ipv6 pim statistics	65-30

ipv6 mroute

Use this command to add or remove a static IPv6 multicast route.

Syntax

ipv6 mroute *<prefix>* {*<prefix-mask>*} | *<prefix/prefix-length>* **vlan** *<vlan-id>* {[*<distance>*] [**tag** *<tag-id>*]} **reject** {[*<distance>*] [**tag** *<tag-id>*]} **blackhole** {[*<distance>*] [**tag** *<tag-id>*]} **interface** *<interface-name>* {[*<distance>*] [**tag** *<tag-id>*]} *<ip-address>* {[**interface** *<interface-name>*] | [**recursive**] [*<distance>*] [**tag** *<tag-id>*] [**probe** {**default** | *<probe-name>*}] **vrf** *<egress-vrf>* {[*<distance>*] [tag *<tag-id>*]}

no ipv6 mroute *<prefix>* {*<prefix-mask>*} | *<prefix/prefix-length>*

Parameters

prefix/prefix-length	Specifies a destination IP address in prefix/prefix-length format.
ipv6-address	Specifies a next hop IP address.
interface *interface-name*	Specifies a next hop interface ID. When entered with the next-hop IPv6 address, it specifies the interface ID the IPv6 address is assigned to.
vlan *vlan-id*	Specifies the next hop VLAN. Valid values for VLAN ID: **1** - **4094**.
vrf *egress-vrf*	Specifies the egress VRF router as the next hop.
blackhole	Specifies that packets destined for this route's subnet are silently dropped. An ICMP network unreachable message is not sent to the packet source.
reject	Specifies that packets destined for this route's subnet are dropped, and an ICMP network unreachable message is sent to the packet source.
recursive	(Optional) Specifies that the next hop interface is determined by route lookup.
distance	(Optional) Specifies an administrative distance metric for this route. Valid values are **1** (default) to **255**. Routes with lower values receive higher preference in route selection.
tag *tag-id*	(Optional) Specifies an OSPF tag ID for this route. Valid values are **1** - **4294967295**.
default	Uses the default static route probe
probe-name	Specifies the name of a probe to use.

Defaults

- If **interface** *interface-name* is not specified when configuring an IPv6 address, a specific interface is not configured for the static route.
- If *distance* is not specified, the default value of 1 will be applied.
- If an OSPF tag ID is not specified, no OSPF tag is associated with the route.
- If **recursive** or **interface** *interface-name* are not specified when configuring an IP address, see usage section below.

Mode

Global configuration**.**

This command is used to configure static multicast routes.

When specifying an IP address as the next hop, it is recommended that you specify the interface the IP address is assigned to. If only the prefix with mask/length and the IP address of the next hop router are entered, and you do not specify the optional **recursive** or the **interface** *interface-name* parameter, when entering the IP address, all configured subnets are searched for a subnet containing the next hop. If found, the static route will be anchored to that interface, else it will become a recursive route.

See “ip mroute” on page 64-2 for IPv4 static multicast route configuration command information.

The **no ipv6 route** command removes the specified static IPv6 route.

Examples

This example shows how to:

- Configure a static route with a prefix and length of **2001:11ac:fd34::/48** and a next hop IPv6 address of **2001:11ac:fd34:3333::4**
- Specify that the next-hop interface should be determined using route lookup
- Assign the OSPF tag **65514** to the route

```
S Chassis(su)->configure
S Chassis(su-config)->ipv6 mroute 2001:11ac:fd34::/48 2001:11ac:fd34:3333::4
recursive tag 65514
S Chassis(su-config)->
```

ipv6 pim sparse mode

Use this command to enable Protocol Independent Multicast (PIM) Sparse Mode (SM) on an IPv6 routing interface.

Syntax

ipv6 pim sparse-mode

no ipv6 pim sparse-mode

Parameters

None.

Defaults

None.

Mode

Interface configuration.

Usage

The “no” form of this command disables IPv6 PIM-SM on an IPv6 interface.

You do not have to enable PIM on a loopback interface for use as a BSR or RP.

Example

This example enables PIM sparse mode on VLAN 1:

```
S Chassis(su-config)->interface vlan 1
S Chassis(su-config-intf-vlan.0.1)->ipv6 pim sparse-mode
```

ipv6 pim dense-mode

Use this command to enable Protocol Independent Multicast (PIM) Dense Mode (DM) on an IPv6 routing interface.

Syntax

ipv6 pim dense-mode

no ipv6 pim dense-mode

Parameters

None.

Defaults

None.

Mode

Interface configuration.

Usage

The “no” form of this command disables PIM dense mode on an interface.

Example

This example enables PIM dense mode on VLAN 1:

```
S Chassis(su-config)->interface vlan 1
S Chassis(su-config-intf-vlan.0.1)->ipv6 pim dense-mode
```

ipv6 pim ssm

Use this command to configure Source Specific Multicast (SSM) mode for the default or a specified multicast group range.

Syntax

ipv6 pim ssm {**default** | *group-address/length*}

no ipv6 pim ssm {**default** | *group-address*/length}

Parameters

default	Specifies that PIM SSM is enabled with the default address-group. The default address groups are enabled for ff34:0000::/16, ff35:0000::/16, ff38:0000::/16 and ff3e:0000::/16.
group-address/length	Specifies that PIM SSM is enabled with the specified IPv6 address range.

Defaults

None.

Mode

Configuration command.

Usage

The "no" form of this command removes PIM SSM configuration. PIM SSM is disabled by default.

When PIM SSM is enabled, the following IPv6 address ranges are enabled by default: **ff34:0000::/16**, **ff35:0000::/16**, **ff38:0000::/16** and **ff3e:0000::/16**. The PIM SSM IPv6 address range is limited to is **ff3x::/32** where (x = 4,5,8, or E).

Example

This example enables PIM SSM for the default group ranges and for a user defined group range of ff3e:2000::/64:

```
S Chassis(su)->configure
S Chassis(su-config)->ip pim ssm default
S Chassis(su-config)->ip pim ssm ff3e:2000::/64
```

ipv6 pim static-rp-override

Use this command to control whether static RP configurations will override dynamic RP information learned for IPv6 groups.

Syntax

ipv6 pim static-rp-override

no ipv6 pim static-rp-override

Defaults

None.

Mode

Configuration command.

Usage

The static RP override feature is enabled by default. If both static and dynamic RP configurations exist, by default the static RP configurations take precedence over the dynamic RP configurations. Disabling this command allows dynamic RP configurations to take precedence over static RP configurations.

The “no” form of this command disables the static RP override feature.

Examples

This example disables static RP override for this device, allowing dynamic RP configurations to take precedence over static RP configurations:

```
S Chassis(su-config)->no ipv6 pim static-rp-override
```

ipv6 pim state-refresh origination-interval

Use this command to set the interval between IPv6 PIM dense mode state refresh messages.

Syntax

ipv6 pim state-refresh origination-interval *interval*

no ipv6 pim state-refresh origination-interval *interval*

Parameters

interval	Specifies the interval in seconds between the sending of PIM dense mode state refresh messages. Default value: **60** seconds.

Defaults

IPv6 PIM dense mode state refresh messages are sent at **60** second intervals by default.

Mode

Configuration command.

Usage

IPv6 PIM dense mode state refresh messages are sent to neighbor routers by the PIM dense mode routers that are connected to a PIM source. State refresh messages convey prune state for the purpose of minimizing overhead to the network.

The “no” form of this command resets the PIM dense mode state refresh message interval to **60** seconds.

Examples

This example sets the PIM dense mode state refresh message interval to **80** seconds:

```
S Chassis(su-config)->ipv6 pim state-refresh origination-interval 80
```

ipv6 pim asm-join-filter

Use this command to specify the Any-Source Multicast groups permitted to cross this interface in either an inbound or outbound direction.

Syntax

ipv6 pim asm-join-filter *standard-acl*

no ipv6 pim asm-join-filter *standard-acl*

Parameters

standard-acl	Specifies the standard ACL containing ASM group permit or deny entries.

Defaults

None.

Mode

Interface command mode.

Usage

The ASM join filter applies a standard permit/deny ACL that defines which Any-Source Multicast groups are permitted to cross this interface either inbound our outbound.

The “no” form of this command removes the specified ASM join filter.

Example

This example defines the ASM groups permitted to cross this interface using the **asmFilter1** standard ACL on VLAN 100:

```
S Chassis(su-config)->interface vlan 100
S Chassis(su-config-intf-vlan.0.100)->ipv6 pim asm-join-filter asmFilter1
S Chassis(su-config-intf-vlan.0.100)->
```

ipv6 pim ssm-join-filter

Use this command to specify the Source-Specific Multicast groups permitted to cross this interface in either an inbound or outbound direction.

Syntax

ipv6 pim ssm-join-filter *extended-acl*

no ipv6 pim ssm-join-filter *extended-acl*

Parameters

standard-acl	Specifies the extended ACL containing SSM group permit or deny entries.

Defaults

None.

Mode

Interface command mode.

Usage

The SSM join filter applies an extended permit/deny ACL, specifying the source or destination IPv6 addresses that define which Source Specific Multicast S,G pairs are permitted to cross the interface.

The "no" form of this command removes the specified SSM join filter.

Example

This example defines the SSM groups permitted to cross this interface using the **ssmFilter1** standard ACL on VLAN 100:

```
S Chassis(su-config)->interface vlan 100
S Chassis(su-config-intf-vlan.0.100)->ip pim ssm-join-filter ssmFilter1
S Chassis(su-config-intf-vlan.0.100)->
```

ipv6 pim bsr candidate bsr

Use this command to enable the router to announce its candidacy as a BootStrap Router (BSR).

Syntax

ipv6 pim bsr candidate bsr *interface-address* [**priority** *priority*]

no ipv6 bsr candidate bsr *interface-address*

Parameters

interface-address	IPv6 address of the BSR candidate interface. With the exception of a loopback interface, the interface used as the BSR candidate must be enabled with PIM as described in "ipv6 pim sparse mode" on page 65-3.
priority *priority*	(Optional) Specifies a BSR priority value ranging from **0–255**. Higher values assign higher priority. The BSR with the larger priority is preferred. If priority values are the same, the IP address breaks the tie. The BSR candidate with the higher IP address is preferred. Default value **0**.

Defaults

If *priority* is not specified, **0** will be applied.

Mode

Configuration command.

Usage

Only one BSR candidate can be configured per router.

The "no" form of this command removes the router as a BSR candidate.

Example

This example sets the BSR priority to 77 on 2001:11ac:fd34::5:

```
S Chassis(su-config)->ipv6 pim bsr-candidate 2001:11ac:fd34::5 priority 77
```

ipv6 pim bsr candidate rp

Use this command to enable the router to advertise itself as a PIM candidate rendezvous point (RP) to the BSR.

Syntax

ipv6 pim bsr candidate rp *pim-interface-address* {[**group-list** *group-list*] [**priority** *priority*]}

no ipv6 pim bsr candidate bsr *pim-interface-address* {[**group-list** *group-list*] [**priority** *priority*]}

Parameters

pim-interface-address	IPv6 address of the interface to advertise as an RP candidate. With the exception of a loopback interface, the interface used as the RP candidate must be enabled with PIM as described in "ipv6 pim sparse mode" on page 65-3.
group-list *group-list*	Specifies a permit only standard access-list containing one or more IPv6 multicast group addresses. All non-permit multicast groups are ignored.
priority *priority*	Specifies an RP priority value, ranging from **0–255**. Lower values assign higher priority. Default value: **192**.

Defaults

If no **group-list** is specified, the specified RP candidate will not be active.

If no **priority** is specified when assigning a group-address or group-list, the priority defaults to **192**.

Mode

Configuration command.

Usage

For each candidate RP, configure groups using a group-list. It is possible to configure a candidate RP without configuring a group list assigned to the RP, but a group list must be specified before this RP will be active. A group-list must exist before it may be used by this command. If a group-list referenced by this command is removed, that configuration will also be removed.

The "no" form of this command removes the candidate RP configuration for the assigned group-list, but resets the priority to the default of **192**, if only the priority is specified.

Examples

This example enables the PIM interface at address **2001:11ac:fd34::7** to advertise itself as an RP candidate with a priority of **5**:

```
S Chassis(su-config)->ipv6 pim rp-candidate 2001:11ac:fd34::7 priority 5
```

This example enables the PIM interface at address **2001:11ac:fd34::7** to advertise itself as an RP candidate with a priority of **5**, for group addresses specified in the the **pimrp** standard access-list:

```
S Chassis(su-config)->ipv6 pim rp-candidate 2001:11ac:fd34::7 group-list pimrp
priority 5
```

ipv6 pim dr-priority

Use this command to set the priority used for the Designated Router (DR) election for this router.

Syntax

ipv6 pim dr-priority *priority*

no ipv6 pim dr-priority *priority*

Parameters

priority	Specifies a priority value for DR selection. Valid values are 0 - 4294967294. Default value: 1

Defaults

None.

Mode

Interface configuration.

Usage

The “no” form of this command disables the DR functionality.

Examples

This example sets the DR priority to 20 on VLAN 1:

```
S Chassis(su-config)->interface vlan 1
S Chassis(su-config-intf-vlan.0.1)->ipv6 pim dr-priority 20
```

ipv6 pim rp-address

Use this command to set an IPv6 static Rendezvous Point (RP) for a multicast group.

Syntax

ipv6 pim rp-address *rp-address* **group-list** *group-list*

no ipv6 pim rp-address *rp-address* **group-list** *group-list*

Parameters

rp-address	Specifies the IP address of the PIM RP router.
group-list *group-list*	Specifies a standard access-list containing one or more multicast groups.

Defaults

None.

Mode

Configuration command

Usage

For each static RP, groups may be configured using a group-list. A group-list must exist before it can be used by this command. If a group-list referenced by this command is removed, the configuration will also be removed.

The "no" form of this command removes the static RP configuration.

Example

This example sets a static RP address at 2010::5 for the multicast groups defined in the standard access-list pimACL1:

```
S Chassis(su-config)->ipv6 pim rp-address 2010::5 group-list pimACL1
S Chassis(su-config)->
```

ipv6 pim anycast-rp

Use this command to configure an anycast Rendezvous Point (RP) set member for a multicast group.

Syntax

ipv6 pim anycast-rp *anycast-address peer-address*

no ipv6 pim anycast-rp *anycast-address peer-address*

Parameters

anycast-address	Specifies the IPv6 address of a loopback interface to be configured on each anycast-RP. The anycast-address is used as the RP address for all members of the anycast-RP set.
peer-address	Specifies the unique peer IPv6 address of a loopback or hardware interface for this anycast RP.

Defaults

None.

Mode

Configuration command.

Usage

The relationship between a source or receiver and the PIM RP router is a one-to-one relationship. The relationship between a source or receiver and an anycast-RP set of routers is a one-to-many relationship, where one of multiple anycast configured RPs is selected by the routing protocol to be the source or receiver RP. The purpose of anycast-RP is to provide a means of fast convergence when a PIM RP router fails.

Anycast-RP provides for the selection of a set of routers to be identified as anycast RPs by configuring:

- A loopback interface with the same IPv6 address for each anycast-RP router in the set
- Either a second loopback interface or another hardware interface to be configured with a unique address for this peer of the anycast-RP set

Each anycast-RP router is configured with the same anycast-RP address and all the peer-addresses of each router in the anycast-RP router set. Each anycast-RP and peer-address combination is configured in its own command line entry using the **ipv6 pim anycast-rp** command.

The routing protocol determines which member of the anycast-RP router set will function as the PIM RP router. Should the PIM RP router fail, the routing protocol determines the next anycast-RP router that will become the new PIM RP router, based upon the routing protocol's routing criteria. Should the failed router return to an operational state, the routing protocol will determine whether a new PIM RP will be selected based upon current conditions.

The "no" form of this command removes a single anycast-RP configuration from the anycast-RP set.

Examples

This example configures an anycast RP set with the anycast address of 2001::1 and peer addresses of 2110::1, 2120::1, and 2130::1 on this anycast-RP router:

```
S Chassis(su-config)->ipv6 pim anycast-rp 2001::1 2110::1
S Chassis(su-config)->ipv6 pim anycast-rp 2001::1 2120::1
S Chassis(su-config)->ipv6 pim anycast-rp 2001::1 2130::1
```

ipv6 pim graceful-restart

Use this command to set the multicast graceful-restart period, which is the period of time in which a restarting router and its neighbors can continue to forward multicast packets during the failover.

Syntax

```
ipv6 pim graceful-restart [period value]
no ipv6 pim graceful-restart
```

Parameters

period *value*	Specifies the maximum amount of time in seconds that this router will remain in multicast graceful-restart mode starting at the time it enters graceful-restart. Possible values are **30–600** seconds. The default value is **120** seconds.

Defaults

The default value is **120** seconds.

Mode

Configuration command.

Usage

Multicast graceful restart requires OSPF graceful restart. Ensure that you have configured and enabled OSPF graceful restart before you enable multicast graceful restart. For more information

about configuring and enabling OSPF graceful restart, see Chapter 73, **OSPFv2 Commands** or Chapter 74, **OSPFv3 Commands**.

The "no" form of this command disables the multicast graceful-restart period.

To view the current graceful-restart setting, use the **show running-config pim** command.

Example

This example shows the multicast graceful-restart period set to 180 seconds.

```
S Chassis(su-config)->ipv6 pim graceful-restart period 180
```

ipv6 pim multipath

Use this command to allow PIM multicast to either load share over ECMP paths or have a single deterministic next hop for ECMP paths.

Syntax

ipv6 pim multipath {**hash** | **highest-nexthop**}

no ipv6 pim multipath {**hash** | **highest-nexthop**}

Parameters

hash	Configure multipath to choose a PIM next hop based on a hash of the source (or RP) being queried.
highest-nexthop	Configure multipath to choose the highest address as the PIM next hop.

Defaults

Multipath will use the first nexthop learned for an ECMP route.

Mode

Configuration command.

Usage

Multipath provides the ability to define the mechanism by which PIM chooses the nexthop. By default, PIM uses the first learned next hop. You can change multipath to use the highest next hop or a next hop based on a hash of the source IP address.

For a deterministic next hop, the **highest-nexthop** algorithm chooses the numerically highest next hop. The **hash** algorithm will attempt to spread multicast over all possible next hops.

For the least disruption during network events (including bootup), use the default (first next-hop). The first next hop learned will be the one used regardless of added or removed next hops.

Multipath also allow PIM graceful restart to choose the same next hop after a router failover because the **highest-nexthop** and the **hash** algorithms will choose the same next hop, assuming the set of next hops is consistent after the failover.

The "no" form of this command resets the multipath configuration to the default value (using the first next hop).

To view the current multipath setting, use the **show running-config pim** command.

Example

This example shows setting the multipath configuration to the highest address as the PIM next hop.

```
S Chassis(su-config)->ipv6 pim multipath highest-nexthop
```

ipv6 pim neighbor-filter

Use this command to specify PIM neighbors to allow.

Syntax

ipv6 pim neighbor-filter *neighbor-filter*

no ipv6 pim neighbor-filter *neighbor-filter*

Parameters

neighbor-filter	Specifies the name of a standard access-list containing a list of neighbors to allow on this IPV6 interface.

Defaults

None.

Mode

Interface configuration.

Usage

The “no” form of this command disables IPv6 PIM neighbor filtering on this interface.

Examples

This example sets the neighbor-filter to permit only 2010::100:10 and 2010::101:10 to participate in the PIM protocol on VLAN 1:

```
S Chassis(su-config)->ipv6 access-list standard pim6_nbr_fltr
S Chassis(su-cfg-std-acl-pim_*fltr)->permit host 2010::100:10
S Chassis(su-cfg-std-acl-pim_*fltr)->permit host 2010::101:10
S Chassis(su-cfg-std-acl-pim_*fltr)->exit
S Chassis(su-config)->interface vlan 1
S Chassis(su-config-intf-vlan.0.1)->ipv6 pim neighbor-filter pim6_nbr_fltr
```

clear ipv6 mroute

Use this command to purge all or the specified group PIM route state, requiring PIM to relearn all active state.

Syntax

clear ipv6 pim mroute [**group** *group-address*]

Parameters

group *group-address*	(Optional) Specifies an address of the multicast group to clear the PIM route state.

Defaults

If **group** *group-address* is not specified, all groups are cleared.

Mode

All command modes.

Usage

This command should be used as a last-resort debug tool. This command only has any effect on PIM-SM state; it has no affect on DVMRP.

Examples

This example purges all PIM route state for this device:

```
S Chassis(su)->clear ip mroute
S Chassis(su)->
```

clear ipv6 pim statistics

Use this command to clear all PIM show command counters.

Syntax

clear ipv6 pim statistics

Defaults

None.

Mode

All command modes.

Example

This example clears all PIM show command IPv6 statistics for this device:

```
S Chassis(su)->clear ipv6 pim statistics
```

show ipv6 mcache

Use this command to display the IPv6 multicast forwarding cache used to program the hardware flow.

Syntax

show ipv6 mcache [**source** *source* | **group** *group*] [**interface**] [**verbose**] [**brief**] [**summary**] [**statistics**] [**-wide**]

Parameters

source *source*	(Optional) Displays information about a specific unicast source address.
group *group*	(Optional) Display information about a multicast destination address.
interface	(Optional) Displays mcache information filtered for the inbound interface.
verbose	(Optional) Displays a detailed level of mcache information.
brief	(Optional) Displays a brief level of specified information.
summary	(Optional) Displays the number of entries found.
statistics	(Optional) Displays IPv6 mcache statistics.
-wide	(Optional) Displays up to 132 characters per line if applicable.

Defaults

If no optional parameters are specified, a standard level of information about all source and destination addresses is displayed. The statistics verbose option uses a standard 80 column format.

Mode

All command modes.

Examples

This example displays a standard level of information for the IPv6 mcache:

```
S Chassis(su)->show ipv6 mcache

IP Multicast Cache Table
FLAGS: S - L2 flow, M - MFIB entry, N - Null OIF, T - static
       C - CPU Flow (not in HW), A - flow active, X - pending deletion
       F - register

 Group            Source           Interface    Flags       Age
 ff04::1:1:1:1    2502::10         vlan.0.2502  MA       0d 23h:14m:53s
     Outgoing interface list:
       vlan.0.2503
       vlan.0.2504
 ff04::1:1:1:1    2503::10         vlan.0.2503  MA       0d 23h:14m:53s
     Outgoing interface list:
       vlan.0.2502
       vlan.0.2504
```

```
 ff04::1:1:1:1    2504::10         vlan.0.2504  MA       0d 23h:14m:53s
     Outgoing interface list:
       vlan.0.2502
       vlan.0.2503

3 mcache entries displayed
S Chassis(su)->
```

This example displays IPv6 mcache statistics:

```
S Chassis(su)->show ipv6 mcache statistics

IP Multicast Cache Statistics
These counters represent IP Multicast packets seen in the soft-path only.

Total IP Multicast packets received        : 47
IPv6 IP Multicast packets received         : 47
Multicast packets dropped due to TTL       : 0
Multicast packets dropped due to ACL       : 0
Data packets sent up to PIM at DR          : 14
Register packets received at RP            : 0
Decapsulated register packets transmitted  : 0
```

show ipv6 mroute

Use this command to display the IPv6 multicast route table.

Syntax

show ipv6 mroute [**source** *source* | **group** *group* | **interface** *interface*] [**brief**] [**type** {**all** | **s-g** | **star-g**}] [**ssm**] [**summary**] [**-wide**]

Parameters

source *source*	(Optional) Displays information about a specific unicast source address.
group *group*	(Optional) Displays information about a multicast destination address.
interface *interface*	(Optional) Displays information about a specific interface entered in format vlan.0.*x*.
brief	(Optional) Displays a brief level of information.
type all | **s-g** | **star-g**	(Optional) Displays the specified route entry type: • **all** – displays all route entries (default) • **s-g** – displays S,G entries • **star-g** – displays *,G entries
ssm	(Optional) Displays all SSM multicast routes.
summary	(Optional) Displays a one line summary for each multicast route based upon the source, group, or interface filter option entered.
-wide	(Optional) Displays up to 136 characters per line.

Defaults

If no optional parameters are specified, a standard level of information about all source and destination addresses is displayed.

Mode

All command modes.

Usage

For the **show ipv6 mroute** command, wide is automatically configured if terminal width is set equal to or greater than 124 characters.

Example

This example displays IPv6 multicast routing table information for all multicast routes:

```
S Chassis(su)->show ipv6 mroute
IPV6 Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Source is connected,
       F - Register flag, N - No outgoing interfaces, J - Join SPT
       Q - Null Forwarding Entry, s - SSM Group

(1111:1111:1111:1111:2222:2222:2222:2222, ff05:1111:2222:3333:4444:5555::7777)
  Uptime 00:01:54, flag: SCF
  Incoming interface: vlan.0.101
  Outgoing interface list:
    register, Forward/Sparse, 00:01:54/00:00:00

(1111:1111:1111:1111:2222:2222:2222:2222, ff08::7777)
  Uptime 00:01:54, flag: SCF
  Incoming interface: vlan.0.101
  Outgoing interface list:
    register, Forward/Sparse, 00:01:54/00:00:00

(101::12, ff09::2)
  Uptime 00:01:57, flag: SCF
  Incoming interface: vlan.0.101
  Outgoing interface list:
    register, Forward/Sparse, 00:01:57/00:00:00

(102::10, ff3e::1)
  Uptime 00:01:57, flag: SCs
  Incoming interface: vlan.0.102
  Outgoing interface list:

4 mroute entries displayed (4 S,G, 0 *,G)
```

show ipv6 pim

Use this command to display summary tables of IPv6 PIM interfaces, neighbors, BSR, and group-to-RP mappings.

Syntax

show ipv6 pim

Parameters

None.

Defaults

None.

Mode

All command modes

Example

This example displays summary tables of IPv6 PIM interfaces, neighbors, BSR, and group-to-RP mappings:

```
S Chassis(su)->show ipv6 pim

[PIM Interfaces]
 Interface    Address          Nbr    Hello  DR         Status  DR-Address
                               Count  Intvl  Priority
 ---------------------------------------------------------------------------
 vlan.0.2501  ----             0      30     1          DOWN    ----
 vlan.0.2502  fe80::21f:45ff:fe5b:f5cf  0      30     1          UP      fe80::21f:45ff:fe5b:f5cf
 vlan.0.2503  fe80::21f:45ff:fe5b:f5cf  0      30     1          UP      fe80::21f:45ff:fe5b:f5cf
 vlan.0.2504  fe80::21f:45ff:fe5b:f5cf  0      30     1          UP      fe80::21f:45ff:fe5b:f5cf
 vlan.0.3014  fe80::21f:45ff:fe5b:f5cf  1      30     1          UP      fe80::21f:45ff:fe5b:f5cf

 5 PIM enabled interfaces

[PIM Neighbors]
 Neighbor Address    Interface      DR Priority    Uptime            Expires
 ---------------------------------------------------------------------------
 fe80::211:88ff:fe37:a582    vlan.0.3014    1              00:04:44          00:01:36

 1 PIM neighbor

[PIM BSR]
 PIMv2 Elected Bootstrap Router Information:
    BSR Address: 3014::4
    BSR Hash Mask Length: 126
    BSR Priority: 0
    Next BSM: 00:00:29

 This Router is a Candidate Bootstrap Router (CBSR)
    Candidate BSR Address: 3014::4
    Hash Mask Length: 126
    Priority: 0

[PIM Group-To-RP Mappings]
 Group Range           RP Address         Mode  Active  Origin    Anycast
```

```
------------------------------------------------------------------------
ff00::/8              2005::5           ASM   Yes     Static    Yes
ff04::/16             2005::5           ASM   Yes     Static    Yes
ff3e::/32             ::                SSM   Yes     Static    no-info
ff00::/8              172:16:4:1::1     ASM   No      BSR       No
ff04::/16             172:16:4:1::1     ASM   No      BSR       No

5 PIM Group to RP mappings (3 static, 2 via BSR)
```

show ipv6 pim anycast-rp

Use this command to display RP anycast information for all or a specified RP.

Syntax

show ipv6 pim anycast-rp [**rp-address** *rp-address*]

Parameters

rp-address	(Optional) Specifies the IP address of the PIM RP router to display.

Defaults

If no RP IP-address is specified, information for all RPs is displayed.

Mode

All command modes.

Example

```
S Chassis(su)->show ipv6 pim anycast-rp rp-address 2005::5

PIM Anycast RP Configuration

  Anycast-RP 2005::5
    Peer 172:16:1:1::1
    Peer 172:16:4:1::1    (local router)
S Chassis(su)->
```

show ipv6 pim bsr

Use this command to display IPv6 BootStrap Router (BSR) information.

Syntax

show ipv6 pim bsr [**detail**]

Parameters

detail	(Optional) Displays a detailed level of information for the BSR.

Defaults

If **detail** is not specified, a standard level of BSR information is displayed.

Mode

All command modes.

Examples

This example displays a standard level of BSR information:

```
S Chassis(su)->show ipv6 pim bsr
 PIMv2 Elected Bootstrap Router Information:
    BSR Address: 3014::4
    BSR Hash Mask Length: 126
    BSR Priority: 0
    Next BSM: 00:00:06

 This Router is a Candidate Bootstrap Router (CBSR)
    Candidate BSR Address: 3014::4
    Hash Mask Length: 126
    Priority: 0
S Chassis(su)->
```

This example displays a detailed level of BSR information:

```
S Chassis(su)->show ipv6 pim bsr detail
 PIMv2 Elected Bootstrap Router Information:
    BSR Address: 3014::4
    BSR Hash Mask Length: 126
    BSR Priority: 0
    Next BSM: 00:00:44

 This Router is a Candidate Bootstrap Router (CBSR)
    Candidate BSR Address: 3014::4
    Hash Mask Length: 126
    Priority: 0
    Elected BSR: true
    Next BSM: 00:00:44
S Chassis(su)->
```

Table 65-1 provides an explanation of the command output.

Table 65-1 show ipv6 pim bsr Output Details

Output...	What it displays...
BSR Address	IPv6 address of the bootstrap router.
BSR Hash Mask Length	Length of a mask that is to be added with the group address before the hash function is called. This value is hard-coded to 126.
BSR Priority	Priority as set using “**ipv6 pim bsr candidate bsr**” on page 65-8.
BSR Expire	Period in which the next bootstrap message is due from this BSR (in hours:minutes:seconds). After 24 hours, format will change into days:hours and, after a week, will change into weeks:days.

Table 65-1 show ipv6 pim bsr Output Details (continued)

Output...	What it displays...
Candidate BSR Address	The (unicast) address that the local router will use to advertise itself as a Candidate-BSR.
Hash Mask Length	The hash mask length (used in the RP hash function) that the local router will advertise in its Bootstrap messages for this zone. This value is hard-coded to 126 for Candidate BSR Address Types **ipv6** and **ipv6z**.
Priority	The priority value for the local router as a Candidate-BSR for this zone. Numerically higher values for this object indicate higher priorities.
Elected BSR	Whether the local router is the elected BSR for this zone. If the value is false, the Next BSM timer does not appear in the output.
Next BSM	The time remaining before the local router next originates a Bootstrap message for this zone.

show ipv6 pim interface

Use this command to display information about PIM interfaces that are currently up (not shutdown).

Syntax

show ipv6 pim interface [*ifName*] [**brief**] [**detail**] [**statistics**]

Parameters

ifName	(Optional) Displays information for the specified PIM interface. Interface name format is **vlan.***x*.*y*.
brief	(Optional) Displays a summary level of information for all or the specified IPv6 interface
detail	(Optional) Displays a detailed level of information for all or the specified IPv6 interface.
statistics	(Optional) Displays PIM statistics for all or the specified IPv6 interface.

Defaults

If no option is not specified, a standard level of PIM information is displayed for all interfaces in a table format.

Mode

All command modes.

Examples

This example displays a standard level of interface configuration information for VLAN 2502:

```
S Chassis(su)->show ipv6 pim interface vlan.0.2502

 Interface    Address                 Nbr    Hello  DR         Status  DR-Address
                                      Count  Intvl  Priority
 ------------------------------------------------------------------------------
 vlan.0.2502  fe80::21f:45ff:fe5b:f5cf  0      30     1          UP      fe80::21f:45ff:fe5b:f5cf
S Chassis(su)->
```

Table 65-2 provides an explanation of the **show ipv6 interface** command output.

Table 65-2 show ipv6 pim interface Output Details

Output...	What it displays...
Interface	Specifies the interface name for the displayed line of information.
Address	Specifies the PIM IPv6 address for the displayed line of information.
Nbr Count	Specifies the number of neighbors for the specified interface.
Hello Intvl	Specifies the value of the Hello Interval.
DR Priority	Specifies the priority value of the designated router.
Status	Specifies the current status of the PIM interface.
DR-Address	Specifies the IPv6 address of the designated router.

This example displays a detailed level of interface configuration information for VLAN 2502:

```
S Chassis(su)->show ipv6 pim interface vlan.0.2502 detail

Interface vlan.0.2502
  PIM IP Address is fe80::21f:45ff:fe5b:f5cf
  PIM version: 2, mode: sparse
  PIM DR Primary Address: fe80::21f:45ff:fe5b:f5cf
  PIM Hello Interval: 30
  PIM Triggered Hello Interval: 5
  PIM Join Prune Interval: 60
  PIM Hello Holdtime: 105
  PIM Join Prune Holdtime: 210
  PIM Generation Id Value: 3504619787 (0xd0e4410b)
  PIM Neighbor Count: 0
  PIM Propagation Delay: 500
  PIM Override Interval: 2500
  PIM DR Priority: 1
  PIM Lan Delay Enabled: true
  PIM Effective Propagation Delay: 500
  PIM Effective Override Interval: 2500
  PIM Suppression Enabled: true
  PIM DR Priority Enabled: true
  PIM Assert Interval: 177
  PIM Assert Holdtime: 180
S Chassis(su)->
```

This example displays PIM statistics information for interface VLAN 2502:

```
S Chassis(su)->show ipv6 pim interface statistics vlan.0.2502

Interface vlan.0.2502
  Valid PIM Hello messages sent: 101
  Valid PIM Join/Prune messages sent: 0
  Valid PIM Assert messages sent: 0
  Valid PIM Bootstrap Router messages sent: 54
  Erroneous PIM Hello messages received: 0
```

```
  PIM messages received from a neighbor before a Hello: 0
  Unknown options received: 0
S Chassis(su)->
```

show ipv6 pim mrt

Use this command to display the IPv6 PIM and DVMRP multicast route (*,G and S,G) table.

Syntax

show ipv6 pim mrt [**source** *source* | **group** *group*] [**interface**] [**detail**] [**brief**] [**summary**]

Parameters

source *source*	(Optional) Displays information about a specific unicast source address.
group *group*	(Optional) Display information about a multicast destination address.
interface	(Optional) Displays information for the multicast route table filtered based upon the inbound interface.
detail	(Optional) Displays a detailed level of multicast route table information.
brief	(Optional) Displays a brief level of specified information.
summary	(Optional) Displays the number of entries found.

Defaults

If no optional parameters are specified, a standard level of information about all source and destination addresses is displayed.

Mode

All command modes.

Usage

This command provides insight into PIM specific data for an mroute such as protocol state and timers for purposes of debugging PIM.

Examples

This example displays a standard level of information for the IPv6 PIM multicast route table for source address **2502::10**:

```
S Chassis(su)->show ipv6 pim mrt source 2502::10

PIM Sparse Mode Multicast Routing Table
Timers: Uptime/Expires

  2502::10, ff04::1:1:1:1, up 1d, 02:33:23
    RPF interface: vlan.0.2502, SPT true, mode ASM
    Downstream S,G state:
      vlan.0.2504, Forward, 1d, 02:32:56/00:00:00
```

```
  2502::10, ff04::1:1:1:2, up 1d, 02:32:56
    RPF interface: vlan.0.2502, SPT false, mode ASM
    Downstream S,G state:
      vlan.0.2504, Forward, 1d, 02:32:56/00:00:00

  2502::10, ff04::1:1:1:3, up 1d, 02:32:56
    RPF interface: vlan.0.2502, SPT false, mode ASM
    Downstream S,G state:
      vlan.0.2504, Forward, 1d, 02:32:56/00:00:00

3 mroute entries displayed (3 S,G, 0 *,G)
S Chassis(su)->
```

This example displays a detailed level of IPv6 PIM multicast route table information for source address **2502::10**:

```
S Chassis(su)->show ipv6 pim mrt source 2502::10 detail

PIM Sparse Mode Multicast Routing Table
Timers: Uptime/Expires

  2502::10, ff04::1:1:1:1, up 1d, 02:36:04
    RPF interface: vlan.0.2502, SPT true, mode ASM
    Upstream join state joined, timer 00:00:00, neighbor ::
    RPF nexthop 2502::10, route 2502::/64 [0/0]
    DR register state prune, timer 00:01:05
    RPT prune state not-pruned, up 1d, 02:35:41, override timer 00:00:00
    Downstream S,G state:
      vlan.0.2504, Forward, 1d, 02:35:37/00:00:00
        local S,G membership true
        joinPrune state no-info
        prunePending timer 00:00:00
        assert state no-info

  2502::10, ff04::1:1:1:2, up 1d, 02:35:37
    RPF interface: vlan.0.2502, SPT false, mode ASM
    Upstream join state joined, timer 00:00:00, neighbor ::
    RPF nexthop 2502::10, route 2502::/64 [0/0]
    DR register state no-info, timer 00:00:00
    Downstream S,G state:
      vlan.0.2504, Forward, 1d, 02:35:37/00:00:00
        local S,G membership true
        joinPrune state no-info
        prunePending timer 00:00:00
        assert state no-info

  2502::10, ff04::1:1:1:3, up 1d, 02:35:37
    RPF interface: vlan.0.2502, SPT false, mode ASM
    Upstream join state joined, timer 00:00:00, neighbor ::
    RPF nexthop 2502::10, route 2502::/64 [0/0]
```

```
    DR register state no-info, timer 00:00:00
    Downstream S,G state:
      vlan.0.2504, Forward, 1d, 02:35:37/00:00:00
        local S,G membership true
        joinPrune state no-info
        prunePending timer 00:00:00
        assert state no-info

3 mroute entries displayed (3 S,G, 0 *,G)
S Chassis(su)->
```

show ipv6 pim mrt type

Use this command to display the IPv6 PIM multicast route (*,G and S,G) table by type.

Syntax

show ipv6 pim mrt type {**all** | **s-g** | **star-g**} [**source** *source* | **group** *group*] [**interface**] [**detail**] [**brief**] [**summary**]

Parameters

all	Displays all PIM multicast route table entries.
s-g	Displays only S,G PIM multicast route table entries.
star-g	Displays only *,G entries PIM multicast route table entries.
source *source*	(Optional) Displays information about a specific unicast source address table entry.
group *group*	(Optional) Display information about a multicast destination address table entry.
interface	(Optional) Displays interface information for the multicast route table.
detail	(Optional) Displays a detailed level of the specified information.
brief	(Optional) Displays a brief level of specified information.
summary	(Optional) Displays the number of entries found.

Defaults

If no optional parameters are specified, a standard level of information about all source and destination addresses is displayed.

Mode

All command modes.

Example

This example displays a standard level of information for all IPv6 PIM multicast route table types for source address **2502::10**:

```
S Chassis(su)->show ipv6 pim mrt type all source 2502::10

PIM Sparse Mode Multicast Routing Table
Timers: Uptime/Expires
```

```
  2502::10, ff04::1:1:1:1, up 01:27:25
    RPF interface: vlan.0.2502, SPT true, mode ASM
    Downstream S,G state:
      vlan.0.2504, Forward, 01:26:58/00:00:00

  2502::10, ff04::1:1:1:2, up 01:26:58
    RPF interface: vlan.0.2502, SPT false, mode ASM
    Downstream S,G state:
      vlan.0.2504, Forward, 01:26:58/00:00:00

  2502::10, ff04::1:1:1:3, up 01:26:58
    RPF interface: vlan.0.2502, SPT false, mode ASM
    Downstream S,G state:
      vlan.0.2504, Forward, 01:26:58/00:00:00

3 mroute entries displayed (3 S,G, 0 *,G)
S Chassis(su)->
```

show ipv6 pim neighbor

Use this command to display information about discovered IPv6 PIM neighbors.

Syntax

show ipv6 pim neighbor [*ifName*] [**brief**] [**detail**] [**statistics**]

Parameters

ifName	(Optional) Displays neighbor information for the specified PIM interface. Interface name format is **vlan.***x.y.*
brief	(Optional) Displays a summary level of neighbor information for all or the specified IPv6 interface
detail	(Optional) Displays a detailed level of neighbor information for all or the specified IPv6 interface.
statistics	(Optional) Displays PIM neighbor statistics for all or the specified IPv6 interface.

Defaults

If no optional parameters are specified, a standard level of information about all PIM interfaces are displayed.

Mode

All command modes.

Examples

This example displays a standard level of IPv6 PIM neighbor information for interface VLAN 3014:

```
S Chassis(su)->show ipv6 pim neighbor vlan.0.3014
```

```
 Neighbor Address            Interface      DR Priority Uptime           Expires
 ------------------------------------------------------------------------------
 fe80::211:88ff:fe37:a582    vlan.0.3014    1           03:41:40         00:01:44

 1 PIM neighbor  for interface vlan.0.3014
```

Table 65-2 provides an explanation of the **show ipv6 pim neighbor** command output.

Table 65-3 show ipv6 pim neighbor Output Details

Output...	What it displays...
Neighbor Address	IPv6 address of the PIM neighbor.
Interface	The interface on this device the neighbor address is neighbor to.
DR Priority	Specifies the value of the designated router priority from the last PIM Hello message received from the neighbor. This object is zero if the pimNeighborDRPriorityPresent object is FALSE.
Uptime	Specifies the length of time in hours, minutes, and seconds that this PIM neighbor has been in the PIM neighbor table.
Expires	Specifies the length of time in hours, minutes, and seconds until this PIM neighbor will be removed from the IP multicast routing table.

This example displays a detailed level of PIM neighbor information for VLAN 3014:

```
S Chassis(su)->show ipv6 pim neighbor vlan.0.3014 detail

Interface vlan.0.3014
  PIM Neighbor Address: fe80::211:88ff:fe37:a582
  PIM Neighbor Secondary Address: 3014::1
  PIM Neighbor Uptime: 03:42:09
  PIM Neighbor Expiry: 00:01:15
  PIM Generation Id : 3662994102 (0xda54dab6)
  PIM DR Priority: 1
  PIM Lan Prune Delay Present: true
  PIM Lan Prune Delay Tbit Present: false
  PIM Propagation Delay: 500
  PIM Override Interval: 2500
  PIM Generation Id Present: true
  PIM DR Priority Present: true

 1 PIM neighbor  for interface vlan.0.3014
S Chassis(su)->
```

This example displays neighbor statistics information for interface VLAN 3014:

```
S Chassis(su)->show ipv6 pim neighbor statistics

Interface vlan.0.3014
  Neighbor Address: fe80::211:88ff:fe37:a582
  Valid PIM Hello messages received: 446
  Valid PIM Join/Prune messages received: 0
  Valid PIM Assert messages received: 0
```

```
  Valid PIM Bootstrap messages received: 0
  Erroneous PIM Join/Prune messages received: 0
  Erroneous PIM Assert messages received: 0
  Erroneous PIM Bootstrap messages received: 0
S Chassis(su)->
```

show ipv6 pim rp

Use this command to display the active IPv6 rendezvous points (RPs) that are cached with associated multicast routing entries.

Syntax

show ipv6 pim rp [**mapping**]

Parameters

brief	(Optional) Display all RP mappings.

Defaults

If **mapping** is not specified, only active RP mappings are displayed.

Mode

All command modes.

Examples

This example displays a standard level of information for active RP mappings:

```
S Chassis(su)->show ipv6 pim rp

PIM Group-to-RP mapping for active groups with *,G state:

Group: ff04::1:1:1:1, RP: 172:16:4:1::1

PIM Group-to-RP mapping for active groups with only S,G state:

Group: ff04::1:1:1:2, RP: 172:16:4:1::1
Group: ff04::1:1:1:3, RP: 172:16:4:1::1
```

This example displays a information for all RP mappings:

```
S Chassis(su)->show ipv6 pim rp mapping

PIM Group to RP Mapping:

    Group(s): ff3e::/32
        RP: ::, via Static Configuration

    Group(s): ff00::/8
        RP: 172:16:4:1::1, Priority: 192, Expiry: 00:02:21

    Group(s): ff04::/16
```

```
        RP: 172:16:4:1::1, Priority: 192, Expiry: 00:02:21

 3 PIM Group to RP mappings (1 static, 2 via BSR)
```

Table 65-2 provides an explanation of the **show ipv6 pim rp mapping** command output.

Table 65-4 show ipv6 pim rp mapping Output Details

Output...	What it displays...
Group(s)	The address of the multicast group(s) about which to display RP data.
RP	The address of the RP for the specified group.
Priority	The RP priority value.
Expiry	The period in hours, minutes, and seconds in which the next bootstrap message is due from this BSR.

show ipv6 pim rp-hash

Use this command to display the rendezvous point (RP) selected for the specified group.

Syntax

show ipv6 pim rp-hash *group-address*

Parameters

group-address	The group-address of the RP to display.

Defaults

None.

Mode

All command modes.

Examples

This example displays a standard level of information for active RP mappings:

```
S Chassis(su)->show ipv6 pim rp-hash ff04::1:1:1:2

 RP  172:16:4:1::1, via  Bootstrap Router
S Chassis(su)->
```

show ipv6 pim statistics

Use this command to display IPv6 PIM statistics for this device.

Syntax

show ipv6 pim statistics

Defaults

None.

Mode

All command modes.

Usage

Neighbor level statistics can be found using the **show ipv6 pim neighbor statistics** command. Interface level statistics can be found using the **show ipv6 pim interface stat** command.

Example

This example displays IPv6 PIM statistics for this device:

```
S Chassis(su)->show ipv6 pim statistics

Time since the stats counters were last reset: 05:47:38
PIM Candidate-RP-Advertisement messages sent: 0
PIM Register messages sent: 1147
PIM Register-Stop messages sent: 1147
Valid PIM Candidate-RP-Advertisement messages received: 0
Valid PIM Register messages received: 1147
Valid PIM Register-Stop messages received: 1147
Erroneous PIM Candidate-RP-Advertisement messages received: 0
Erroneous PIM Register messages received: 0
Erroneous PIM Register-Stop messages received: 0
PIM messages with a known but unsupported PIM message type received: 0
PIM messages with an unknown PIM message type received: 0
PIM messages with an unknown PIM version received: 0
PIM messages with an incorrect PIM checksum received: 1
PIM messages with a length too short received: 0
Groups for which non-interface specific (*,G) and/or (S,G) state is stored: 3
Groups for which non-interface specific (S,G) state is stored: 7
{group, interface} pairs for which  (*,G,I) is stored: 2
{source, group, interface} triplets for which (S,G,I) state is stored: 6
S Chassis(su)->
```

66

MSDP Commands

This chapter describes the MSDP (Multicast Source Discovery Protocol) set of commands and how to use them. For information about configuring MSDP, refer to the "MSDP Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

Note: This feature requires licenses for the following S-Series platforms:

- For the S130 platform: **S-EOS-L3-S130** (S130 class I/O and SSA130)
- For the S150 platform: **S-EOS-L3-S150** (S150 class I/O and SSA150)

The S155/S140/S180 platforms and SSA180 platform are fully entitled to all features and do not require a license.

For information about...	Refer to page...
show ip msdp peer	66-1
show ip msdp peer	66-1
clear ip msdp peer	66-3
ip msdp shutdown	66-3
ip msdp originator-id	66-4
show ip msdp sa-cache	66-5
clear ip msdp sa-cache	66-5
ip msdp sa-filter in	66-6
ip msdp sa-filter out	66-6
ip msdp mesh-group	66-7
show ip msdp summary	66-8
clear ip msdp peer statistics	66-8

show ip msdp peer

Use this command to display detailed information about an MSDP peer.

Syntax

show ip msdp peer [*peer address*]

Parameters

peer-address	(Optional) Specifies the IP address of the MSDP peer to display.

Defaults

All MSDP peers are displayed.

Mode

All command modes.

Usage

If this command is run without the peer-address parameter, all MSDP peers are displayed.

Examples

This example shows how to display information about MSDP peer 192.168.30.20:

```
S Chassis(su-config)->show ip msdp peer 192.168.30.20
MSDP Peer 192.168.30.20, AS 300
 Connection status:
  State: ESTABLISHED, Connection source: vlan.0.30
  Uptime: 2d, 12:30:56, Messages sent/received: 4167/4163
 Peer ttl threshold: 0
 SAs learned from this peer: 0
 SA Filtering:
  Input (S,G) filter: none
  Output (S,G) filter: none
 Mesh group: none
```

ip msdp peer

Use this command to enable MSDP by configuring an MSDP peer to the local router.

Syntax

ip msdp peer *peer-address* **connect-source** *type-number* [**remote-as** *as-number*]

[**no**] **ip msdp peer** *peer-address* **connect-source** *type-number* [**remote-as** *as-number*]

Parameters

msdp peer *peer-address*	Specifies the IP address of the MSDP peer.
connect-source *type-number*	Specifies the identifier (type number) of the connecting source.
remote-as *as-number*	(Optional) Specifies the identifier (as-number) of the remote autonomous system

Defaults

None.

Mode

Global configuration mode.

Usage

Use the "no" form of this command to delete an MSDP peer.

Examples

This example shows 192.168.30.20 configured as an MSDP peer whose connect source is VLAN 0.30 and the remote AS is 300:

```
S Chassis(su-config)->ip msdp peer 192.168.30.20 connect-source vlan.0.30
remote-as 300
```

clear ip msdp peer

Use this command to clear the TCP connection to an MSDP peer and reset all MSDP message counters.

Syntax

clear ip msdp peer [*peer address*]

Parameters

peer-address	(Optional) Specifies the IP address of the MSDP peer to which the TCP connection is to be cleared.

Defaults

All MSDP peers are cleared.

Mode

Global configuration mode.

Usage

If this command is run without the peer-address parameter, all MSDP peers are cleared.

Examples

This example shows how to clear the connection to MSDP peer 192.168.30.20:

```
S Chassis(su-config)->clear ip msdp peer 192.168.30.20
```

ip msdp shutdown

Use this command to administratively shut down a configured MSDP peer.

Syntax

ip msdp shutdown *peer-address*

[**no**] **ip msdp shutdown** *peer-address*

Parameters

peer-address	Specifies the IP address of the MSDP peer to shut down.

Defaults

None.

Mode

Global configuration mode.

Usage

Use the “no” form of this command to re-enable MSDP.

Examples

This example shows how to shut down MSDP peer 192.168.30.20:

```
S Chassis(su-config)->ip msdp shutdown 192.168.30.20
```

ip msdp originator-id

Use this command to allow an MSDP speaker that originates a source active (SA) message to use the IP address of its interface as the RP address in the SA message.

Syntax

ip msdp originator-id *interface-id*

[**no**] **ip msdp originator-id** *interface-id*

Parameters

interface-id	Specifies the RP address in SA messages to be the address of the originating router’s interface.

Defaults

None.

Mode

Global configuration mode.

Usage

Use the “no” form of this command to delete this function.

Examples

This example shows how to:

```
S Chassis(su-config)->ip msdp originator-id loop.0.1
```

show ip msdp sa-cache

Use this command to display recent cached source (S) and group (G) state information from MSDP peers.

Syntax

show ip msdp sa-cache

Parameters

None.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to display SA cache information from MSDP peers:

```
S Chassis(su-config)->show ip msdp sa-cache
Group Address    Source Address   RP Address       Expire     Uptime
 ------------------------------------------------------------------------------
 234.1.1.1        192.168.4.100    101.1.1.1        00:00:20   00:00:54
 234.2.2.2        192.168.4.100    101.1.1.1        00:00:20   00:00:54
```

clear ip msdp sa-cache

Use this command to clear all SA cache entries for all MSDP peers.

Syntax

clear ip msdp sa-cache

Parameters

None.

Defaults

None.

Mode

Global configuration mode.

Examples

This example shows how to clear SA cache information from MSDP peers:

```
S Chassis(su-config)->clear ip msdp sa-cache
```

ip msdp sa-filter in

Use this command to configure a filter list for incoming source active (SA) messages from a specified MSDP peer.

Syntax

ip msdp sa-filter in *peer-address* [**list** *access-list-name*]

[**no**] **ip msdp sa-filter in** *peer-address* [**list** *access-list-name*]

Parameters

peer-address	Specifies the IP address of the MSDP peer from which incoming SA messages are filtered.
access-list-name	(Optional) Specifies the name of the filter list of incoming SA messages.

Defaults

- If this command is not configured, no incoming messages are filtered; all SA messages are accepted from the peer.
- If the command is configured, but no access list is specified, all source/group pairs are filtered.

Mode

Global configuration mode.

Usage

MSDP filters allow MSDP to control how multicast sources and groups are learned and advertised.

Use the “no” form of this command to remove the filter.

Examples

This example shows how to apply an SA filter to messages from MSDP peer 192.168.30.20:

```
S Chassis(su-config)->ip msdp sa-filter in 192.168.30.20
```

ip msdp sa-filter out

Use this command to configure a filter list for outgoing source active (SA) messages sent to a specified MSDP peer.

Syntax

ip msdp sa-filter out *peer-address* [**list** *access-list-name*]

[**no**] **ip msdp sa-filter out** *peer-address*

Parameters

peer-address	Specifies the IP address of the MSDP peer from to which outgoing SA messages are filtered.
list *access-list-name*	(Optional) Specifies the name of the filter list of outgoing SA messages.

Defaults

- If this command is not configured, no outgoing messages are filtered; all SA messages received are forwarded to the peer.
- If the command is configured, but no access list is specified, all source/group pairs are filtered.

Mode

Global configuration mode.

Usage

MSDP filters allow MSDP to control how multicast sources and groups are learned and advertised.

Use the “no” form of this command to remove the filter.

Examples

This example shows how to apply an SA filter (of all source/group pairs) to messages to MSDP peer 192.168.30.20:

```
S Chassis(su-config)->ip msdp sa-filter out 192.168.30.20
```

ip msdp mesh-group

Use this command to configure a mesh group of MSDP peers.

Syntax

ip msdp mesh-group *group-name peer-address*

[**no**] **ip msdp mesh-group** *group-name peer-address*

Parameters

mesh-group *group-name*	Specifies the name of the mesh group to which you are adding (or removing) MSDP peers.
peer-address	Specifies the IP address of the MSDP peer which belongs to that mesh group.

Defaults

None.

Mode

Global configuration mode.

Usage

An MSDP mesh group consists of a group of MSDP peers which have fully meshed MSDP connectivity between each other. By default, MSDP peers do not belong to a mesh group. Execute this command once for each MSDP peer in the group.

Use the “no” form of this command to remove a peer from the group.

Examples

This example shows how to add MSDP peer 192.168.30.20 to mesh group angel:

```
S Chassis(su-config)->ip msdp mesh-group angel 192.168.30.20
```

show ip msdp summary

Use this command to display the status of all MSDP peers.

Syntax

show ip msdp summary

Parameters

None.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to display status of all MSDP peers:

```
S Chassis(su-config)->show ip msdp summary
Peer Address     Remote AS Peer State  Status   Uptime         Local Address
 ------------------------------------------------------------------------------
 103.3.3.3        100       ESTABLISHED UP       2d, 12:28:17   101.1.1.1
 192.168.30.20    300       ESTABLISHED UP       2d, 12:28:47   192.168.30.10
 192.168.50.2     200       ESTABLISHED UP       2d, 12:28:47   192.168.50.1
```

clear ip msdp peer statistics

Use this command to clear the statistics counters for one or all MSDP peers.

Syntax

clear ip msdp peer statistics [*peer address*]

Parameters

peer-address	(Optional) Specifies the IP address of the MSDP peer for which the statistics counters are to be cleared.

Defaults

If no peer is specified, the statistics counters of all MSDP peers are cleared.

Mode

Global configuration mode.

Usage

If this command is run without the peer-address parameter, the statistics counters of all MSDP peers are cleared.

Examples

This example shows how to clear the statistics of MSDP peer 192.168.30.20:

```
S Chassis(su-config)->clear ip msdp peer statistics 192.168.30.20
```

67

DVMRP Commands

This chapter describes Distance Vector Multicast Routing Protocol (DVMRP) commands and how to configure them. For information about configuring DVRMP, refer to the "Multicast Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

Note: IGMP must be enabled on all VLANs running DVMRP. To do this, use the **set igmp enable** command as described in "set igmp enable" on page 62-2. It is also recommended that IGMP querying be enabled on all VLANs running DVMRP. To do this, use the **set igmp query-enable** command as described in "set igmp query-enable" on page 62-20.

For information about...	Refer to page...
ip dvmrp	67-1
ip dvmrp metric	67-2
show ip dvmrp route	67-3
show ip dvmrp	67-4
show ip dvmrp interface	67-5
show ip dvmrp neighbor	67-5

ip dvmrp

Use this command to enable or disable DVMRP on an interface.

Syntax

```
ip dvmrp
no ip dvmrp
```

Parameters

None.

Defaults

None.

Mode

Configuration command, interface configuration.

Usage

IGMP must be enabled on all VLANs running DVMRP. To do this, use the **set igmp enable** command as described in "set igmp enable" on page 62-2. It is also recommended that IGMP querying be enabled on all VLANs running DVMRP. To do this, use the **set igmp query-enable** command as described in "set igmp query-enable" on page 62-20.

Ensure that PIM is completely disabled before enabling DVMRP.

The "no" form of this command disables DVMRP.

Example

This example shows how to enable, IGMP, IGMP querying, and DVMRP on VLAN 1:

```
S Chassis(rw)->set igmp enable 1
S Chassis(rw)->set igmp query-enable 1
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip dvmrp
```

ip dvmrp metric

Use this command to configure the metric associated with a set of destinations for DVMRP reports.

Syntax

ip dvmrp metric *metric*

no ip dvmrp metric *metric*

Parameters

metric	Specifies a metric associated with a set of destinations for DVMRP reports. Valid values are from **1** – **31**. The default value is **1**.

Defaults

None.

Mode

Configuration command, interface configuration.

Usage

Use the "no" version of this command to reset the DVMRP metric to the default value of **1**.

Example

This example shows how to set a DVMRP of 16 on VLAN 1:

```
S Chassis(rw-config-intf-vlan.0.1)->ip dvmrp metric 16
```

show ip dvmrp route

Use this command to display DVMRP routing information.

Syntax

show ip dvmrp route [**address** | **masklen**]

Parameters

address	(Optional) Display DVMRP routes sorted by IP address.
masklen	(Optional) Display DVMRP routes sorted by mask length.

Defaults

If neither parameter is specified, the output is sorted by IP address.

Mode

Configuration command, any router mode.

Example

This example shows how to display DVMRP routing table entries. In this case, the routing table has twenty-five entries. The first entry shows that the destination network **9.9.9.0/24** can be reached via next-hop router **168.3.1.1**. This route has a metric of **2**. It has been in the DVMRP routing table for **5** days, **17** hours, **20** minutes and **40** seconds and will expire in **1** minute and **21** seconds.

```
S Chassis(rw)->show ip dvmrp route

Destination        Next Hop        Interface    Metric  Expire   Uptime
-------------------------------------------------------------------------------
9.9.9.0/24         168.3.1.1       vlan.0.3100  2       00:01:21 5d, 17:20:40
21.2.2.0/24        168.3.2.210     vlan.0.3200  2       00:01:40 5d, 17:20:40
21.21.21.0/24      168.3.2.210     vlan.0.3200  2       00:01:40 5d, 17:20:40
29.2.2.0/24        168.3.2.210     vlan.0.3200  2       00:01:40 5d, 17:20:40
32.1.1.0/24        168.3.2.210     vlan.0.3200  2       00:01:40 5d, 17:20:40
32.11.11.0/24      168.3.2.210     vlan.0.3200  2       00:01:40 5d, 17:20:40
92.9.2.0/24        168.3.2.210     vlan.0.3200  2       00:01:40 5d, 17:20:40
100.3.3.0/24       Connected       vlan.0.3200  1       00:00:00 5d, 17:04:42
139.3.9.0/28       Connected       vlan.0.390   1       00:00:00 5d, 17:20:43
144.3.3.0/24       168.3.2.210     vlan.0.3200  2       00:01:39 5d, 17:20:40
160.2.2.0/24       168.3.2.210     vlan.0.3200  2       00:01:39 5d, 17:20:40
168.2.1.0/24       168.3.1.1       vlan.0.3100  2       00:01:21 5d, 17:20:40
168.3.0.0/16       Connected       vlan.0.3200  1       00:00:00 5d, 17:04:42
168.3.1.0/26       Connected       vlan.0.3100  1       00:00:00 5d, 17:20:44
168.8.1.0/24       168.3.1.1       vlan.0.3100  2       00:01:20 5d, 17:20:40
188.21.21.0/24     168.3.2.210     vlan.0.3200  2       00:01:39 5d, 17:20:40
188.23.23.0/24     168.3.2.210     vlan.0.3200  2       00:01:39 5d, 17:20:40
189.8.9.0/24       168.3.1.1       vlan.0.3100  3       00:01:20 5d, 17:20:41
```

```
191.9.1.0/24       168.3.1.1       vlan.0.3100  2       00:01:20 5d, 17:20:41
191.9.9.0/24       168.3.1.1       vlan.0.3100  2       00:01:20 5d, 17:20:41
192.9.2.0/24       168.3.2.210     vlan.0.3200  2       00:01:38 5d, 17:20:41
198.9.8.0/24       168.3.1.1       vlan.0.3100  3       00:01:20 5d, 17:20:41
198.23.23.0/24     168.3.2.210     vlan.0.3200  2       00:01:38 5d, 17:20:41
199.23.23.0/24     168.3.2.210     vlan.0.3200  2       00:01:38 5d, 17:20:41
250.9.9.0/24       168.3.2.210     vlan.0.3200  2       00:01:38 5d, 17:20:41

The number of DVMRP routes is  25
```

show ip dvmrp

Use this command to display DVMRP interface, neighbor, and route summary information.

Syntax

show ip dvmrp

Parameters

None.

Defaults

None.

Mode

Configuration command, any router mode.

Example

```
S Chassis(rw)->show ip dvmrp

[DVMRP router information]

 DVMRP prune life time is 600 seconds

[DVMRP interface information]

Interface    Interface Address   MaskLen   Status    Metric    Nbr Count
-------------------------------------------------------------------------
vlan.0.390   139.3.9.1           28        UP        1         0
vlan.0.930   ----                0         DOWN      1         0
vlan.0.3100  168.3.1.2           26        UP        1         1
vlan.0.3200  168.3.2.218         16        UP        1         1


[DVMRP neighbor information]

Neighbor Address  Interface   GenerationID   Uptime          Expire
```

```
--------------------------------------------------------------------------------
168.3.1.1         vlan.0.3100 0x128f1648     5d, 17:20:53    00:00:31
168.3.2.210       vlan.0.3200 0x128f0fe7     5d, 17:04:51    00:00:27


[DVMRP route summary information]

The number of DVMRP routes is  25
```

show ip dvmrp interface

Use this command to display DVMRP interface information.

Syntax

show ip dvmrp interface

Parameters

None.

Defaults

None.

Mode

Configuration command, any router mode.

Example

```
S Chassis(rw)->show ip dvmrp interface

Interface    Interface Address   MaskLen   Status    Metric    Nbr Count
--------------------------------------------------------------------------------
vlan.0.390   139.3.9.1           28        UP        1         0
vlan.0.930   ----                0         DOWN      1         0
vlan.0.3100  168.3.1.2           26        UP        1         1
vlan.0.3200  168.3.2.218         16        UP        1         1
```

show ip dvmrp neighbor

Use this command to display DVMRP neighbor information.

Syntax

show ip dvmrp neighbor

Parameters

None.

Defaults

None.

Mode

Configuration command, any router mode.

Example

```
S Chassis(rw)->show ip dvmrp neighbor

Neighbor Address  Interface   GenerationID   Uptime          Expire
-------------------------------------------------------------------------------
168.3.1.1         vlan.0.3100 0x128f1648     5d, 17:20:34    00:00:30
168.3.2.210       vlan.0.3200 0x128f0fe7     5d, 17:04:32    00:00:26
```

68

Network Address Translation (NAT) Commands

This chapter describes the Network Address Translation (NAT) set of commands and how to use them. For information about configuring NAT, refer to the "Network Address Translation (NAT) Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

Note: NAT is currently not supported on the S-Series S-130 module.

For information about...	Refer to page...
ip nat pool	68-2
ipv6 nat pool	68-3
ip nat inside	68-4
ipv6 nat inside	68-4
ip nat outside	68-5
ipv6 nat outside	68-6
ip nat inside source list	68-6
ipv6 nat inside source list	68-8
ip nat inside source static (NAT)	68-10
ipv6 nat inside source static (NAT)	68-11
ip nat inside source static (NAPT)	68-12
ip nat ftp-control-port	68-14
ip nat translation max-entries	68-14
ipv6 nat translation max-entries	68-15
ip nat translation (timeouts)	68-16
ipv6 nat translation (timeouts)	68-17
ip nat translation protocol	68-17
ipv6 nat translation protocol	68-18
ip nat log translations	68-19
ipv6 nat log translations	68-20
ip nat inspect dns	68-21
ipv6 nat inspect dns	68-21
show ip nat bindings	68-22

For information about...	Refer to page...
show ipv6 nat bindings	68-24
clear ip nat bindings	68-26
clear ipv6 nat bindings	68-27
show ip nat info	68-28
show ipv6 nat info	68-29
show ip nat lists	68-31
show ipv6 nat lists	68-32
show ip nat pools	68-33
show ipv6 nat pools	68-34
show ip nat statics	68-35
show ipv6 nat statics	68-36
show ip nat statistics	68-36
show ipv6 nat statistics	68-37
clear ip nat statistics	68-38
clear ipv6 nat statistics	68-39

ip nat pool

Use this command to define an IPv4 NAT address pool used by the dynamic address binding feature for NAT translation.

Syntax

ip nat pool *name start-ip-address end-ip-address* [**netmask** *netmask* | **prefix-length** *prefix-length*]

no ip nat pool *name* [*start-ip-address end-ip-address*]

Parameters

name	Specifies the name of up to 63 characters in length of this NAT pool.
start-ip-address	Specifies the start of the IP address range for members of this NAT pool.
end-ip-address	Specifies the end of the IP address range for members of this NAT pool.
netmask *netmask*	(Optional) Specifies the netmask for this NAT pool range.
prefix-length *prefix-length*	(Optional) Specifies the prefix length for this NAT pool range.

Defaults

If neither netmask or prefix-length are specified, all addresses in the range are used.

Mode

Configuration command, Global configuration.

Usage

The dynamic address binding feature draws interfaces from a specified NAT pool. A host route will be added for each IP address in the pool.

The “no” form of the command deletes the specified NAT pool.

Example

This example defines the **doc1** NAT address pool with a start address of **10.10.10.25** and end address of **10.10.10.45**

```
S Chassis(rw-config)->ip nat pool doc1 10.10.10.25 10.10.10.45
```

ipv6 nat pool

Use this command to define an IPv6 NAT address pool used by the dynamic address binding feature for NAT translation.

Syntax

ipv6 nat pool *name start-ip-address/prefix-length* **count** *count*

no ipv6 nat pool *name*

Parameters

name	Specifies the name of up to 63 characters in length of this NAT pool.
start-ip-address/ prefix-length	Specifies the start of the IP address range and prefix length for members of the IPv6 NAT pool. The prefix length must be set to **112**.
count *count*	Specifies the number of contiguous addresses of the start IP address to include in this pool after the 16-bit checksum-neutral address address portion.

Defaults

None.

Mode

Configuration command, Global configuration**.**

Usage

The dynamic address binding feature draws interfaces from a specified NAT pool. A host route will be added for each IP address in the pool.

When configuring an IPv6 NAT pool, the first 16 bits of each address are reserved for implementing the checksum-neutral calculation as defined in RFC6296. The prefix length must be set to 112.

The count value determines the size of the pool. With a count of 9, the command creates a NAT binding pool range. For example: with a start address and prefix length of 3001:1111:2222:3333::0/112, the pool range would be 3001:1111:2222:3333::1:*x* to 3001:1111:2222:3333::9:*x*, with *x* representing the reserved checksum-neutral portion of the address.

The “no” form of the command deletes the specified NAT pool.

Example

This example defines the **doc1** NAT address pool with a start address of **2001:11a1::0** and end address of **2001:11a1::9**

```
S Chassis(rw-config)->ipv6 nat pool doc1 2001:11a1::0/112 count 10
```

ip nat inside

Use this command to enable an interface for IPv4 inside NAT.

Syntax

```
ip nat inside
no ip nat inside
```

Parameters

None.

Defaults

IPv4 inside NAT is disabled on the interface.

Mode

Configuration command, Interface configuration**.**

Usage

The internal client is on the inside NAT interface. This interface must be enabled for inside NAT using this command. This interface can be a VLAN, L3 tunnel, or L2 tunnel interface.

The "no" form for this command disables IPv4 inside NAT on this interface.

Example

This example enables IPv4 inside NAT on VLAN 1:

```
S Chassis(su-config)->interface vlan 1
S Chassis(su-config-intf-vlan.0.1)->ip nat inside
S Chassis(su-config-intf-vlan.0.1)->exit
S Chassis(su-config)->
```

ipv6 nat inside

Use this command to enable an interface for IPv6 inside NAT.

Syntax

```
ipv6 nat inside
no ipv6 nat inside
```

Parameters

None.

Defaults

IPv6 inside NAT is disabled on the interface.

Mode

Configuration command, Interface configuration.

Usage

The internal client is on the inside NAT interface. This interface must be enabled for inside NAT using this command. This interface can be a VLAN, L3 tunnel, or L2 tunnel interface.

The "no" form for this command disables IPv6 inside NAT on this interface.

Example

This example enables IPv6 inside NAT on VLAN 1:

```
S Chassis(su-config)->interface vlan 1
S Chassis(su-config-intf-vlan.0.1)->ipv6 nat inside
S Chassis(su-config-intf-vlan.0.1)->exit
S Chassis(su-config)->
```

ip nat outside

Use this command to enable an interface for IPv4 outside NAT.

Syntax

ip nat outside
no ip nat outside

Parameters

None.

Defaults

IPv4 outside NAT is disabled on the interface.

Mode

Configuration command, Interface configuration.

Usage

The external server is on the outside NAT interface. This interface must be enabled for outside NAT using this command. This interface can be a VLAN, L3 tunnel, or L2 tunnel interface.

The "no" form for this command disables IPv4 outside NAT on this interface.

Example

This example enables IPv4 outside NAT on VLAN 10:

```
S Chassis(su-config)->interface vlan 10
S Chassis(su-config-intf-vlan.0.10)->ip nat outside
S Chassis(su-config-intf-vlan.0.10)->exit
```

```
S Chassis(su-config)->
```

ipv6 nat outside

Use this command to enable an interface for IPv6 outside NAT.

Syntax

ipv6 nat outside
no ipv6 nat outside

Parameters

None.

Defaults

IPv6 outside NAT is disabled on the interface.

Mode

Configuration command, Interface configuration.

Usage

The external server is on the outside NAT interface. This interface must be enabled for outside NAT using this command. This interface can be a VLAN, L3 tunnel, or L2 tunnel interface.

The "no" form for this command disables IPv6 outside NAT on this interface.

Example

This example enables IPv6 outside NAT on VLAN 10:

```
S Chassis(su-config)->interface vlan 10
S Chassis(su-config-intf-vlan.0.10)->ipv6 nat outside
S Chassis(su-config-intf-vlan.0.10)->exit
S Chassis(su-config)->
```

ip nat inside source list

Use this command to enable dynamic translation of inside (local) source IPv4 addresses based upon an ACL.

Syntax

ip nat inside source list *access-list* [**pool** *pool-name*] [**interface** *interface-name*] [**overloaded**] [**inside-vrf** *vrf-name*] [**fullcone** *acl* | **restricted-cone** *acl* | **port-restricted-cone** *acl*]

no ip nat inside source list *access-list* [**pool** *pool-name*] [**interface** *interface-name*] [**overloaded**] [**inside-vrf** *vrf-name*] [**fullcone** *acl* | **restricted-cone** *acl* | **port-restricted-cone** *acl*]

Parameters

access-list	Specifies an access-list of IPv4 IP addresses to translate for this inside source address.

pool *pool-name*	(Optional) Specifies a pool of IPv4 addresses to translate for this outside address. The name can be up to 63 characters in length.
interface *interface-name*	(Optional) Specifies the outside interface string to which a translation is applied.
overloaded	(Optional) Specifies NAPT translation.
inside-vrf *vrf-name*	(Optional) Specifies the name of the inside VRF to which the IP address(es) specified in the access-list belong.
fullcone *acl*	(Optional) Specifies an access list that identifies protocols and ports to process as fullcone NAT.
restricted-cone *acl*	(Optional) Specifies an access list that identifies protocols and ports to process as restricted cone NAT.
port-restricted-cone *acl*	(Optional) Specifies an access list that identifies protocols and ports to process as port restricted cone NAT.

Defaults

If **pool** *pool-name* is not specified, a dynamic NAT firewall list rule is configured.

If **overloaded** is not specified, NAT translation occurs.

If **interface** *interface-name* is not specified, translation is enabled on all supported interfaces.

If **inside-vrf** *vrf-name* is not specified, an inside VRF is not associated with this translation.

If an access list for **fullcone**, **restricted-cone**, or **port-restricted-cone** NAT is not specified, or the packet does not match a cone access list entry, NAT applies a basic NAT binding to the packet flow.

Mode

Configuration command, Global configuration**.**

Usage

Packets from IPv4 addresses that match those on the specified IPv4 access list are translated using global addresses allocated from the named pool. The optional **overload** key enables NAPT translation. The optional interface parameter ensures that the translation only applies to packets being transmitted out the specified interface.

If a full, restricted, or port restricted cone NAT access list is specified, and the IPv4 packet protocol and port matches an access list entry, a cone NAT binding for the cone type is applied to the packet. See the Network Address Translation (NAT) Configuration chapter of the *Extreme Networks S-Series Configuration Guide* for a detailed cone NAT feature discussion.

This command is used when configuring a dynamic NAT firewall list rule. If the **pool** option is not specified, a dynamic NAT firewall list rule is configured. See the NAT firewall discussion in the Network Address Translation (NAT) Configuration chapter of the *Extreme Networks S-Series Configuration Guide*.

The “no” form of the command disables dynamic translation of inside source addresses for the specified NAT pool.

Examples

This example enables dynamic translation of inside interfaces for packets sourced for IP addresses that match the contents of access list **1** with outside IP addresses matching the contents of pool **doc1** on outside interface VLAN **5**:

```
S Chassis(rw-config)->ip nat inside source list 1 pool doc1 interface vlan 5
```

This example enables dynamic translation, on VRF vrf2, of inside addresses that match access list 1 on inside VRF **vr1** with outside IP addresses matching pool **doc1**:

```
S Chassis(rw-vrf2-config)->ip nat inside source list 1 pool doc1 inside-vrf vr1
```

This example applies a full cone NAT binding, mapping the IPv4 source IP address and port to a global IP address and port selected from the **doc1** pool for either:

- Packets on an inside interface destined for any IPv4 address on an outside interface that match the address of an access list **acl1** entry and match the protocol and port specified in an **fc_acl1** entry
- or, any outside traffic destined to the binding's doc1 selected global IP address and port to be mapped to the original client IP address and port

```
S Chassis(rw-config)->ip nat inside source list acl1 pool doc1 fullcone fc_acl1
```

ipv6 nat inside source list

Use this command to enable dynamic translation of inside (local) source IPv6 addresses based upon an ACL.

Syntax

ipv6 nat inside source list *access-list* **pool** *pool-name* [**interface** *interface-name*] [**inside-vrf** *vrf-name*] [**fullcone** *acl* | **restricted-cone** *acl* | **port-restricted-cone** *acl*]

no ipv6 nat inside source list *access-list* **pool** *pool-name* [**interface** *interface-name*] [**inside-vrf** *vrf-name*] [**fullcone** *acl* | **restricted-cone** *acl* | **port-restricted-cone** *acl*]

Parameters

access-list	Specifies an access-list of IPv6 addresses to translate for this inside source address.
pool *pool-name*	Specifies a pool of IPv6 addresses to translate for this outside address. The name can be up to 63 characters in length.
interface *interface-name*	(Optional) Specifies the outside interface string to which a translation is applied.
inside-vrf *vrf-name*	(Optional) Specifies the name of the inside VRF to which the IP address(es) specified in the access-list belong.
fullcone *acl*	(Optional) Specifies an access list that identifies protocols and ports to process as fullcone NAT.
restricted-cone *acl*	(Optional) Specifies an access list that identifies protocols and ports to process as restricted cone NAT.
port-restricted-cone *acl*	(Optional) Specifies an access list that identifies protocols and ports to process as port restricted cone NAT.

Defaults

If **interface** *interface-name* is not specified, translation is enabled on all supported interfaces.

If **inside-vrf** *vrf-name* is not specified, an inside VRF is not associated with this translation.

If an access list for **fullcone**, **restricted-cone**, or **port-restricted-cone** NAT is not specified, or the packet does not match a cone access list entry, a cone NAT binding is not applied to the packet.

Mode

Configuration command, Global configuration**.**

Usage

Packets from addresses that match those on the specified access list are translated using global addresses allocated from the named pool. You create the pool using "ipv6 nat pool" on page 68-3.

The overload option for enabling NAPT translation is not supported for NAT IPv6.

The optional interface parameter ensures that the translation only applies to packets being transmitted out the specified interface.

If the specified access list contains IP addresses that belong to another local VRF, that VRF must be specified using the **inside-vrf** option.

If a full, restricted, or port restricted cone NAT access list is specified, and the IPv6 packet protocol and port matches an access list entry, a cone NAT binding for the cone type is applied to the packet. See the Network Address Translation (NAT) Configuration chapter of the *Extreme Networks S-Series Configuration Guide* for a detailed cone NAT feature discussion.

The "no" form of the command disables dynamic translation of inside source addresses for the specified NAT pool.

Examples

This example enables dynamic translation of inside interfaces for packets sourced for IP addresses that match the contents of access list **acl1** with outside IP addresses matching the contents of pool **doc1** on outside interface VLAN **5**:

```
S Chassis(rw-config)->ipv6 nat inside source list acl1 pool doc1 interface vlan 5
```

This example enables dynamic translation, on VRF vrf2, of inside addresses that match access list **acl**2 on inside VRF **vrf1** with outside IP addresses matching pool **doc1**:

```
S Chassis(rw-vrf2-config)->ipv6 nat inside source list acl2 pool doc1 inside-vrf
vrf1
```

This example applies a full cone NAT binding, mapping the IPv6 source IP address and port to a global IP address and port selected from the NAT **doc1** pool for either:

- Packets on an inside interface destined for any IPv6 address on an outside interface that match the address of an access list **acl1** entry and match the protocol and port specified in an **fc_acl1** entry
- or, any outside traffic destined to the binding's **doc1** selected global IP address and port to be mapped to the original client IP address and port

```
S Chassis(rw-config)->ipv6 nat inside source list acl1 pool doc1 fullcone fc_acl1
```

ip nat inside source static (NAT)

Use this command to enable static NAT translation of inside source IPv4 addresses.

Syntax

ip nat inside source static *local-ip global-ip* [**inside-vrf** *vrf-name*] [**fullcone** *acl* | **restricted-cone** *acl* | **port-restricted-cone** *acl*]

no ip nat inside source static *local-ip global-ip* [**inside-vrf** *vrf-name*] [**fullcone** *acl* | **restricted-cone** *acl* | **port-restricted-cone** *acl*]

Parameters

local-ip	Specifies the private (local) address to be associated with a public (global) address for this translation.
global-ip	Specifies the public (global) address to be associated with a private (local) address for this translation.
inside-vrf *vrf-name*	(Optional) Specifies the name of the VRF to which the local IP address belongs.
fullcone *acl*	(Optional) Specifies an access list that identifies protocols and ports to process as fullcone NAT.
restricted-cone *acl*	(Optional) Specifies an access list that identifies protocols and ports to process as restricted cone NAT.
port-restricted-cone *acl*	(Optional) Specifies an access list that identifies protocols and ports to process as port restricted cone NAT.

Defaults

If **inside-vrf** *vrf-name* is not specified, an inside VRF is not associated with this translation.

If an access list for **fullcone**, **restricted-cone**, or **port-restricted-cone** NAT is not specified, or the packet does not match a cone access list entry, a cone NAT binding is not applied to the packet.

Mode

Configuration command, Global configuration**.**

Usage

If a full, restricted, or port restricted cone NAT access list is specified, and the IPv4 packet protocol and port matches an access list entry, a cone NAT binding for the cone type is applied to the packet. See the Network Address Translation (NAT) Configuration chapter of the *Extreme Networks S-Series Configuration Guide* for a detailed cone NAT feature discussion.

The “no” form of the command deletes the specified static NAT translation.

Example

This example enables a static NAT translation of inside source addresses for private local address **10.10.10.50** destined for and transmitting from unique public address **45.20.10.5**:

```
S Chassis(rw-config)->ip nat inside source static 10.10.10.50 45.20.10.5
```

This example enables a static NAT translation, on VRF vrf2, of inside source addresses for private local address **10.10.10.50** destined for and transmitting from unique public address **45.20.10.5**, specifying that the local address belongs to VRF **vr1**:

```
S Chassis(rw-vrf2-config)->ip nat inside source static 10.10.10.50 45.20.10.5
inside-vrf vr1
```

This example applies a full cone NAT binding, mapping the IPv4 source IP address 10.10.10.50 to the global IP address 45.20.10.5 for either:

- Packets on an inside interface destined for any IPv6 address on an outside interface that match the protocol and port specified in an **fc_acl1** entry
- or, any outside traffic destined to the binding's **45.20.10.5** global IP address to be mapped to the **10.10.10.50** inside address

```
S Chassis(rw-config)->ip nat inside source static 10.10.10.50 45.20.10.5 fullcone
fc_acl1
```

ipv6 nat inside source static (NAT)

Use this command to enable static NAT translation of inside source IPv6 addresses.

Syntax

ipv6 nat inside source static *local-ipv6/prefix-length global-ipv6/prefix-length* [**inside-vrf** *vrf-name*] [**fullcone** *acl* | **restricted-cone** *acl* | **port-restricted-cone** *acl*]

no ipv6 nat inside source static *local-ipv6/prefix-length global-ipv6/prefix-length* [**inside-vrf** *vrf-name*] [**fullcone** *acl* | **restricted-cone** *acl* | **port-restricted-cone** *acl*]

Parameters

local-ip/prefix-length	Specifies the private (local) address to be associated with a public (global) address for this translation. The prefix-length can not be greater than **112**.
global-ip/prefix-length	Specifies the public (global) address to be associated with a private (local) address for this translation. The prefix-length can not be greater than **112**.
inside-vrf *vrf-name*	(Optional) Specifies the name of the VRF to which the local IP address belongs.
fullcone *acl*	(Optional) Specifies an access list that identifies protocols and ports to process as fullcone NAT.
restricted-cone *acl*	(Optional) Specifies an access list that identifies protocols and ports to process as restricted cone NAT.
port-restricted-cone *acl*	(Optional) Specifies an access list that identifies protocols and ports to process as port restricted cone NAT.

Defaults

If **inside-vrf** *vrf-name* is not specified, an inside VRF is not associated with this translation.

If an access list for **fullcone**, **restricted-cone**, or **port-restricted-cone** NAT is not specified, or the packet does not match a cone access list entry, a cone NAT binding is not applied to the packet.

Mode

Configuration command, Global configuration**.**

Usage

If a full, restricted, or port restricted cone NAT access list is specified, and the IPv6 packet protocol and port matches an access list entry, a cone NAT binding for the cone type is applied to the packet. See the Network Address Translation (NAT) Configuration chapter of the *Extreme Networks S-Series Configuration Guide* for a detailed cone NAT feature discussion.

The "no" form of the command deletes the specified static NAT translation.

Example

This example enables a static NAT translation of inside source addresses for private local addresses **2001:abcd:ef01::0/64** destined for and transmitting from unique public addresses **2001:fdea:4321::0/64**:

```
S Chassis(rw-config)->ipv6 nat inside source static 2001:abcd:ef01::0/64
2001:fdea:4321::0/64
```

This example enables a static NAT translation, on VRF vrf2, of inside source addresses for private local address **2001:abcd:ef01::0/64** destined for and transmitting from unique public addresses **2001:fdea:4321::0/64**, specifying that the local addresses belong to VRF **vrf1**:

```
S Chassis(rw-vrf2-config)->no ipv6 nat inside source static 2001:abcd:ef01::0/64
2001:fdea:4321::0/64 inside-vrf vrf1
```

This example applies a full cone NAT binding, mapping the IPv6 source IP addresses **2001:abcd:ef01::0/64** to the global IP address **2001:fdea:4321::0/64** for either:

- Packets on the inside interface destined for any IPv6 address on an outside interface that match the protocol and port specified in an **fc_acl1** entry
- or, any outside traffic destined to the binding's **2001:fdea:4321::0/64** global IP address to be mapped to the **2001:abcd:ef01::0/64** inside address

```
S Chassis(rw-config)->ipv6 nat inside source static 2001:abcd:ef01::0/64
2001:fdea:4321::0/64 fullcone fc_acl1
```

ip nat inside source static (NAPT)

Use this command to enable static NAPT translation of inside source addresses.

Syntax

ip nat inside source static {**tcp** | **udp**} *local-ip local-port global-ip global-port* [**inside-vrf** *vrf-name*] [**fullcone** *acl* | **restricted-cone** *acl* | **port-restricted-cone** *acl*]

no ip nat inside source static {**tcp** | **udp**} *local-ip local-port global-ip global-port* [**inside-vrf** *vrf-name*] [**fullcone** *acl* | **restricted-cone** *acl* | **port-restricted-cone** *acl*]

Parameters

tcp | **udp**	Specifies the protocol to be used for this static NAPT translation.
local-ip	Specifies the private IP address for this static NAPT translation.
local-port	Specifies the L4 source port associated with the private IP address for this static NAPT translation.

global-ip	Specifies the unique public IP address for this static NAPT translation.
global-port	Specifies the L4 translated source port port associated with the unique public IP address for this static NAPT translation.
inside-vrf *vrf-name*	(Optional) Specifies the name of the VRF to which the local IP address belongs.
fullcone *acl*	(Optional) Specifies an access list that identifies protocols and ports to process as fullcone NAT.
restricted-cone *acl*	(Optional) Specifies an access list that identifies protocols and ports to process as restricted cone NAT.
port-restricted-cone *acl*	(Optional) Specifies an access list that identifies protocols and ports to process as port restricted cone NAT.

Defaults

If **inside-vrf** *vrf-name* is not specified, an inside VRF is not associated with this translation.

Mode

Configuration command, Global configuration**.**

Usage

Packets for the specified protocol from addresses that match the IP address and port for this static entry are translated.

If a full, restricted, or port restricted cone NAT access list is specified, and the IPv4 packet protocol and port matches an access list entry, a cone NAT binding for the cone type is applied to the packet. See the Network Address Translation (NAT) Configuration chapter of the *Extreme Networks S-Series Configuration Guide* for a detailed cone NAT feature discussion.

The “no” form of the command deletes the specified static NAPT translation.

Example

This example enables a static NAPT translation of inside source addresses for private local address **10.10.10.51** on port **123** destined for and transmitting from unique public address **45.20.10.6** on port **121**:

```
S Chassis(rw-config)->ip nat inside source static tcp 10.10.10.51 123 45.20.10.6
121
```

This example enables a static NAPT translation of inside source addresses for private local address **10.10.10.51** on port **123** destined for and transmitting from unique public address **45.20.10.6** on port **121**, specifying that the inside address is on VRF **vr1**:

```
S Chassis(rw-config)->ip nat inside source static tcp 10.10.10.51 123 45.20.10.6
121 inside-vrf vr1
```

This example applies a full cone NAT binding, mapping the IPv4 source IP address **10.10.10.50** on port **123** to the global IP address **45.20.10.5** on port **123** for either:

- Packets on an inside interface destined for any IPv6 address on an outside interface that match the protocol and port specified in an **fc_acl1** entry
- or, any outside traffic destined to the binding’s **45.20.10.5** global IP address to be mapped to the **10.10.10.50** inside address

```
S Chassis(rw-config)->ip nat inside source static 10.10.10.50 45.20.10.5 fullcone
fc_acl1
```

ip nat ftp-control-port

Use this command to specify the IPv4 NAT FTP control port.

Syntax

ip nat ftp-control-port *port-number*

no ip nat ftp-control-port

Parameters

port-number	Specifies the FTP control port. The default value is port 21.

Defaults

The default FTP control port is 21.

Mode

Configuration command, Global configuration**.**

Usage

The “no” form of the command resets the FTP control port to the default value of port 21.

Example

This example sets the NAT FTP control port to **22**:

```
S Chassis(rw-config)->ip nat ftp-control-port 22
```

ip nat translation max-entries

Use this command to configure the IPv4 NAT maximum number of translation entries.

Syntax

ip nat translation max-entries *number*

no ip nat translation max-entries

Parameters

number	Specifies the maximum number of translation entries allowed for this router. Default value of **0** (no-limit). Valid values: **1** - **65535**.

Defaults

The maximum number of translation entries defaults to 0 (no-limit).

Mode

Configuration command, Global configuration**.**

Usage

65535 entries is currently the maximum value allowed for this command. Certain applications such as NAT, LSNAT, TWCB share the same hardware resource pool of 65535 bindings on a first

come first serve basis. Lowering this value assures resources will be available for other applications.

The “no” form of the command resets the number of maximum entries to the default value of **0** (no-limit).

Example

This example sets the maximum number of NAT translation entries to **20000**:

```
S Chassis(rw-config)->ip nat translation max-entries 20000
```

ipv6 nat translation max-entries

Use this command to configure the IPv6 NAT maximum number of translation entries.

Syntax

ipv6 nat translation max-entries *number*

no ipv6 nat translation max-entries

Parameters

number	Specifies the maximum number of translation entries allowed for this router. Default value of **0** (no-limit). Valid values: **1** - **65535**.

Defaults

The maximum number of NAT translation entries defaults to 0 (no limit).

Mode

Configuration command, Global configuration**.**

Usage

65535 entries is currently the maximum value allowed for this command. Certain applications such as NAT, LSNAT, TWCB share the same hardware resource pool of 65535 bindings on a first come first serve basis. Lowering this value assures resources will be available for other applications.

The “no” form of the command resets the number of maximum entries to the default value of **0** (no-limit).

Example

This example sets the maximum number of NAT translation entries to **20000**:

```
S Chassis(rw-config)->ipv6 nat translation max-entries 20000
```

ip nat translation (timeouts)

Use this command to configure the IPv4 NAT maximum timeout value in seconds per flow type.

Syntax

```
ip nat translation {timeout | udp-timeout | tcp-timeout | icmp-timeout |
dns-timeout | ftp-timeout | finrst-timeout} [seconds]
no ip nat translation {timeout | udp-timeout | tcp-timeout | icmp-timeout |
dns-timeout | ftp-timeout | finrst-timeout}
```

Parameters

timeout	Specifies the timeout value applied to dynamic translations. Default: **240** seconds.
udp-timeout	Specifies the timeout value applied to the UDP translations. Default: **240** seconds.
tcp-timeout	Specifies the timeout value applied to the TCP translations. Default: **240** seconds.
icmp-timeout	Specifies the timeout value applied to the ICMP translations. Default: **240** seconds.
dns-timeout	Specifies the timeout value applied to the DNS translations. Default: **240** seconds.
ftp-timeout	Specifies the timeout value applied to the FTP translations. Default: **240** seconds.
finrst-timeout	Specifies the delay applied after the TCP finish reset (FIN/RST) is observed on an IPv4 NAT binding.
seconds	(Optional) Specifies the timeout value in seconds.

Defaults

If seconds is not specified, the default value of **240** seconds is applied.

Mode

Configuration command, Global configuration**.**

Usage

The "no" form of the command resets the timeouts to the default value of **240** seconds.

Example

This example sets the NAT IPv4 timeout value applied to UDP flows to **400** seconds:

```
S Chassis(rw-config)->ip nat translation udp-timeout 400
```

ipv6 nat translation (timeouts)

Use this command to configure the IPv6 NAT maximum timeout value in seconds per flow type.

Syntax

ipv6 nat translation {**timeout** | **udp-timeout** | **tcp-timeout** | **icmp-timeout** | **dns-timeout** | **finrst-timeout**} [*seconds*]

no ipv6 nat translation {**timeout** | **udp-timeout** | **tcp-timeout** | **icmp-timeout** | **dns-timeout** | **finrst-timeout**}

Parameters

timeout	Specifies the timeout value applied to dynamic translations. Default: **240** seconds.
udp-timeout	Specifies the timeout value applied to the UDP translations. Default: **240** seconds.
tcp-timeout	Specifies the timeout value applied to the TCP translations. Default: **240** seconds.
icmp-timeout	Specifies the timeout value applied to the ICMP translations. Default: **240** seconds.
dns-timeout	Specifies the timeout value applied to the DNS translations. Default: **240** seconds.
finrst-timeout	Specifies the delay applied after the TCP finish reset (FIN/RST) is observed on an IPv6 NAT binding.
seconds	(Optional) Specifies the timeout value in seconds.

Defaults

If seconds is not specified, the default value of **240** seconds is applied.

Mode

Configuration command, Global configuration**.**

Usage

The “no” form of the command resets the timeouts to the default value of **240** seconds.

Example

This example sets the NAT IPv6 timeout value applied to UDP flows to **400** seconds:

```
S Chassis(rw-config)->ipv6 nat translation udp-timeout 400
```

ip nat translation protocol

Use this command to configure an IPv4 NAT translation protocol rule.

Syntax

ip nat translation protocol *protocol* **timeout** *seconds* [**one-shot**]

no ip nat translation protocol *protocol* **timeout** *seconds* [**one-shot**]

Parameters

protocol	Specifies the protocol the rule will be applied to. • ***** - Specifies any protocol • **1** - **255** - Specifies a protocol by its number ID • **udp** [***** | **1** - **65535**] - Specifies the UDP protocol, optionally followed by a ***** for any port or the number of a specific port • **tcp** [***** | **1** - **65535**] - Specifies the TCP protocol, optionally followed by a ***** for any port or the number of a specific port • **icmp** - Specifies the ICMP protocol
timeout *seconds*	Specifies the timeout in seconds to be associated with the specified protocol.
one-shot	(Optional) Specifies that the one-shot feature is associated with this protocol. The one-shot feature is not configurable for the TCP protocol.

Defaults

If a port is not specified for UDP or TCP, the rule applies to all ports. If one-shot is not specified, the one-shot feature is not associated with the rule. Translation timers for protocols with no rule applied default to **240** seconds.

Mode

Configuration command, Global configuration**.**

Usage

Protocol rules are used to assign an idle timeout based on IP protocol and port number for UDP, TCP, and ICMP.

The “no” form of the command deletes the rule and resets the timeout for the specified protocol to the default value of 240 seconds.

One-shot is a feature specific to bindings for protocols such as ICMP or UDP (DNS), which are generally both bi-directional and only send one packet in each direction. One-shot provides the benefit of quickly cleaning up such bindings given their temporary nature. The one-shot binding will behave as follows: when a processed packet results in a binding being created and a packet is sent on to its destination, the binding is deleted after approximately 1 second from the time the packet is sent back to the peer. One-shot behavior only applies to overloaded dynamic bindings.

Example

This example sets the timeout value applied to ICMP flows to **300** and enables the one-shot feature for the ICMP protocol:

```
S Chassis(rw-config)->ip nat translation protocol icmp timeout 300 one-shot
```

ipv6 nat translation protocol

Use this command to configure an IPv6 NAT translation protocol rule.

Syntax

ipv6 nat translation protocol *protocol* **timeout** *seconds* [**one-shot**]

no ipv6 nat translation protocol *protocol* **timeout** *seconds* [**one-shot**]

Parameters

protocol	Specifies the protocol the rule will be applied to. • ***** - Specifies any protocol • **1** - **255** - Specifies a protocol by its number ID • **udp** [***** | **1** - **65535**] - Specifies the UDP protocol, optionally followed by a ***** for any port or the number of a specific port • **tcp** [***** | **1** - **65535**] - Specifies the TCP protocol, optionally followed by a ***** for any port or the number of a specific port • **icmp** - Specifies the ICMP protocol
timeout *seconds*	Specifies the timeout in seconds to be associated with the specified protocol.
one-shot	(Optional) Specifies that the one-shot feature is associated with this protocol. The one-shot feature is not configurable for the TCP protocol.

Defaults

If a port is not specified for UDP or TCP, the rule applies to all ports. If one-shot is not specified, the one-shot feature is not associated with the rule. Translation timers for protocols with no rule applied default to **240** seconds.

Mode

Configuration command, Global configuration**.**

Usage

Protocol rules are used to assign an idle timeout based on IP protocol and port number for UDP, TCP, and ICMP.

The “no” form of the command deletes the rule and resets the timeout for the specified protocol to the default value of 240 seconds.

One-shot is a feature specific to bindings for protocols such as ICMP or UDP (DNS), which are generally both bi-directional and only send one packet in each direction. One-shot provides the benefit of quickly cleaning up such bindings given their temporary nature. The one-shot binding will behave as follows: when a processed packet results in a binding being created and a packet is sent on to its destination, the binding is deleted after approximately 1 second from the time the packet is sent back to the peer. One-shot behavior only applies to overloaded dynamic bindings.

Example

This example sets the timeout value applied to ICMP flows to **300** and enables the one-shot feature for the ICMP protocol:

```
S Chassis(rw-config)->ipv6 nat translation protocol icmp timeout 300 one-shot
```

ip nat log translations

Use this command to enable logging a message when an IPv4 binding is either created or deleted.

Syntax

ip nat log translations

no ip nat log translations

Parameters

None.

Defaults

Logging a message when a binding is either created or deleted is disabled by default.

Mode

Configuration command, Global configuration.

Usage

The generated log provides the IPv4 NAT address translation information.

The “no” form of this command disables logging a message when an IPv4 binding is either created or deleted.

Example

This example enables logging to log each occurrence of a NAT binding creation or deletion:

```
S Chassis(rw-config)->ip nat log translations
```

ipv6 nat log translations

Use this command to enable logging a message when an IPv6 binding is either created or deleted.

Syntax

ipv6 nat log translations

Parameters

None.

Defaults

Logging a message when a binding is either created or deleted is disabled by default.

Mode

Configuration command, Global configuration.

Usage

The generated log provides the IPv6 NAT address translation information.

Example

This example enables logging to log each occurrence of an IPv6 NAT binding creation or deletion:

```
S Chassis(rw-config)->ipv6 nat log translations
```

ip nat inspect dns

Use this command to enable IPv4 NAT inspection and fixup of DNS packets forwarded by the NAT process.

Syntax

```
ip nat inspect dns
no ip nat inspect dns
```

Parameters

None.

Defaults

IPv4 NAT inspection and fixup of DNS packets is disabled by default.

Mode

Configuration command, Global configuration.

Usage

When NAT inspection is enabled, NAT inspects DNS packets that are being forwarded by the NAT process. NAT DNS packet inspection and fixup consists of parsing DNS request or response packets, identifying IP addresses contained within that may need to be NATed, and fixing up the DNS packet with the appropriate NAT translations.

NAT inspection of DNS packets is disabled by default.

The "no" form for this command disables NAT inspection of DNS packets.

Example

This example enables logging to log each occurrence of an IPv4 NAT binding creation or deletion:

```
S Chassis(rw-config)->ip nat inspect dns
```

ipv6 nat inspect dns

Use this command to enable IPv6 NAT inspection and fixup of DNS packets forwarded by the NAT process.

Syntax

```
ipv6 nat inspect dns
no ipv6 nat inspect dns
```

Parameters

None.

Defaults

IPv6 NAT inspection and fixup of DNS packets is disabled by default.

Mode

Configuration command, Global configuration.

Usage

When NAT inspection is enabled, NAT inspects DNS packets that are being forwarded by the NAT process. NAT DNS packet inspection and fixup consists of parsing DNS request or response packets, identifying IP addresses contained within that may need to be NATed, and fixing up the DNS packet with the appropriate NAT translations.

NAT inspection of DNS packets is disabled by default.

The "no" form for this command disables NAT inspection of DNS packets.

Example

This example enables logging to log each occurrence of an IPv6 NAT binding creation or deletion:

```
S Chassis(rw-config)->ipv6 nat inspect dns
```

show ip nat bindings

Use this command to display IPv4 NAT bindings.

Syntax

show ip nat bindings {**pool** *pool* | **id** *id* | **summary** | **match** {*protocol* | ***** | **icmp** {*sip* | *****} {*dip* | *****} | **tcp** {*sip* | *****} {*sport* | *****} {*dip* | *****} {*dport* | *****} | **udp** {*sip* | *****} {*dip* | *****}} [**detail**]}

Parameters

pool *pool*	Displays bindings for the specified pool.
id *id*	Displays bindings for the specified NAT ID.
match	Displays bindings for the specified protocol: • *protocol* **-** Specifies an IP protocol number. Valid values **0** - **255**. • *** -** Displays NAT bindings information for all protocols. • **icmp** Displays NAT bindings information for the Internet Control Message Protocol source and destination IP addresses. • **tcp** - Displays NAT bindings information for the Transmission Control Protocol for the specified source and destination IP address and port combination. • **udp** - Displays NAT bindings information for the User Datagram Protocol source and destination IP addresses.
sip	Specifies the source IP address for display of NAT bindings.
dip	Specifies the destination IP address for the display of NAT bindings.
sport	Specifies the source port for the binding to display.
dport	Specifies the destination port for the binding to display
*	Specifies the display of bindings for all source or destination IP addresses.
summary	Displays a summary of NAT bindings information.
detail	(Optional) Specifies that a detailed level of information should display.

Defaults

None.

Mode

All command modes.

Examples

This example displays a summary of all NAT bindings for this router:

```
S Chassis(rw-config)->show ip nat bindings summary
NAT Binding Summary

Codes: T   = Type ( S-Static, D-Dynamic, R-Reserved )
                  ( F-FullCone, A-AddrRestrCone, P-PortAddrRestrCone )
       IPP = IP Protocol

              Source
Id     IPP    Destination                                    Direction T   Hw Conns
-------------------------------------------------------------------------------
131071 ANY    12.12.12.12                                     Forward   SR        0
              *.*.*.*
              *.*.*.*                                           Reverse
              13.13.13.13

Number of bindings displayed: 1
S Chassis(rw-config)->
```

This example displays NAT binding information for binding ID **131071**:

```
S Chassis(rw-config)->show ip nat bindings id 131071

Id:                131071 (ESTABLISHED)
Forward Addresses:
 Source:            12.12.12.12
 Destination:       *.*.*.*
Reverse (NAT) Addresses:
 Source:            *.*.*.*
 Destination:       13.13.13.13
Rule Type:         Static (Reserved)
Cone Type:         None
IP Protocol:       ANY
Created Date:      FRI JUL 13 13:45:07 2012
Expire Date:       Never (Idle: 24368s)
Hardware Conns:    0
S Chassis(rw-config)->
```

show ipv6 nat bindings

Use this command to display IPv6 NAT bindings.

Syntax

show ipv6 nat bindings {**pool** *pool* | **id** *id* | **summary** | **match** {*protocol* | ***** | **icmp** {*sip* | *****} {*dip* | *****} | **tcp** {*sip* | *****} {*sport* | *****} {*dip* | *****} {*dport* | *****} | **udp** {*sip* | *****} {*dip* | *****}} [**detail**]}

Parameters

pool *pool*	Displays bindings for the specified pool.
id *id*	Displays bindings for the specified NAT ID.
match	Displays bindings for the specified protocol: • *protocol* **-** Specifies an IP protocol number. Valid values **0** - **255**. • *** -** Displays NAT bindings information for all protocols. • **icmp** Displays NAT bindings information for the Internet Control Message Protocol source and destination IP addresses. • **tcp** - Displays NAT bindings information for the Transmission Control Protocol for the specified source and destination IP address and port combination. • **udp** - Displays NAT bindings information for the User Datagram Protocol source and destination IP addresses.
sip	Specifies the source IP address for display of NAT bindings.
dip	Specifies the destination IP address for the display of NAT bindings.
sport	Specifies the source port for the binding to display.
dport	Specifies the destination port for the binding to display
*****	Specifies the display of bindings for all source or destination IP addresses.
summary	Displays a summary of NAT bindings information.
detail	(Optional) Specifies that a detailed level of information should display.

Defaults

None.

Mode

All command modes**.**

Examples

This example displays a summary of all NAT bindings for this router:

```
S Chassis(rw-config)->show ipv6 nat bindings summary

NAT Binding Summary

Codes: T   = Type ( S-Static, D-Dynamic, R-Reserved )
                  ( F-FullCone, A-AddrRestrCone, P-PortAddrRestrCone )
       IPP = IP Protocol

             Source
Id     IPP   Destination                                    Direction T   Hw Conns
-------------------------------------------------------------------------------
130974 ANY   1920:10:10:10::11                             Forward   D         0
             ::*
             ::*                                             Reverse
             1234:3333:4444:2300::1:6cb4
130975 ANY   1920:10:10:10::10                             Forward   D         0
             ::*
             ::*                                             Reverse
             1234:3333:4444:2300::6cb4

Number of bindings displayed: 2
S Chassis(rw-config)->
```

This example displays NAT binding information for binding ID **131071**:

```
S Chassis(rw-config)->show ipv6 nat bindings id 130974

Id:               130974 (ESTABLISHED)
Forward Addresses:
 Source:           1920:10:10:10::11
 Destination:      ::*
Reverse (NAT) Addresses:
 Source:           ::*
 Destination:      1234:3333:4444:2300::1:6cb4
Rule Type:        Dynamic
Cone Type:        None
Pool:             ipv6-pool
IP Protocol:      ANY
Created Date:     TUE JUL 17 17:29:30 2012
Expire Date:      TUE JUL 17 17:35:50 2012  (Timeout: 240s, Expires: 230s, Idle:
10s)
Hardware Conns:   0
S Chassis(rw-config)->
```

clear ip nat bindings

Use this command to clear the specified IPv4 NAT bindings.

Syntax

```
clear ip nat bindings {all | pool pool | id id | match {protocol | * | icmp {sip | *} {dip | *} | tcp {sip | *} {sport | *} {dip | *} {dport | *} | udp {sip | *} {dip | *}}
```

Parameters

all	Clears all IPv4 NAT bindings
pool *pool*	Clears IPv4 NAT bindings for the specified pool.
id *id*	Clears IPv4 NAT bindings for the specified NAT ID.
match	Clears IPv4 NAT bindings for the specified protocol: • *protocol* **-** Specifies an IP protocol number. Valid values **0** - **255**. • *** -** Clears NAT bindings information for all Internet protocols. • **icmp** Clears NAT bindings information for the Internet Control Message Protocol source and destination IP addresses. • **tcp** - Clears NAT bindings information for the Transmission Control Protocol for the specified source and destination IP address and port combination. • **udp** - Clears NAT bindings information for the User Datagram Protocol source and destination IP addresses.
sip	Clears IPv4 NAT bindings for the specified source IP address.
dip	Clears IPv4 NAT bindings for the specified destination IP address.
sport	Clears the IPv4 binding with the specified source port. Valid values **1** - **65535.**
dport	Clears the IPv4 binding with the specified destination port. Valid values **1** - **65535.**
*	Clears NAT bindings for all source or destination IP addresses.

Defaults

None.

Mode

Configuration command, Global configuration**.**

Examples

This example clears all NAT bindings for this router:

```
S Chassis(rw-config)->clear ip nat bindings all
```

This example clears NAT UDP bindings for all source IP addresses and the 200.50.50.10 destination IP address for this router:

```
S Chassis(rw-config)->clear ip nat bindings match udp * 200.50.50.10
```

clear ipv6 nat bindings

Use this command to clear the specified IPv6 NAT bindings.

Syntax

clear ipv6 nat bindings {**all** | **pool** *pool* | **id** *id* | **match** {*protocol* | * | **icmp** {*sip* | ***} {*dip* | ***} | **tcp** {*sip* | ***} {*sport* | ***} {*dip* | ***} {*dport* | ***} | **udp** {*sip* | ***} {*dip* | ***}}

Parameters

all	Clears all IPv6 NAT bindings
pool *pool*	Clears IPv6 NAT bindings for the specified pool.
id *id*	Clears IPv6 NAT bindings for the specified NAT ID.
match	Clears IPv6 NAT bindings for the specified protocol: • *protocol* **-** Specifies an IP protocol number. Valid values **0** - **255**. • *** -** Clears NAT bindings information for all Internet protocols. • **icmp** Clears NAT bindings information for the Internet Control Message Protocol source and destination IP addresses. • **tcp** - Clears NAT bindings information for the Transmission Control Protocol for the specified source and destination IP address and port combination. • **udp** - Clears NAT bindings information for the User Datagram Protocol source and destination IP addresses.
sip	Clears IPv6 NAT bindings for the specified source IP address.
dip	Clears IPv6 NAT bindings for the specified destination IP address.
sport	Clears IPv6 NAT bindings for the specified source port. Valid values **1** - **65535.**
dport	Clears IPv6 NAT bindings for the specified destination port. Valid values **1** - **65535.**
*	Clears NAT bindings for all source or destination IP addresses.

Defaults

None.

Mode

Configuration command, Global configuration**.**

Examples

This example clears all IPv6 NAT bindings for this router:

```
S Chassis(rw-config)->clear ipv6 nat bindings all
```

This example clears IPv6 NAT UDP bindings for all source IP addresses and the 2001:1::5 destination IP address for this router:

```
S Chassis(rw-config)->clear ipv6 nat bindings match udp * 2001:1::5
```

show ip nat info

Use this command to display IPv4 NAT configuration information.

Syntax

show ip nat info

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example displays the NAT statistics for this router:

```
S Chassis(rw)->show ip nat info

Object                System Max    Avail VRF Used
-------------------------------------------------
Pools                         10        8        2
List Rules                    10        6        2
Static Rules                1000      998        1
IP Addresses                2000     1978       21
Portmaps                      20       20        0

Log Translations:        Enabled
Inspect/Fixup DNS:      Disabled
FTP Control Port:             21
Max Entries:            No Limit
timeout:                     240
udp-timeout:                 240
tcp-timeout:                 240
ftp-timeout:                 240
dns-timeout:                 240
icmp-timeout:                240
finrst-timeout:                3
TCP Half-Close uses FIN/RST Timeout:    Enabled
```

Table 68-1 provides an explanation of the command output.

Table 68-1 show ip nat info Output Display

Output...	What it displays...
Object	The NAT object to display information for. Current supported objects are pools, list rules, static rules, IP addresses, and Port maps.
System Max	Specifies the maximum number allowed on the system for this row's NAT object.
Avail	Specifies the current number of objects available on the system for this row's NAT object.
VRF	Specifies the number of virtual routers on which this row's NAT object exists. Currently only 1 router is supported.
Used	Specifies the number of this row's NAT objects actually in use.
Log Translations	Specifies whether log translations is enabled or disabled as set by "ip nat log translations" on page 68-19.
Inspect/Fixup DNS:	Specifies whether IPv4 NAT inspection and fixup of DNS packets forwarded by the NAT process is enabled or disabled as set by "ip nat inspect dns" on page 68-21.
FTP Control Port:	Specifies the FTP control port as set by "ip nat ftp-control-port" on page 68-14.
Max Entries:	Specifies the IPv4 NAT maximum number of translation entries as set by "ip nat translation max-entries" on page 68-14.
timeout:	Specifies the timeout value applied to dynamic translations as set by "ip nat translation (timeouts)" on page 68-16.
udp-timeout:	Specifies the timeout value applied to the UDP translations as set by "ip nat translation (timeouts)" on page 68-16.
tcp-timeout:	Specifies the timeout value applied to the TCP translations as set by "ip nat translation (timeouts)" on page 68-16.
ftp-timeout:	Specifies the timeout value applied to the FTP translations as set by "ip nat translation (timeouts)" on page 68-16.
dns-timeout:	Specifies the timeout value applied to the DNS translations as set by "ip nat translation (timeouts)" on page 68-16.
icmp-timeout:	Specifies the timeout value applied to the ICMP translations as set by "ip nat translation (timeouts)" on page 68-16.
finrst-timeout:	Specifies the delay applied after the TCP finish reset (FIN/RST) is observed on an IPv4 NAT binding as set by "ip nat translation (timeouts)" on page 68-16.
TCP Half-Close uses FIN/RST Timeout:	Specifies whether TCP Half-Close uses the finrst-timout value.

show ipv6 nat info

Use this command to display IPv6 NAT configuration information.

Syntax

```
show ipv6 nat info
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example displays the NAT statistics for this router:

```
S Chassis(rw)->show ipv6 nat info

Object                System Max    Avail VRF Used
-------------------------------------------------
Pools                         10        8         2
List Rules                    10        6         2
Static Rules                1000      998         1
IP Addresses                2000     1978        21
Portmaps                      20       20         0

Log Translations:        Enabled
Inspect/Fixup DNS:      Disabled
Max Entries:            No Limit
timeout:                     240
udp-timeout:                 240
tcp-timeout:                 240
dns-timeout:                 240
icmp-timeout:                240
finrst-timeout:                3
TCP Half-Close uses FIN/RST Timeout:    Enabled
```

Table 68-2 provides an explanation of the command output.

Table 68-2 show ipv6 nat info Output Display

Output...	What it displays...
Object	The NAT object to display information for. Current supported objects are pools, list rules, static rules, IP addresses, and Port maps.
System Max	Specifies the maximum number allowed on the system for this row's NAT object.
Avail	Specifies the current number of objects available on the system for this row's NAT object.
VRF	Specifies the number of virtual routers on which this row's NAT object exists. Currently only 1 router is supported.
Used	Specifies the number of this row's NAT objects actually in use.

Table 68-2 show ipv6 nat info Output Display

Output...	What it displays...
Log Translations	Specifies whether log translations is enabled or disabled as set by "ipv6 nat translation protocol" on page 68-18.
Inspect/Fixup DNS:	Specifies whether IPv4 NAT inspection and fixup of DNS packets forwarded by the NAT process is enabled or disabled as set by "ipv6 nat inspect dns" on page 68-21.
Max Entries:	Specifies the IPv4 NAT maximum number of translation entries as set by "ipv6 nat translation max-entries" on page 68-15.
timeout:	Specifies the timeout value applied to dynamic translations as set by "ipv6 nat translation (timeouts)" on page 68-17.
udp-timeout:	Specifies the timeout value applied to the UDP translations as set by "ipv6 nat translation (timeouts)" on page 68-17.
tcp-timeout:	Specifies the timeout value applied to the TCP translations as set by "ipv6 nat translation (timeouts)" on page 68-17.
dns-timeout:	Specifies the timeout value applied to the DNS translations as set by "ipv6 nat translation (timeouts)" on page 68-17.
icmp-timeout:	Specifies the timeout value applied to the ICMP translations as set by "ipv6 nat translation (timeouts)" on page 68-17.
finrst-timeout:	Specifies the delay applied after the TCP finish reset (FIN/RST) is observed on an IPv4 NAT binding as set by "ipv6 nat translation (timeouts)" on page 68-17.
TCP Half-Close uses FIN/RST Timeout:	Specifies whether TCP Half-Close uses the finrst-timout value.

show ip nat lists

Use this command to display IPv4 NAT ACL list rules information.

Syntax

show ip nat lists [*list-name*] [**detail**]

Parameters

list-name	(Optional) Displays list matching rules for the specified list.
detail	(Optional) Displays detailed lists information.

Defaults

- If an ACL rules list is not specified, all rules lists are displayed.
- If **detail** is not specified, a standard output is displayed.

Mode

All command modes.

Examples

This example displays the IPv4 NAT ACL list rules for this router:

```
S Chassis(rw-config)->show ip nat lists

List Rules
list                    |pool                    |ovld|conns|hits
------------------------------------------------------------------
acl1                    |nat-pool                |No  |0    |0
S Chassis(rw-config)->
```

This example displays a detailed level of the IPv4 NAT ACL list rules for this router:

```
S Chassis(rw-config)->show ip nat lists detail
List: acl1 (Pool: nat-pool)
   Current Conns:                    0 Hits:                          0
   Direction:                   inside Match Type:                source
   Overloaded :                     No Interface:                    Any
   Inside VRF:                  Not Set
   Cone Type:                      None
S Chassis(rw-config)->
```

show ipv6 nat lists

Use this command to display IPv6 NAT ACL list rules information.

Syntax

show ipv6 nat lists [*list-name*] [**detail**]

Parameters

list-name	(Optional) Displays list matching rules for the specified list.
detail	(Optional) Displays detailed lists information.

Defaults

- If an ACL rules list is not specified, all rules lists are displayed.
- If **detail** is not specified, a standard output is displayed.

Mode

All command modes.

Examples

This example displays the IPv6 NAT ACL list rules for this router:

```
S Chassis(rw-config)->show ipv6 nat lists
List Rules
list                    |pool                    |conns|hits
------------------------------------------------------------------
```

```
aclv6                    |ipv6-pool                |0    |2
S Chassis(rw-config)->
```

This example displays the detailed information level for IPv6 NAT ACL list rules for this router:

```
S Chassis(rw-config)->show ipv6 nat lists
List: aclv6 (Pool: ipv6-pool)
   Current Conns:                      0 Hits:                          2
   Direction:                    inside Match Type:                 source
   Interface:                       Any Inside VRF:                Not Set
   Cone Type:                 Full Cone (cone_acl)
S Chassis(rw-config)->
```

show ip nat pools

Use this command to display IPv4 NAT pool information.

Syntax

show ip nat pools [*name*] [*detail*]

Parameters

name	Displays pool information for the specified pool.
detail	Displays detailed pool information.

Defaults

If the pool name is not specified, all pools are displayed. If **detail** is not specified, a standard level of information is displayed.

Mode

All command modes.

Examples

This example displays the NAT pools for this router:

```
S Chassis(rw-config)->show ip nat pools

pool                            |conns|hits
--------------------------------------------------
acl1                            |0    |0
 First: 1.1.1.1
 Last:  1.1.1.10
S Chassis(rw-config)->
```

This example display a detailed level of information for NAT pools for this router:

```
S Chassis(rw-config)->show ip nat pools detail
Pool: acl1
   First IP Address: 1.1.1.1
   Last  IP Address: 1.1.1.10
```

```
   Next  IP Address: 1.1.1.10
   Total Addr Count:                  10 Total Addr Used:                 0
   Total Addr Allocs:                  0 Out of Addrs:                    0
   Total Port Allocs:                  0 Out of Ports:                    0
   Current Conns:                      0 Hits:                            0
   Netmask:               255.255.255.0 Prefix-Len:                      24
   List Rules:                         0
   LSNAT VServers:                     0
   TWCB Webcaches:                     0
S Chassis(rw-config)->
```

show ipv6 nat pools

Use this command to display IPv6 NAT pool information.

Syntax

show ipv6 nat pools [*name*] [*detail*]

Parameters

name	Displays pool information for the specified pool.
detail	Displays detailed pool information.

Defaults

If the pool name is not specified, all pools are displayed. If **detail** is not specified, a standard level of information is displayed.

Mode

All command modes.

Examples

This example displays the NAT pools for this router:

```
S Chassis(rw-config)->show ipv6 nat pools

pool                            |conns|hits
------------------------------------------------
ipv6-pool                       |2    |51
 First: 2300::
 Last:  2300::9:0
v6tcp_pool                      |0    |0
 First: aaaa:bbbb:aaaa:bbbb::
 Last: aaaa:bbbb:aaaa:bbbb::9:0
```

This example display a detailed level of information for NAT pools for this router:

```
S Chassis(rw-config)->show ipv6 nat pools detail
Pool: v6tcp_pool
```

```
   First IP Address: aaaa:bbbb:aaaa:bbbb::
   Last  IP Address: aaaa:bbbb:aaaa:bbbb::9:0
   Next  IP Address: aaaa:bbbb:aaaa:bbbb::9:0
   Total Addr Count:                  10 Total Addr Used:                0
   Total Addr Allocs:                  0 Out of Addrs:                   0
   Total Port Allocs:                  0 Out of Ports:                   0
   Current Conns:                      0 Hits:                           0
   Prefix-Len:                       112 List Rules:                     0
   LSNAT VServers:                     0
   TWCB Webcaches:                     0
S Chassis(rw-config)->
```

show ip nat statics

Use this command to display NAT static rules information.

Syntax

show ip nat statics [**detail**]

Parameters

detail	(Optional) Displays a detailed level of NAT statics rules information.

Defaults

If **detail** is not specified, the standard output is displayed.

Mode

All command modes.

Example

This example displays the NAT static matching rules for this router:

```
S Chassis(rw-config)->show ip nat statics detail
Static Rule:
   VRID: 0
   Local  Address: 12.12.12.12
   Global Address: 13.13.13.13
   Current Conns:                      1 Hits:                           1
   Direction:                     inside Match Type:                source
   Overloaded:                        No IP Protocol                   ANY
   Reserved Binding Id:           131071
   Inside VR:                    Not Set
   Cone Type:                       None
S Chassis(rw-config)->
```

show ipv6 nat statics

Use this command to display IPv6 NAT static rules information.

Syntax

show ipv6 nat statics [**detail**]

Parameters

detail	(Optional) Displays a detailed level of IPv6 NAT statics rules information.

Defaults

If **detail** is not specified, the standard output is displayed.

Mode

All command modes.

Example

This example displays the NAT static matching rules for this router:

```
S Chassis(rw-config)->show ipv6 nat statics detail
Static Rule:
   VRID: 0
   Local  Address: 5566:1234:3333:4321::/64
   Global Address: 1234:5678:1234:5678::/64
   Global Prefix Len                  64 Local Prefix Len                64
   Current Conns:                      0 Hits:                            0
   Direction:                     inside Match Type:                  source
   IP Protocol                       ANY Inside VR:                 Not Set
   Reserved Binding Id:                0
   Cone Type:                       None
S Chassis(rw-config)->
```

show ip nat statistics

Use this command to display NAT statistics.

Syntax

show ip nat statistics [**-interesting**] [**-all_vrfs**]

Parameters

-interesting	(Optional) Displays only counters with non-zero values.
-all_vrfs	(Optionsl) Displays statistics for all VRFs.

Defaults

If no option is specified, all statistics for the current VRF context display.

Mode

All command modes.

Usage

NAT statistics display as combined count of IPv4 and IPv6 statistics.

Example

This example displays the NAT statistics for this router:

```
S Chassis(rw)->show ip nat statistics

NOTE: This command displays statistics combined from both IPv4 and IPv6 NAT.

NAT Statistics

                Current    High       Deleted    Total
Bindings        1          21         93         94

Resources
Bindings Exhausted:       0          Max Entries Reached:      0
No Global IP Addr:        0          No Portmap Port:          0
No FTP ALG Available:     0

Counters Last Cleared: FRI JUL 13 13:45:05 2012

NAT Extended Statistics (Normalized for 5 seconds)
Bindings Per Sec:         0
```

show ipv6 nat statistics

Use this command to display NAT statistics.

Syntax

show ipv6 nat statistics [**-interesting**] [**-all_vrfs**]

Parameters

-interesting	(Optional) Displays only counters with non-zero values.
-all_vrfs	(Optionsl) Displays statistics for all VRFs.

Defaults

If no option is specified, all statistics for the current VRF context display.

Mode

All command modes.

Usage

NAT statistics display as combined count of IPv4 and IPv6 statistics.

Example

This example displays the NAT statistics for this router:

```
S Chassis(rw)->show ipv6 nat statistics

NOTE: This command displays statistics combined from both IPv4 and IPv6 NAT.

NAT Statistics

                Current    High       Deleted    Total
Bindings        1          21         93         94

Resources
Bindings Exhausted:       0          Max Entries Reached:      0
No Global IP Addr:        0          No Portmap Port:          0
No FTP ALG Available:     0

Counters Last Cleared: FRI JUL 13 13:45:05 2012

NAT Extended Statistics (Normalized for 5 seconds)

Bindings Per Sec:         0
```

clear ip nat statistics

Use this command to clear all IPv4 NAT statistics.

Syntax

clear ip nat statistics

Parameters

None.

Defaults

None.

Mode

Configuration command, Global configuration.

Example

This example clears all IPv4 NAT statistics for this router:

```
S Chassis(rw-config)->clear ip nat statistics
```

clear ipv6 nat statistics

Use this command to clear all IPv6 NAT statistics.

Syntax

clear ipv6 nat statistics

Parameters

None.

Defaults

None.

Mode

Configuration command, Global configuration.

Example

This example clears all IPv6 NAT statistics for this router:

```
S Chassis(rw-config)->clear ipv6 nat statistics
```

69

LSNAT Commands

This chapter describes the IPv4 and IPv6 Load Sharing Network Address Translation (LSNAT) set of commands and how to use them. For information about configuring LSNAT, refer to the "Load Sharing Network Address Translation (LSNAT) Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show ip slb serverfarms	69-3
show ipv6 slb serverfarms	69-3
description	69-4
inservice	69-5
this	69-6
ip slb binding finrst-timeout	69-6
ipv6 slb binding finrst-timeout	69-7
ip slb binding finrst-timeout disabled	69-8
ipv6 slb binding finrst-timeout disabled	69-8
ip slb tftpctrlport	69-9
ipv6 slb tftpctrlport	69-10
ip slb serverfarm	69-10
ipv6 slb serverfarm	69-11
real	69-11
predictor	69-12
faildetect probe	69-13
faildetect type	69-14
faildetect reset	69-15
show ip slb reals	69-16
show ipv6 slb reals	69-18
maxconns	69-21
weight	69-22
show ip slb vservers	69-23
show ipv6 slb vservers	69-24

For information about...	Refer to page...
ip slb vserver	69-26
ipv6 slb vserver	69-26
binding match source-port	69-27
serverfarm (Virtual Server)	69-28
virtual	69-29
virtual-range	69-30
udp-one-shot	69-32
vrrp vlan	69-33
client	69-34
source nat pool	69-35
idle timeout	69-36
sticky type	69-37
sticky timeout	69-38
ip slb real-server access client	69-39
ipv6 slb real-server access client	69-39
ip slb real-server access tcp-reset	69-40
ipv6 slb real-server access tcp-reset	69-41
ip slb real-server access unrestricted	69-41
ipv6 slb real-server access unrestricted	69-42
show ip slb statistics	69-42
show ipv6 slb statistics	69-43
show ip slb info	69-44
show ipv6 slb info	69-45
show ip slb sticky	69-46
show ipv6 slb sticky	69-47
show ip slb statistics-sticky	69-49
show ipv6 slb statistics-sticky	69-49
show ip slb bindings	69-50
show ipv6 slb bindings	69-51
clear ip slb	69-53
clear ipv6 slb	69-54
clear ip slb statistics	69-54
clear ipv6 slb statistics	69-55

show ip slb serverfarms

Use this command to display IPv4 Server Load Balancing (SLB) server farm information.

Syntax

show ip slb serverfarms [**detail** | *serverfarmname*]

Parameters

detail	(Optional) Displays detailed output for a specific server farm or for all configured server farms.
serverfarmname	(Optional) Specifies a server farm name of up to 63 characters in length for which to display information.

Defaults

If no parameter is specified, summary information for all configured server farms will be displayed.

Mode

All command modes.

Example

This example shows how to display a detailed level of IPv4 LSNAT server farm information:

```
S Chassis(rw)->show ip slb serverfarms
reals reals
server-farm                     status   cfg   up    conns hits
-------------------------------------------------------------------
portt                           ACTIVE   1     1     0     0
ftp-sf                          ACTIVE   1     1     0     0
v4_sf_all                       ACTIVE   1     1     0     0
v4_tftp_sf                      ACTIVE   1     1     0     0

Serverfarms in active state: 4
```

show ipv6 slb serverfarms

Use this command to display IPv6 Server Load Balancing (SLB) server farm information.

Syntax

show ipv6 slb serverfarms [**detail** | *serverfarmname*]

Parameters

detail	(Optional) Displays detailed output for a specific server farm or for all configured server farms.
serverfarmname	(Optional) Specifies a server farm name of up to 63 characters in length for which to display information.

Defaults

If no parameter is specified, summary information for all configured server farms will be displayed.

Mode

All command modes.

Example

This example shows how to display a detailed level of IPv6 LSNAT server farm information:

```
S Chassis(rw)->show ipv6 slb serverfarms detail
Server-Farm: http-farm (ACTIVE) (IPv6)
   Predictor:                ROUND-ROBIN Connections:                24037
   Reals Configured:                   5 Hits:                       24038
   Reals Up:                           5 State Changes:                  1
   VServers Configured:                1
   Last state change:   MON JUL 16 13:59:14 2012
Server-Farm: smtp-farm (ACTIVE) (IPv6)
   Predictor:                ROUND-ROBIN Connections:                 9508
   Reals Configured:                   5 Hits:                       9508
   Reals Up:                           5 State Changes:                  1
   VServers Configured:                1
   Last state change:   MON JUL 16 13:59:14 2012

Serverfarms in active state: 2
```

description

Use this command to configure a description for the IPv4 or IPv6 LSNAT server farm, real server, or virtual server.

Syntax

description *description*

no description

Parameters

description	Specifies a description of up to 63 characters in length for the server farm, real server, or virtual server. If spaces are used, the description must be enclosed in double quotes (“”).

Defaults

None.

Mode

Configuration command, SLB Server Farm Configuration mode.
Configuration command, SLB Real Server Configuration mode.
Configuration command, SLB Virtual Server Configuration mode.

Usage

The “no” form of this command deletes the description for this server farm context.

Example

This example shows how to set the description for server farm named “**myproductHTTP66**” to **“2nd floor documentation”** :

```
S Chassis(rw-config)->ipv6 slb serverfarm myproductHTTP66
S Chassis(rw-config-slb-sfarm)->description “2nd floor documentation”
```

inservice

Use this command to enable an IPv4 or IPv6 SLB real server, a virtual server, or a server farm.

Syntax

inservice

no inservice

Parameters

None.

Defaults

None.

Mode

Configuration command, SLB Server Farm Configuration mode.
Configuration command, SLB Real Server Configuration mode.
Configuration command, SLB Virtual Server Configuration mode.

Usage

The server farm, real server, and virtual server are in service by default.

The “no” form of this command disables the item being configured.

For a real server the **inservice** command starts any configured fail-detects and **no inservice** stops them.

Examples

This example shows how to enable the IPv4 real server IP 10.1.2.3 in the “myproductHTTP” server farm:

```
S Chassis(rw-config)->ip slb serverfarm myproductHTTP
S Chassis(rw-config-slb-sfarm)->real 10.1.2.3 port 80
S Chassis(rw-config-slb-real)->inservice
```

This example shows how to enable the IPv6 real server IP 2001:11ac:fd34::5 in the “myproductHTTP66” server farm:

```
S Chassis(rw-config)->ip slb serverfarm myproductHTTP66
S Chassis(rw-config-slb-sfarm)->real 2001:11ac:fd34::5 port 80
S Chassis(rw-config-slb-real)->inservice
```

this

Use the **this** command to display IPv4 or IPv6 server farm, real server or virtual server information when within the configuration command mode for the desired entity.

Syntax

this

Parameters

None.

Defaults

None.

Mode

Configuration command, Server farm configuration mode, real server configuration mode, or virtual server configuration mode.

Example

This example displays information for the serverS1 server farm:

```
S Chassis(rw)->configure
S Chassis(rw-config)->ip slb serverfarm serverS1
Created serverfarm serverS1
S Chassis(rw-config-slb-sfarm)->this
Server-Farm: serverS1 (DOWN)
   Predictor:                ROUND-ROBIN Connections:                    0
   Reals Configured:                   0 Hits:                           0
   Reals Up:                           0 State Changes:                  0
   VServers Configured:                0

Serverfarms in active state: 0

S Chassis(rw-config-slb-sfarm)->
```

ip slb binding finrst-timeout

Use this command to specify an idle time in seconds after the TCP finish reset (FIN/RST) message is observed on an IPv4 NAT binding.

Syntax

ip slb binding finrst-timeout *idle-time* [**apply-to-half-closed**]

no ip slb binding finrst-timeout

Parameters

idle-time	Specifies the number of idle time seconds after the TCP FIN/RST is observed on an IPv4 NAT binding. Valid values are from **1** - **65553** seconds. The default value is **3** seconds.
apply-to-half-closed	(Optional) Applies the FIN/RST setting to half-closed TCP connections (A TCP connection that has been terminated in one direction only). The idle timer is applied to TCP half-closed connections by default.

Defaults

The FIN/RST idle time defaults to 3 seconds and the timer is applied to TCP half-closed connections. If, when modifying the idle time, the **apply-to-half-closed** option is not specified, the timer does not apply to TCP half-closed connections.

Mode

Configuration command, Global configuration mode**.**

Usage

The "no" form of this command resets the FIN/RST idle timeout to the default value of 3 seconds, and the timer is applied to TCP half-closed connections.

Example

This example shows how to set the TCP FIN/RST idle time to 4 seconds and do not apply the idle timer setting to TCP half-closed connections:

```
S Chassis(rw-config)->ip slb binding finrst-timeout 4
```

ipv6 slb binding finrst-timeout

Use this command to specify an idle time in seconds after the TCP finish reset (FIN/RST) is observed on an IPv6 NAT binding.

Syntax

ipv6 slb binding finrst-timeout *idle-time* [**apply-to-half-closed**]

no ipv6 slb ftpctrlport

Parameters

idle-time	Specifies the number of idle time seconds after the TCP RIN/RST is observed on an IPv6 NAT binding. Valid values are from **1** - **65553** seconds. The default value is **3** seconds.
apply-to-half-closed	(Optional) Applies the FIN/RST setting to half-closed TCP connections (A TCP connection that has been terminated in one direction only). The idle timer is applied to TCP half-closed connections by default.

Defaults

The FIN/RST idle time defaults to 3 seconds, and the timer is applied to TCP half-closed connections. If the apply-to-half-closed option is not specified, the timer does not apply to TCP half-closed connections.

Mode

Configuration command, Global configuration mode.

Usage

The “no” form of this command resets the FIN/RST idle timeout to the default value of 3 seconds, and the timer is applied to TCP half-closed connections.

Example

This example shows how to set the TCP FIN/RST idle time to 4 seconds and do not apply the idle timer setting to TCP half-closed connections:

```
S Chassis(rw-config)->ipv6 slb binding finrst-timeout 4
```

ip slb binding finrst-timeout disabled

Use this command to disable the TCP FIN/RST idle timer for IPv4 connections.

Syntax

ip slb binding finrst-timeout disabled

no ip slb binding finrst-timeout

Parameters

None.

Defaults

The TCP FIN/RST idle timer is enabled by default for 3 seconds.

Mode

Configuration command, Global configuration mode.

Usage

The “no” form of this command resets the FIN/RST idle timeout to the default value of 3 seconds, and the timer is applied to TCP half-closed connections.

Example

This example shows how to disable TCP FIN/RST idle timer:

```
S Chassis(rw-config)->ip slb binding finrst-timeout disabled
```

ipv6 slb binding finrst-timeout disabled

Use this command to disable the TCP FIN/RST idle timer for IPv6 connections.

Syntax

ipv6 slb binding finrst-timeout disabled

no ipv6 slb binding finrst-timeout

Parameters

None.

Defaults

None.

Mode

Configuration command, Global configuration mode.

Usage

The “no” form of this command resets the FIN/RST idle timeout to the default value of 3 seconds, and the timer is applied to TCP half-closed connections.

Example

This example shows how to disable TCP FIN/RST idle timer for IPv6 connections:

```
S Chassis(rw-config)->ipv6 slb binding finrst-timeout disabled
```

ip slb tftpctrlport

Use this command to specify an IPv4 TFTP control port for load balancing functionality. By default, this is port 69.

Syntax

ip slb tftpctrlport *port-number*

no ip slb tftpctrlport

Parameters

port-number	Specifies an IPv4 TFTP port number.

Defaults

The TFTP control port defaults to 69.

Mode

Configuration command, Global configuration mode.

Usage

The “no” form of this command resets the TFTP control port to 69.

Example

This example shows how to specify port 70 as the IPv4 TFTP control port for server load balancing:

```
S Chassis(rw-config)->ip slb tftpctrlport 70
```

ipv6 slb tftpctrlport

Use this command to specify an IPv6 TFTP control port for load balancing functionality. By default, this is port 69.

Syntax

ipv6 slb tftpctrlport *port-number*

no ipv6 slb tftpctrlport

Parameters

port-number	Specifies an IPv6 TFTP port number.

Defaults

The TFTP control port defaults to 69.

Mode

Configuration command, Global configuration mode**.**

Usage

The “no” form of this command resets the TFTP control port to 69.

Example

This example shows how to specify port 70 as the IPv6 TFTP control port for server load balancing:

```
S Chassis(rw-config)->ipv6 slb tftpctrlport 70
```

ip slb serverfarm

Use this command to create an IPv4 LSNAT server farm and enter SLB server farm configuration mode.

Syntax

ip slb serverfarm *serverfarmname*

no ip slb serverfarm *serverfarmname*

Parameters

serverfarmname	Specifies a server farm name of up to 63 characters in length.

Defaults

None.

Mode

Configuration command, Global configuration mode.

Usage

The “no” form of this command deletes the server farm from the LSNAT configuration.

Example

This example shows how to configure a server farm named "myproductHTTP":

```
S Chassis(rw-config)->ip slb serverfarm myproductHTTP
S Chassis(rw-config-slb-sfarm)->
```

ipv6 slb serverfarm

Use this command to create an IPv6 LSNAT server farm and enter IPv6 SLB server farm configuration mode.

Syntax

ipv6 slb serverfarm *serverfarmname*

no ipv6 slb serverfarm *serverfarmname*

Parameters

serverfarmname	Specifies an IPv6 server farm name of up to 63 characters in length.

Defaults

None.

Mode

Configuration command, Global configuration mode.

Usage

The "no" form of this command deletes the server farm from the LSNAT configuration.

An IPv6 server farm must be associated with an IPv6 virtual server. See "ipv6 slb vserver" on page 69-26 for the command to enter IPv6 virtual server configuration mode.

When configuring an IPv6 server farm, the source NAT pool must also be IPv6.

Example

This example shows how to configure a server farm named "myproductHTTP66":

```
S Chassis(rw-config)->ipv6 slb serverfarm myproductHTTP66
S Chassis(rw-config-slb-sfarm)->
```

real

Use this command to add a real SLB server to an IPv4 or IPv6 server farm and to enter SLB real server configuration mode.

Syntax

real *ip-address* [**port** *number*]

no real *ip-address*

Parameters

ip-address	Specifies a server IPv4 or IPv6 address.
port *number*	(Optional) Specifies a port number for this server.

Defaults

If port is not specified, no port is associated with this real server.

Mode

Configuration command, SLB Server Farm Configuration mode.

Usage

The real server IP address type (IPv4 or IPv6), specified with this command, must agree with the IP address type for the server farm being configured.

If no port number is specified, then the real server will not cause the UDP/TCP destination port number to be NATed. Also if no port number is specified, then the real server can not use UDP or TCP fail-detection types.

Examples

This example shows how to add a real server 10.1.2.3 to the server farm named "myproductHTTP" and to configure the port number to be used for the service provided by this server:

```
S Chassis(rw-config)->ip slb serverfarm myproductHTTP
S Chassis(rw-config-slb-sfarm)->real 10.1.2.3 port 80
S Chassis(rw-config-slb-real)->
```

This example shows how to add a real server 2001:11ac:fd34::5 to the server farm named "myproductHTTP66" and to configure the port number to be used for the service provided by this server:

```
S Chassis(rw-config)->ipv6 slb serverfarm myproductHTTP66
S Chassis(rw-config-slb-sfarm)->real 2001:11ac:fd34::5 port 80
S Chassis(rw-config-slb-real)->
```

predictor

Use this command to specify which load balancing algorithm to use for selecting a real server in an IPv4 or IPv6 LSNAT server farm.

Syntax

predictor [**roundrobin** | **leastconns**]

no predictor

Parameters

roundrobin	(Optional) Specifies round robin as the selection algorithm (default).
leastconns	(Optional) Specifies least connections as the selection algorithm.

Defaults

The predictor defaults to round robin. If the load balancing algorithm is not specified, round robin will be used as the selection algorithm.

Mode

Configuration command, SLB Server Farm Configuration mode**.**

Usage

The "no" form of this command resets the selection algorithm to Round Robin.

Examples

This example shows how to specify Least Connections as the server selection algorithm for the IPv4 "myproductHTTP" server farm:

```
S Chassis(rw-config)->ip slb serverfarm myproductHTTP
S Chassis(rw-config-slb-sfarm)->predictor leastconns
```

This example shows how to specify Least Connections as the server selection algorithm for the IPv6 "myproductHTTP66" server farm:

```
S Chassis(rw-config)->ipv6 slb serverfarm myproductHTTP66
S Chassis(rw-config-slb-sfarm)->predictor leastconns
```

faildetect probe

Use this command to assign up to two probes to the IPv4 or IPv6 SLB real server faildetect configuration.

Syntax

faildetect probe {**one** | **two**} *probe-name*

no faildetect probe {**one** | **two**} *probe-name*

Parameters

one | **two**	Specifies probe label the named probe is assigned to for this real server.
probe-name	Specifies the name of the probe to be assigned to monitor this real server.

Defaults

None.

Mode

Configuration command, SLB Real Server Configuration mode**.**

Usage

The LSNAT fail detection feature supports the assigning of up to two probes per real server. A probe can be assigned to probe **one** or probe **two**. By default the probe **$slb_default** is assigned to probe **one**. If you do not wish any faildetect monitoring to occur for this real server, set the faildetect type to **none**, using "faildetect type" on page 69-14.

Use the **no faildetect probe** command to remove the specified probe for this real server context. When an administratively configured probe is removed from probe **one**, the default **$slb_default** probe is auto-configured for probe **one**.

Examples

This example shows how to create a TCP probe named **TCP-HTTP** and assign it to probe **one** of the **10.1.2.3** port **80** real server on the server farm **myproductHTTP**:

```
S Chassis(su)->configure
S Chassis(su-config)->probe TCP-HTTP tcp
S Chassis(su-config-probe)->inservice
S Chassis(su-config-probe)->exit
S Chassis(su-config)->ip slb serverfarm myproductHTTP
S Chassis(su-config-slb-sfarm)->real 10.1.2.3 port 80
S Chassis(su-config-slb-real)->faildetect probe one TCP-HTTP
S Chassis(su-config-slb-real)->inservice
```

This example shows how to create a TCP probe named **TCP-HTTP66** and assign it to probe **one** of the **2001:11ac:fd34::5** port **80** real server on the server farm **myproductHTTP66**:

```
S Chassis(su)->configure
S Chassis(su-config)->probe TCP-HTTP66 tcp
S Chassis(su-config-probe)->inservice
S Chassis(su-config-probe)->exit
S Chassis(su-config)->ipv6 slb serverfarm myproductHTTP66
S Chassis(su-config-slb-sfarm)->real 2001:11ac:fd34::5 port 80
S Chassis(su-config-slb-real)->faildetect probe one TCP-HTTP66
S Chassis(su-config-slb-real)->inservice
```

faildetect type

Use this command to set whether fail detection is active or inactive for this IPv4 or IPv6 real server configuration context.

Syntax

faildetect type {**none** | **probe**}

no faildetect type

Parameters

none	Specifies that fail detection is inactive for this real server and LSNAT sets the real server's operational state to UP, regardless of the actual operational state of the real server.
probe	Specifies that fail detection is active. Fail detection monitors the real server in accordance with its configuration. The default faildetect type is **probe**.

Defaults

None.

Mode

Configuration command, SLB Real Server Configuration mode**.**

Usage

The **faildetect type** configuration determines whether fail detection is active or inactive for this real server context.

The **no faildetect** command resets the fail detection type to the default value of **probe**.

Examples

This example shows how to set the faildetect type to **none** for real server **10.1.2.3** port **80** of the **myproductHTTP** server farm:

```
S Chassis(su-config)->ip slb serverfarm myproductHTTP
S Chassis(su-config-slb-sfarm)->real 10.1.2.3 port 80
S Chassis(su-config-slb-real)->faildetect type none
S Chassis(su-config-slb-real)->inservice
S Chassis(su-config-slb-real)->
```

This example shows how to set the faildetect type to **none** for real server **2001:11ac:fd34::5** port **80** of the **myproductHTTP66** server farm:

```
S Chassis(su-config)->ipv6 slb serverfarm myproductHTTP66
S Chassis(su-config-slb-sfarm)->real 2001:11ac:fd34::5 port 80
S Chassis(su-config-slb-real)->faildetect type none
S Chassis(su-config-slb-real)->inservice
S Chassis(su-config-slb-real)->
```

faildetect reset

Use this command to reset an IPv4 or IPv6 SLB real server faildetect configuration to its factory default settings.

Syntax

```
faildetect reset
```

Parameters

None.

Defaults

None.

Mode

Configuration command, SLB Real Server Configuration mode**.**

Usage

The **faildetect reset** command in a real server configuration context does the following:

- Sets the faildetect type to the default value of **probe**
- Sets the probe for faildetect probe **one** to **$slb_default**

- Removes any configured probe for faildetect probe **two**

Examples

This example shows how to reset all faildetect configuration to the factory default settings for the **10.1.2.3** port **80** real server on the server farm **myproductHTTP**:

```
S Chassis(su-config)->ip slb serverfarm myproductHTTP
S Chassis(su-config-slb-sfarm)->real 10.1.2.3 port 80
S Chassis(su-config-slb-real)->faildetect reset
S Chassis(su-config-slb-real)->
```

show ip slb reals

Use this command to display information about the IPv4 real servers.

Syntax

show ip slb reals [**detail** | *serverfarmname* [**detail**]]

Parameters

detail	(Optional) Displays detailed output for a specific server farm or for all configured server farms.
serverfarmname	(Optional) Specifies a server farm name for which to display real server information.

Defaults

If no parameter is specified, summary information about all configured server farms will be displayed.

Mode

All command modes**.**

Examples

This example shows how to display summary information for real servers:

```
S Chassis(rw)->show ip slb reals
                                              fail      max   curr
real                |ins|server-farm       |type |wgt|conns|conns|hits
-------------------------------------------------------------------------------
1.2.3.4:80          |DIS|snmpserver        |Probe|1  |0    |0    |0
220.20.1.1:0        |UP |snmpserver        |None |1  |0    |0    |0
220.20.1.10:80      |DIS|snmpserver        |Probe|1  |0    |0    |0

Reals in active state: 1
S Chassis(rw)->
```

Table 69-1 provides an explanation of the command output.

Table 69-1 show ip slb reals Output Display

Output...	What it displays...
real	Specifies the IP address of the real server.
ins	Specifies the service state: • **UP** – Real server is in service and available • **DN** – Real server is in service and not available • **DIS** – Real server is not in service
server-farm	Specifies the server farm this real server belongs to.
fail type	Specifies the faildetection type configured for this real server: • **None** – Faildetect is not active on this device • **Probe** – Faildetect is active on this device
wgt	Specifies the weight configured for this real server.
max conns	Specifies the maximum number of connections allowed for this real server.
curr conns	Specifies the current number of connections in use for this real server.
hits	Specifies the total number of connections used since the last time statistics were cleared.

This example shows how to display detailed information for real servers:

```
S Chassis(rw)->show ip slb reals detail
Server-Farm: snmpserver
  Real Server: 1.2.3.4:80 (DISABLED)
    Fail-Detect:                    Probe Connections:                    0
    Weight:                             1 Hits:                           0
    Max Conns:                   No Limit State Changes:                  0
    Probe One:   Not Set (default: "$slb_default")
    Probe Two:   Not Set
    Last state change:   TUE OCT 26 14:46:07 2010
Server-Farm: snmpserver
  Real Server: 220.20.1.1:0 (ACTIVE)
    Fail-Detect:                     None Connections:                    0
    Weight:                             1 Hits:                           0
    Max Conns:                   No Limit State Changes:                  1
    Probe One:   Not Set (default: "$slb_default")
    Probe Two:   Not Set
    Last state change:   TUE OCT 26 14:46:08 2010
Server-Farm: snmpserver
  Real Server: 220.20.1.10:80 (DISABLED)
    Fail-Detect:                    Probe Connections:                    0
    Weight:                             1 Hits:                           0
    Max Conns:                   No Limit State Changes:                  0
    Probe One:   Not Set (default: "$slb_default")
    Probe Two:   Not Set
```

```
    Last state change:   TUE OCT 26 14:46:07 2010

Reals in active state: 1
S Chassis(rw)->
```

Table 69-2 provides an explanation of the detailed command output.

Table 69-2 show ip slb reals detail Output Details

Output...	What it displays...
server-farm	Name of the server farm associated with this server. Assigned using the **ip slb serverfarm** command as described in "ip slb serverfarm" on page 69-10.
real-server	Address of the real server(s) assigned to this server farm. Assigned using the **real** command as described in "real" on page 69-11.
fail-detect	The fail detection type assigned using the **faildetect type** command as described in "faildetect type" on page 69-14.
connections	Specifies the current number of connections in use for this server.
weight	Specifies the weight configured for this real server using the **weight** command as described in "weight" on page 69-22.
Hits	Specifies the total number of connections used since the last time statistics were cleared.
Max Conns	Specifies the maximum number of connections allowed for this real server using the **maxconns** command as described in "maxconns" on page 69-21.
State Changes	Specifies the number of times the connection state has changed for this server.
Probe one	Specifies the probe set for probe one or "not set" if no probe is configured using the **faildetect probe** command as described in "faildetect probe" on page 69-13. If a default probe is set, **not set** displays along with the default probe in parenthesis.
Probe two	Specifies the probe set for probe two or "not set" if no probe is configured using the **faildetect probe** command as described in "faildetect probe" on page 69-13.
Last state change	Specifies the date and time of the last connection state change for this server.
Reals in active state	Specifies the number of servers in the active state for this device.

show ipv6 slb reals

Use this command to display information about the IPv6 real servers.

Syntax

show ipv6 slb reals [**detail** | *serverfarmname* [**detail**]]

Parameters

detail	(Optional) Displays detailed output for a specific server farm or for all configured server farms.

serverfarmname	(Optional) Specifies a server farm name for which to display real server information.

Defaults

If no parameter is specified, summary information about all configured server farms will be displayed.

Mode

All command modes.

Examples

This example shows how to display summary information for real servers:

```
S Chassis(rw)->show ipv6 slb reals
                                                                        fail      max   curr
real                                          |ins|server-farm       |type |wgt|conns|conns|hits
-------------------------------------------------------------------------------------------------
-----
2222::2:51                                    |UP |http-farm-ipv6    |None |1  |0    |284  |284
2222::3:51                                    |UP |http-farm-ipv6    |None |1  |0    |12335|12335
2222::4:51                                    |UP |http-farm-ipv6    |None |1  |0    |284  |284
2222::5:51                                    |UP |http-farm-ipv6    |None |1  |0    |6291 |6291
2222::6:51                                    |UP |http-farm-ipv6    |None |1  |0    |6329 |6329

Reals in active state: 5
S Chassis(rw)->
```

Table 69-1 provides an explanation of the command output.

Table 69-3 show ipv6 slb reals Output Display

Output...	What it displays...
real	Specifies the IP address of the real server.
ins	Specifies the service state: • **UP** – Real server is in service and available • **DN** – Real server is in service and not available • **DIS** – Real server is not in service
server-farm	Specifies the server farm this real server belongs to.
fail type	Specifies the faildetection type configured for this real server: • **None** – Faildetect is not active on this device • **Probe** – Faildetect is active on this device
wgt	Specifies the weight configured for this real server.
max conns	Specifies the maximum number of connections allowed for this real server.
curr conns	Specifies the current number of connections in use for this real server.
hits	Specifies the total number of connections used since the last time statistics were cleared.

This example shows how to display detailed information for real servers belonging to the **http-farm-ipv6** server farm:

```
S Chassis(rw)->show ipv6 slb reals http-farm-ipv6 detail
Server-Farm: http-farm-ipv6
  Real Server: 2222::2:51 (ACTIVE) (IPv6)
    Fail-Detect:                    None Connections:                  284
    Weight:                            1 Hits:                         284
    Max Conns:                 No Limit State Changes:                   1
    Probe One:   "icmp-probe"
    Probe Two:   "tcp-probe"
    Last state change:   MON JUL 16 15:19:55 2012
Server-Farm: http-farm-ipv6
  Real Server: 2222::3:51 (ACTIVE) (IPv6)
    Fail-Detect:                    None Connections:                13623
    Weight:                            1 Hits:                         13623
    Max Conns:                 No Limit State Changes:                   1
    Probe One:   "icmp-probe"
    Probe Two:   "tcp-probe"
    Last state change:   MON JUL 16 15:19:55 2012
Server-Farm: http-farm-ipv6
  Real Server: 2222::4:51 (ACTIVE) (IPv6)
    Fail-Detect:                    None Connections:                  284
    Weight:                            1 Hits:                         284
    Max Conns:                 No Limit State Changes:                   1
    Probe One:   "icmp-probe"
    Probe Two:   "tcp-probe"
    Last state change:   MON JUL 16 15:19:55 2012
Server-Farm: http-farm-ipv6
  Real Server: 2222::5:51 (ACTIVE) (IPv6)
    Fail-Detect:                    None Connections:                 6935
    Weight:                            1 Hits:                         6935
    Max Conns:                 No Limit State Changes:                   1
    Probe One:   "icmp-probe"
    Probe Two:   "tcp-probe"
    Last state change:   MON JUL 16 15:19:55 2012
Server-Farm: http-farm-ipv6
  Real Server: 2222::6:51 (ACTIVE) (IPv6)
    Fail-Detect:                    None Connections:                 6973
    Weight:                            1 Hits:                         6973
    Max Conns:                 No Limit State Changes:                   1
    Probe One:   "icmp-probe"
    Probe Two:   "tcp-probe"
    Last state change:   MON JUL 16 15:19:55 2012

Reals in active state: 5
```

```
S Chassis(rw)->
```

Table 69-2 provides an explanation of the detailed command output.

Table 69-4 show ipv6 slb reals detail Output Details

Output...	What it displays...
server-farm	Name of the server farm associated with this server. Assigned using the **ip slb serverfarm** command as described in "show ipv6 slb serverfarms" on page 69-3.
real-server	Address of the real server(s) assigned to this server farm. Assigned using the **real** command as described in "real" on page 69-11.
fail-detect	The fail detection type assigned using the **faildetect type** command as described in "faildetect type" on page 69-14.
connections	Specifies the current number of connections in use for this server.
weight	Specifies the weight configured for this real server using the **weight** command as described in "weight" on page 69-22.
Hits	Specifies the total number of connections used since the last time statistics were cleared.
Max Conns	Specifies the maximum number of connections allowed for this real server using the **maxconns** command as described in "maxconns" on page 69-21.
State Changes	Specifies the number of times the connection state has changed for this server.
Probe one	Specifies the probe set for probe one or "not set" if no probe is configured using the **faildetect probe** command as described in "faildetect probe" on page 69-13. If a default probe is set, **not set** displays along with the default probe in parenthesis.
Probe two	Specifies the probe set for probe two or "not set" if no probe is configured using the **faildetect probe** command as described in "faildetect probe" on page 69-13.
Last state change	Specifies the date and time of the last connection state change for this server.
Reals in active state	Specifies the number of real servers in the active state for this device.

maxconns

Use this command to limit the number of connections to an IPv4 or IPv6 real server.

Syntax

maxconns *maximum-number*

no maxconns

Parameters

maximum-number	Specifies the maximum number of connections allowed. The default condition is unlimited number of connections.

Defaults

None.

Mode

Configuration command, SLB Real Server Configuration mode.

Usage

The “no” form of this command removes the limit of connections to the server.

Examples

This example shows how to limit the number of connections to 20 on the real server at IP 10.1.2.3 in the “myproductHTTP” server farm:

```
S Chassis(rw-config)->ip slb serverfarm myproductHTTP
S Chassis(rw-config-slb-sfarm)->real 10.1.2.3 port 80
S Chassis(rw-config-slb-real)->maxconns 20
S Chassis(rw-config-slb-real)->inservice
```

This example shows how to limit the number of connections to 20 on the real server at IP 2001:11ac:fd34::5 in the “myproductHTTP66” server farm:

```
S Chassis(rw-config)->ipv6 slb serverfarm myproductHTTP66
S Chassis(rw-config-slb-sfarm)->real 2001:11ac:fd34::5 port 80
S Chassis(rw-config-slb-real)->maxconns 20
S Chassis(rw-config-slb-real)->inservice
```

weight

Use this command to specify the weight load number of an IPv4 or IPv6 real server.

Syntax

weight *weight-number*

no weight *weight-number*

Parameters

weight-number	Specifies the weight load number. Valid values are **1**-**255**. The default value is **1**.

Defaults

Weight defaults to **1**.

Mode

Configuration command, SLB Real Server Configuration mode.

Usage

Weight is a way of accounting for the resource differences between servers. If a real server has the capacity to handle twice the number of sessions as another real server, its weight ratio to the other server can be set to 2:1. The default weight for all real servers is 1. When all real servers are

configured with the default weight, each real server is treated equally. When a non-default weight is applied to any real servers in the server farm, the algorithm takes that weight into account when assigning sessions to the real servers.

The “no” form of this command resets the weight load number to the default value of 1.

Examples

This example shows how to set the weight load number to 3 on the real server at IP 10.1.2.3 in the “myproductHTTP” server farm:

```
S Chassis(rw-config)->ip slb serverfarm myproductHTTP
S Chassis(rw-config-slb-sfarm)->real 10.1.2.3 port 80
S Chassis(rw-config-slb-real)->weight 3
S Chassis(rw-config-slb-real)->inservice
```

This example shows how to set the weight load number to 3 on the real server at IP 2001:11ac:fd34::5 in the “myproductHTTP66” server farm:

```
S Chassis(rw-config)->ipv6 slb serverfarm myproductHTTP66
S Chassis(rw-config-slb-sfarm)->real 2001:11ac:fd34::5 port 80
S Chassis(rw-config-slb-real)->weight 3
S Chassis(rw-config-slb-real)->inservice
```

show ip slb vservers

Use this command to display IPv4 virtual server information.

Syntax

show ip slb vservers [**detail** | **name** *virtserver-name*]

Parameters

detail	(Optional) Displays detailed output.
name *virtserver-name*	(Optional) Specifies a virtual server name for which to display information.

Defaults

If *virtserver-name* is not entered, information about all configured virtual servers will be displayed.

If **detail** is not specified, summary information will be displayed.

Mode

All command modes.

Examples

This example shows how to display a detailed level of information about all IPv4 LSNAT virtual servers:

```
S Chassis(rw)->show ip slb vservers detail
Virtual-Server: http-lsnat44 (ACTIVE) (IPv4)
   First IP Address: 5.5.5.1
```

```
   Last  IP Address: 5.5.5.1
   Virtual IP Global to all VRFs: No
   Port:                              80 Hits:                        27548
   IP Protocol:                      TCP Current Conns:               11159
   Sticky Timeout:                  7200 Sticky Type:          SIP,DIP,DPORT
   Idle Timeout:                   65535 UDP One Shot:                    NO
   VRRP Intf:                       None VRRP Vrid:                       0
   State Changes:                      3 Match Source Port:            Exact
   Service Type:                    None Access Clients:                   0
   Server-Farm:               http-farm (IPv4)
   Source NAT Pool:             Not Set
   Client Access Acl:           Not Set

   Last state change:            MON JUL 16 15:26:02 2012
   Last state change reason:     Source NAT Pool configuration

Virtual-Server: http-lsnat46 (ACTIVE) (IPv4)
   First IP Address: 5.5.5.2
   Last  IP Address: 5.5.5.2
   Virtual IP Global to all VRFs: No
   Port:                              80 Hits:                        27547
   IP Protocol:                      TCP Current Conns:               11160
   Sticky Timeout:                  7200 Sticky Type:          SIP,DIP,DPORT
   Idle Timeout:                   65535 UDP One Shot:                    NO
   VRRP Intf:                       None VRRP Vrid:                       0
   State Changes:                      1 Match Source Port:            Exact
   Service Type:                    None Access Clients:                   0
   Server-Farm:          http-farm-ipv6 (IPv6)
   Source NAT Pool:           2333::/111
   Client Access Acl:           Not Set

   Last state change:            MON JUL 16 15:19:56 2012
   Last state change reason:     INSERVICE setting changed

Vservers in active state: 2
S Chassis(rw)->
```

show ipv6 slb vservers

Use this command to display IPv6 virtual server information.

Syntax

show ipv6 slb vservers [**detail** | **name** *virtserver-name*]

Parameters

detail	(Optional) Displays detailed output.
name *virtserver-name*	(Optional) Specifies a virtual server name for which to display information.

Defaults

If *virtserver-name* is not entered, information about all configured virtual servers will be displayed.

If **detail** is not specified, summary information will be displayed.

Mode

All command modes.

Examples

This example shows how to display a detailed level of information about all IPv6 LSNAT virtual servers:

```
S Chassis(rw)->show ipv6 slb vserver detail
Virtual-Server: http-lsnat64 (ACTIVE) (IPv6)
   First IP Address: 2555::1
   Last  IP Address: 2555::1
   Virtual IP Global to all VRFs: No
   Port:                              80 Hits:                        27895
   IP Protocol:                      TCP Current Conns:               11330
   Sticky Timeout:                  7200 Sticky Type:          SIP,DIP,DPORT
   Idle Timeout:                   65535 UDP One Shot:                    NO
   VRRP Intf:                       None VRRP Vrid:                       0
   State Changes:                      3 Match Source Port:           Exact
   Service Type:                    None
   Server-Farm:                http-farm (IPv4)
   Source NAT Pool:           4.4.0.0/15
   Client Access Acl:            Not Set
   Last state change:             MON JUL 16 15:25:15 2012
   Last state change reason:      Source NAT Pool configuration

Virtual-Server: http-lsnat66 (ACTIVE) (IPv6)
   First IP Address: 2555::2
   Last  IP Address: 2555::2
   Virtual IP Global to all VRFs: No
   Port:                              80 Hits:                        27895
   IP Protocol:                      TCP Current Conns:               11330
   Sticky Timeout:                  7200 Sticky Type:          SIP,DIP,DPORT
   Idle Timeout:                   65535 UDP One Shot:                    NO
   VRRP Intf:                       None VRRP Vrid:                       0
   State Changes:                      1 Match Source Port:           Exact
```

```
   Service Type:                    None
   Server-Farm:           http-farm-ipv6 (IPv6)
   Source NAT Pool:           2444::/111
   Client Access Acl:            Not Set
   Last state change:             MON JUL 16 15:19:56 2012
   Last state change reason:      INSERVICE setting changed

Vservers in active state: 2
S Chassis(rw)->
```

ip slb vserver

Use this command to configure an IPv4 virtual server and to enter the virtual server configuration mode.

Syntax

ip slb vserver *vserver-name*

no ip slb vserver *vserver-name*

Parameters

vserver-name	Specifies a virtual server name of up to 63 characters in length.

Defaults

None.

Mode

Configuration command, Global configuration mode.

Usage

The “no” form of this command deletes the virtual server.

Example

This example shows how to identify a virtual server named “virtual-http” and enable configuration mode for that virtual server:

```
S Chassis(rw-config)->ip slb vserver virtual-http
S Chassis(rw-config-slb-vserver)->
```

ipv6 slb vserver

Use this command to configure an IPv6 virtual server and to enter the virtual server configuration mode.

Syntax

ipv6 slb vserver *vserver-name*

no ipv6 slb vserver *vserver-name*

Parameters

vserver-name	Specifies an IPv6 virtual server name of up to 63 characters in length.

Defaults

None.

Mode

Configuration command, Global configuration mode.

Usage

The "no" form of this command deletes the virtual server.

For IPv6 LSNAT, virtual server configuration requires that a source NAT pool be defined.

Example

This example shows how to identify a virtual server named "virtual-http66" and enable configuration mode for that virtual server:

```
S Chassis(rw-config)->ipv6 slb vserver virtual-http66
S Chassis(rw-config-slb-vserver)->
```

binding match source-port

Use this command to set the source port to virtual server binding behavior for the IPv4 virtual server.

Syntax

```
binding match source-port {any | exact}
no binding match source-port
```

Parameters

any	Specifies that a single binding will match any source port the client uses destined to the same virtual server. This option is supported for IPv4 virtual servers only.
exact	Specifies that a binding should be created for each source port the client uses destined to a virtual server. The default mode is **exact**.

Defaults

The virtual server binding match source port mode defaults to **exact**.

Mode

Configuration command, SLB Virtual Server Configuration mode.

Usage

An IPv6 virtual server only supports the **exact** source port binding mode. Since this is the default binding mode, there is no reason to use this command in an IPv6 virtual server context.

When the match source-port **any** mode is set in an IPv4 virtual server context, SLB connections through the virtual server create a binding that will match any source port the client uses destined to the same virtual server VIP address and UDP/TCP port. The match source-port any mode provides a means for SLB to set up fewer bindings per client for cases where only one load balancing decision will be made for this client to virtual server for all TCP/UPD connections. Once the binding is set up, the client is bound to the initial real server for all connections to the same virtual server.

The match source-port any mode will be automatically overridden for Application Layer Gateways (ALG) FTP Control/Data, TFTP, or any virtual server using a source NAT pool.

The match source-port any mode should not be used if multiple virtual servers are configured to use real servers that have the same IP address and destination UDP/TCP port.

The "no" form of this command resets the source port to virtual server binding behavior to the default value of **exact**.

Example

This example shows how to set the binding match source port mode to any for the virtual-http virtual server:

```
S Chassis(rw-config)->ip slb vserver virtual-http
S Chassis(rw-config-slb-vserver)->binding match source-port any
```

serverfarm (Virtual Server)

Use this command to configure the server farm that the IPv4 or IPv6 virtual server will use.

Syntax

serverfarm *serverfarm-name*

no serverfarm *serverfarm-name*

Parameters

serverfarm-name	Specifies a server farm name. Must be previously configured with "ip slb serverfarm" on page 69-10 for an IPv4 server farm or "ipv6 slb serverfarm" on page 69-11 for an IPv6 server farm.

Defaults

None.

Mode

Configuration command, SLB Virtual Server Configuration mode**.**

Usage

The "no" form of this command removes the virtual server association.

The IP address type for the server farm does not have to agree with the IP address type of the virtual server. The virtual server IP address type must always agree with the client IP address type. For example, in a client IPv4 to real server IPv6 configuration, the server farm must be defined as an IPv6 server farm using "ipv6 slb serverfarm" on page 69-11 and the virtual server is configured for IPv4

Examples

This example shows how to associate the IPv4 virtual server named “virtual-http” to the “myproductHTTP” IPv4 server farm:

```
S Chassis(rw-config)->ip slb vserver virtual-http
S Chassis(rw-config-slb-vserver)->serverfarm myproductHTTP
```

This example shows how to associate the IPv4 virtual server named “virtual-http” to the “myproductHTTP46” IPv6 server farm:

```
S Chassis(rw-config)->ip slb vserver virtual-http
S Chassis(rw-config-slb-vserver)->serverfarm myproductHTTP46
```

virtual

Use this command to configure an IPv4 or IPv6 virtual server IP address and port.

Syntax

virtual *ip-address* {**tcp** | **udp**} *port* [**service** *service-name*] [**all-vrfs**]

Parameters

ip-address	Specifies an IPv4 or IPv6 IP address for the virtual server.
tcp | **udp**	Specifies TCP or UDP as the protocol used by the virtual server.
port	Specifies a TCP or UDP port number (0 through 65535) or port name to be used by this virtual server. Specifying 0 indicates all ports can be used by this virtual server. When port 0 is specified and a sticky type session persistence is applied that sticky type must be SIP. The following port name keywords may be used: **ftp** — File Transfer Protocol, port 21 (IPv4 only) **telnet** — Telnet, port 23 **www** — World Wide Web, port 80 **all** — All protocol ports
service *service-name*	(Optional) Specifies the service to be accessed through this virtual server IP address. When TCP has been specified as the protocol, service-name should be **ftp**. When UDP has been specified as the protocol, service name should be **tftp**.
all-vrfs	(Optional) Specifies that this VRF will handle SLB services for all VRFs for this router.

Defaults

- If **service** *service-name* is not specified, **ftp** is the service when TCP is the specified protocol; **tftp** is the service when UDP is the specified protocol.
- If **all-vrfs** is not specified, SLB services are only handled for this VRF router.

Mode

Configuration command, SLB Virtual Server Configuration mode**.**

Usage

The virtual server IP address type must be the same as the client IP address type.

Use this command to configure an IPv4 or IPv6 virtual IP address, IP protocol, and UDP/TCP Port. Optionally specify a service type if the configured port is not the services default.

Use the **all-vrfs** parameter to configure this VRF router to handle SLB services for all VRFs on this system.

Examples

This example shows how to set the IPv4 address and TCP port for the "virtual-http" virtual server:

```
S Chassis(rw-config)->ip slb vserver virtual-http
S Chassis(rw-config-slb-vserver)->serverfarm myproductHTTP
S Chassis(rw-config-slb-vserver)->virtual 10.1.4.5 tcp www
```

This example shows how to set the IPv6 address and UDP port for the "virtual-http66" virtual server:

```
S Chassis(rw-config)->ipv6 slb vserver virtual-http66
S Chassis(rw-config-slb-vserver)->serverfarm myproductHTTP66
S Chassis(rw-config-slb-vserver)->virtual 2001:11ac:fd34::5 udp tftp
```

This example shows how to set the IP address and TCP port for the "WWW" virtual server and for this virtual server to to handle SLB services for all VRFs on this router:

```
S Chassis(su)->router Services
S Chassis(su-Services)->configure
S Chassis(su-Services-config)->ip slb vserver WWW
S Chassis(su-Services-config-slb-vserver)->virtual 10.21.141.100 tcp www all-vrfs
```

virtual-range

Use this command to configure a range of virtual server IPv4 or IPv6 addresses.

Syntax

virtual-range *start-address end-address* {**tcp** | **udp**} *port* [**service** *service-name*] [**all-vrfs**]

Parameters

start-address *end-address*	Specifies a start and an end IP address that defines a range of virtual servers.
tcp | **udp**	Specifies TCP or UDP as the protocol used by the virtual server.

port	Specifies a TCP or UDP port number (0 through 65535) or port name to be used by this virtual server. Specifying 0 indicates all ports can be used by this virtual server, and should be used only with SIP sticky session persistence configuration. The following port name keywords may be used: **ftp** — File Transfer Protocol, port 21 (IPv4 only) **telnet** — Telnet, port 23 **www** — World Wide Web, port 80 **all** — All protocol ports
service *service-name*	(Optional) Specifies the service to be accessed through this virtual server IP address. When TCP has been specified as the protocol, service-name should be **ftp**. When UDP has been specified as the protocol, service name should be **tftp**.
all-vrfs	(Optional) Specifies that this VRF will handle SLB services for all VRFs for this router.

Defaults

- If **service** *service-name* is not specified, **ftp** is the service when TCP is the specified protocol; **tftp** is the service when UDP is the specified protocol.
- If **all-vrfs** is not specified, this VRF does not handle SLB services for other VRFs in this router.

Mode

Configuration command, SLB Virtual Server Configuration mode**.**

Usage

Use this command to configure a virtual IP address range, IP protocol, and UDP/TCP Port. Optionally specify a service type if the configured port is not the service's default.

Use the **all-vrfs** parameter to configure this VRF router to handle SLB services for all VRFs on this system.

Example

This example shows how to set the an IP address range and TCP port for the "virtual-http" virtual server:

```
S Chassis(rw-config)->ip slb vserver virtual-http
S Chassis(rw-config-slb-vserver)->serverfarm myproductHTTP
S Chassis(rw-config-slb-vserver)->virtual-range 10.1.4.5 10.1.4.10 tcp www
```

This example shows how to set the an IPv6 address range and UDP port for the "virtual-http66" virtual server and for this virtual server to handle SLB services for all VRFs on this router:

```
S Chassis(rw-config)->ipv6 slb vserver virtual-http66
S Chassis(rw-config-slb-vserver)->serverfarm myproductHTTP66
S Chassis(rw-config-slb-vserver)->virtual-range 2001:11ac:fd34::5
2001:11ac:fd34::10 udp tftp all-vrfs
```

This example shows how to set the IP address range from 10.21.141.100 through 10.21.141.105 and TCP port for the “WWW” virtual server, and for this virtual server to to handle SLB services for all VRFs on this router:

```
S Chassis(su)->router Services
S Chassis(su-Services)->configure
S Chassis(su-Services-config)->ip slb vserver WWW
S Chassis(su-Services-config-slb-vserver)->virtual 10.21.141.100 10.21.141.105
tcp www all-vrfs
```

udp-one-shot

Use this vserver configuration command to configure the IPv4 or IPv6 vserver so that UDP applications that only send a single request and reply packet exchange will not set up hardware connections.

Syntax

udp-one-shot

no udp-one-shot

Parameters

None.

Defaults

None

Mode

Configuration command, SLB Virtual Server Configuration mode**.**

Usage

Bindings created by UDP-one-shot will not result in the installation of a hardware connection. Many UDP applications send only two packets in the form of a request and a reply. With UDP-one-shot configured, a binding is created and the request packet is sent. The reception of a reply packet back causes the binding to be deleted within one second.

The “no” form of this command removes the UDP-one-shot configuration for this virtual server.

Example

This example shows how to configure a virtual server for UDP-one-shot:

```
S Chassis(rw-config)->ip slb vserver virtual-http
S Chassis(rw-config-slb-vserver)->udp-one-shot
```

vrrp vlan

Use this command to configure this IPv4 or IPv6 virtual server to participate in VRRP state changes.

Syntax

vrrp vlan *vlan vrid*

no vrrp vlan

Parameters

vlan	Specifies the VLAN on which the VRRP is configured.
vrid	Specifies the virtual router ID associated with the routing interface for this VRRP. Valid Values: **1** - **255**.

Defaults

None.

Mode

Configuration command, SLB Virtual Server Configuration mode**.**

Usage

The LSNAT VRRP feature is used to provide LSNAT redundancy in multiple chassis without connection state mirroring support. For firmware release 7.0 or greater, by default LSNAT does not participate in VRRP state changes. Virtual servers configured for VRRP, using this command, match the configured VLAN and virtual router ID with any configured VRRPs. If a matching VRRP returns a state of master then the virtual server will be allowed to come up. Any other VRRP state would prevent the virtual server from ever coming up.

The “no” form of this command clears the virtual server configuration.

Examples

This example shows how to configure this IPv4 virtual server to participate in VRRP state changes for VLAN 10 virtual router 1 :

```
S Chassis(rw-config)->ip slb vserver virtual-http
S Chassis(rw-config-slb-vserver)->serverfarm myproductHTTP
S Chassis(rw-config-slb-vserver)->virtual 10.1.4.5 tcp www
S Chassis(rw-config-slb-vserver)->vrrp vlan 10 1
```

This example shows how to configure this IPv6 virtual server to participate in VRRP state changes for VLAN 10 virtual router 1 :

```
S Chassis(rw-config)->ipv6 slb vserver virtual-http66
S Chassis(rw-config-slb-vserver)->serverfarm myproductHTTP66
S Chassis(rw-config-slb-vserver)->virtual 2001:11ac:fd34::5 udp tftp
S Chassis(rw-config-slb-vserver)->vrrp vlan 10 1
```

client

Use this command to allow a specific client to use a virtual server.

Syntax

client {*ip-address network-mask* | *ip-address/prefixlength* | *acl-list*}

no client [*ip-address network-mask*]

Parameters

ip-address network-mask	Specifies a client's IP address and network mask (IPv4 only).
ip-address/prefixlength	Specifies a client's IP address or IP address and prefix length (IPv4 only).
acl-list	A standard ACL list containing IP address permit statements (IPv4 or IPv6).

Defaults

All clients can use a virtual server.

Mode

Configuration command, SLB Virtual Server Configuration mode**.**

Usage

The *ip-address network-mask* and *ip-address/prefixlength* parameter options can only be used in an IPv4 virtual server context. An IPv4 or IPv6 standard ACL list containing permit statements for client IP addresses can be used in an IPv4 or IPv6 virtual server context.

If no client networks are specified with this command, all clients will be allowed to use a virtual server. When client networks are specified with this command, only specified clients will be allowed to use a virtual server.

The "no" form of this command removes permission for a client to use the virtual server.

Example

This example shows how to allow a client network at **100.12.22.42 255.255.255.0** to use the virtual server named **virtual-lsnat**:

```
S Chassis(rw-config)->ip slb vserver virtual-lsnat
S Chassis(rw-config-slb-vserver)->client 100.12.22.42 255.255.255.0
```

This example shows how to allow all clients specified in the **aclvs66** ACL list to use the virtual server named **virtual-lsnat66**:

```
S Chassis(rw-config)->ipv6 slb vserver virtual-lsnat66
S Chassis(rw-config-slb-vserver)->client aclvs66
```

source nat pool

Use this command to cause all connections to nat the client IP address with an address from the specified NAT source pool.

Syntax

source nat pool {*poolname* | *ip-address/prefix-len*}

no source nat pool {*poolname* | *ip-address/prefix-len*}

Parameters

poolname	Specifies a configured pool of NAT addresses to use as the source IP. (Supported for IPv4-to-IPv4 LSNAT context only).
ip-address/prefix-len	Specifies an IPv4 or IPv6 address and prefix length for the NAT source address pool. In an IPv4 context the prefix length must be 15 or less. In an IPv6 context the prefix length must be 111 or less.

Defaults

None.

Mode

Configuration command, SLB Virtual Server Configuration mode**.**

Usage

Standard LSNAT passes the client's IP address through the router unnatted. This constrains the physical location of the real server in the network. Since the client IP addresses are usually unknown, most real servers must set their default router to the LSNAT router. If the LSNAT router is not configured as the default router then the LSNAT router and real server must be located inline in the network topology. This guarantees return traffic flows through the LSNAT router.

If the client IP address is natted, the real server can be located anywhere in a network because the packets from the router to the real server will be source natted with an IP address owned by the LSNAT router itself. Client source natting is accomplished with this virtual server command that provides a NAT pool to use for source natting. The NAT pool specified is used in an overloaded fashion allowing a single address for multiple clients differentiating each using a separate port.

In an LSNAT IPv6-to-IPv6 or LSNAT IPv4-to-IPv6 virtual server context, an IPv6 source NAT pool definition is required with a prefix length of 111 or less for checksum neutral calculation of IPv6 addresses (see the LSNAT chapter in the *Extreme Networks S-Series Configuration Guide* for a detailed LSNAT combined IPv4 and IPv6 context discussion). When configuring the virtual server in an LSNAT IPv6-to-IPv4 or IPv4-to-IPv4 context, an IPv4 source NAT pool definition with an IP address and prefix length can be used. The mask or prefix length must be 15 or less. In an LSNAT IPv4-to-IPv4 context you can also specify a NAT pool.

The "no" form of this command returns to the default of no source NAT for this virtual server.

Examples

This example allows a client at **100.12.22.10 255.255.255.0** to use the virtual server named **virtual-lsnat** by assigning the client address range 100.12.22.0/15 to the virtual server NAT source pool:

```
S Chassis(rw-config)->ip slb vserver virtual-lsnat
```

```
S Chassis(rw-config-slb-vserver)->source nat pool 100.12.22.0/15
S Chassis(rw-config-slb-vserver)->client 100.12.22.10 255.255.255.0
```

This example allows a client at **2001:11ac:fd34::5** to use the virtual server named **virtual-lsnat66** by assigning the client IPv6 address range 2001:11ac:fd35::/111 to the virtual server NAT source pool:

```
S Chassis(rw-config)->ipv6 slb vserver virtual-lsnat66
S Chassis(rw-config-slb-vserver)->client 2001:11ac:fd34::5
S Chassis(rw-config-slb-vserver)->source nat pool 2001:11ac:fd35::/111
```

idle timeout

Use this command to set the number of seconds of idle time to elapse before a binding will be deleted for both an IPv4 or IPv6 virtual server configuration.

Syntax

idle timeout *timeperiod*

no idle timeout

Parameters

timeperiod	Specifies the time (in seconds) after which an idle binding connection between clients and the virtual server will be removed. Default value = 240 seconds.

Defaults

240 seconds.

Mode

Configuration command, SLB Virtual Server Configuration mode**.**

Usage

The “no” form of this command resets the timeout to the default of 240 seconds.

Examples

This example shows how to set the non-sticky session idle timeout to 360 seconds on the virtual server named “virtual-http”:

```
S Chassis(rw-config)->ip slb vserver virtual-http
S Chassis (rw-config-slb-vserver)->serverfarm myproductHTTP
S Chassis (rw-config-slb-vserver)->virtual 10.1.4.5 tcp www
S Chassis (rw-config-slb-vserver)->idle timeout 360
S Chassis (rw-config-slb-vserver)->inservice
```

This example shows how to set the non-sticky session idle timeout to 360 seconds on the virtual server named “virtual-http66”:

```
S Chassis(rw-config)->ipv6 slb vserver virtual-http66
S Chassis (rw-config-slb-vserver)->serverfarm myproductHTTP66
S Chassis (rw-config-slb-vserver)->virtual 2001:11ac:fd34::5 udp tftp
S Chassis (rw-config-slb-vserver)->idle timeout 360
```

```
S Chassis (rw-config-slb-vserver)->inservice
```

sticky type

Use this command to set the sticky type for the IPv4 or IPv6 virtual-servers.

Syntax

sticky type {**sip** | **sip dip-dport**}

no sticky type

Parameters

sip	Specifies stickiness based on the source IP address.
sip dip-dport	Specifies stickiness based on the source IP address, destination IP address, and destination port.

Defaults

None.

Mode

Configuration command, SLB Virtual Server Configuration mode**.**

Usage

A sticky entry contains a mapping of the client source IP address (and optionally, destination IP and destination UDP/TCP port number) and the selected real server. Bindings can come and go, but a sticky entry persists using a separate idle timer. When a new request is processed by a vserver, the sticky table is checked for an entry matching the vserver's sticky type. If an entry is found, then the load balancing algorithm is skipped and the request is mapped to the sticky entry's real server.

The "no" form of this command sets the binding type to non-sticky.

Example

This example shows how to apply the sticky binding type SIP to the virtual-lsnat virtual server:

```
S Chassis(rw-config)->ip slb vserver virtual-lsnat
S Chassis(rw-config-slb-vserver)->serverfarm lsnat
S Chassis(rw-config-slb-vserver)->virtual 10.1.4.5 tcp 0
S Chassis(rw-config-slb-vserver)->sticky type sip
S Chassis(rw-config-slb-vserver)->inservice
```

This example shows how to apply the sticky binding type SIP to the virtual-lsnat66 virtual server:

```
S Chassis(rw-config)->ipv6 slb vserver virtual-lsnat66
S Chassis(rw-config-slb-vserver)->serverfarm lsnat66
S Chassis(rw-config-slb-vserver)->virtual 2001:11ac:fd34::5 udp tftp
S Chassis(rw-config-slb-vserver)->sticky type sip
S Chassis(rw-config-slb-vserver)->inservice
```

sticky timeout

Use this command to set the number of seconds a sticky entry will remain idle before being deleted.

Syntax

sticky timeout *timeout*

no sticky timeout

Parameters

timeout	Specifies the number of seconds a sticky entry will remain idle before being deleted. Valid values: **41** - **65535**. Default: **7200** seconds.

Defaults

7200 seconds.

Mode

Configuration command, SLB Virtual Server Configuration mode**.**

Usage

The “no” form of this command resets the number of seconds to the default value.

An idle sticky entry is defined as a period of time when the entry has no bindings.

Examples

This example shows how to apply the sticky timeout value of 9000 seconds:

```
S Chassis(rw-config)->ip slb vserver virtual-lsnat
S Chassis(rw-config-slb-vserver)->serverfarm lsnat
S Chassis(rw-config-slb-vserver)->virtual 10.1.4.5 tcp 0
S Chassis(rw-config-slb-vserver)->sticky type sip
S Chassis(rw-config-slb-vserver)->sticky timeout 9000
S Chassis(rw-config-slb-vserver)->inservice
```

This example shows how to apply the sticky timeout value of 9000 seconds:

```
S Chassis(rw-config)->ipv6 slb vserver virtual-lsnat66
S Chassis(rw-config-slb-vserver)->serverfarm lsnat66
S Chassis(rw-config-slb-vserver)->virtual 2001:11ac:fd34::5 udp tftp0
S Chassis(rw-config-slb-vserver)->sticky type sip
S Chassis(rw-config-slb-vserver)->sticky timeout 9000
S Chassis(rw-config-slb-vserver)->inservice
```

ip slb real-server access client

Use this command to allow specified clients to access the real servers without address translation.

Syntax

ip slb real-server access client {*ip-address mask* | *ip-prefix/length* | *acl-list*}

no ip slb real-server access client {*ip-address mask* | *ip-prefix/length* | *acl-list*}

Parameters

ip-address mask	Specifies the client IP address and mask.
ip-prefix/length	Specifies the client IP prefix and length.
acl-list	Specifies the name of a standard IPv4 ACL list containing permitted client IP addresses.

Defaults

None.

Mode

Configuration command, Global configuration mode.

Usage

Specified clients can set up connections directly to the real servers' IP addresses.

The "no" form of this command removes the specified client network.

Example

This example shows how to allow all clients within the 10.24.16.0 subnet non-LSNAT access to all real servers:

```
S Chassis(rw-config)->ip slb real-server access client 10.24.16.0/24
```

ipv6 slb real-server access client

Use this command to allow clients configured in the specified ACL list to access the real servers without address translation.

Syntax

ipv6 slb real-server access client *acl-list*

no ipv6 slb real-server access client *acl-list*

Parameters

acl-list	Specifies a standard ACL list containing rules for one or more client IPv6 addresses.

Defaults

None.

Mode

Configuration command, Global configuration mode.

Usage

Clients with IPv6 addresses specified in the ACL list can set up connections directly to the real servers.

The “no” form of this command removes clients in the specified ACL from being able to access the real servers without address translation.

Example

This example shows how to allow all clients access to all real servers that are specified as permit in the **clientpermit** ACL list:

```
S Chassis(rw-config)->ipv6 slb real-server access client clientpermit
```

ip slb real-server access tcp-reset

Use this command to cause the router to return a TCP RST (reset) packet when a client tries to access an IPv4 real server directly on a TCP port used by LSNAT.

Syntax

ip slb real-server access tcp-reset

no ip slb real-server access tcp-reset

Parameters

None.

Defaults

TCP reset is disabled by default.

Mode

Configuration command, Global configuration mode.

Usage

The “no” form of this command resets the TCP reset configuration to the default value of disabled.

Example

This example shows how to enable the return of a TCP RST packet when a client tries to access an IPv4 real server directly on a TCP port used by LSNAT:

```
S Chassis(rw-config)->ip slb real-server access tcp-reset
```

ipv6 slb real-server access tcp-reset

Use this command to cause the router to return a TCP RST (reset) packet when a client tries to access an IPv6 real server directly on a TCP port used by LSNAT.

Syntax

ipv6 slb real-server access tcp-reset

no ipv6 slb real-server access tcp-reset

Parameters

None.

Defaults

TCP reset is disabled by default.

Mode

Configuration command, Global configuration mode.

Usage

The "no" form of this command resets the TCP reset configuration to the default value of disabled.

Example

This example shows how to enable the return of a TCP RST packet when a client tries to access an IPv6 real server directly on a TCP port used by LSNAT:

```
S Chassis(rw-config)->ipv6 slb real-server access tcp-reset
```

ip slb real-server access unrestricted

Use this command to allow all clients to access the IPv4 real servers directly without restriction.

Syntax

ip slb real-server access unrestricted

no ip slb real-server access unrestricted

Parameters

None.

Defaults

Real-server access is restricted by default.

Mode

Configuration command, Global configuration mode.

Usage

The "no" form of this command removes globally configured direct access for all clients.

Example

This example shows how to allow all clients to have direct access to real servers for all services :

```
S Chassis(rw-config)->ip slb real-server access unrestricted
```

ipv6 slb real-server access unrestricted

Use this command to allow all clients to access the IPv6 real servers directly without restriction.

Syntax

ipv6 slb real-server access unrestricted

no ipv6 slb real-server access unrestricted

Parameters

None

Defaults

Real-server access is restricted by default.

Mode

Configuration command, Global configuration mode.

Usage

The “no” form of this command removes globally configured direct access for all clients.

Example

This example shows how to allow all clients to have direct access to real servers for all services :

```
S Chassis(rw-config)->ipv6 slb real-server access unrestricted
```

show ip slb statistics

Use this command to display SLB statistics.

Syntax

show ip slb statistics [**-all_vrfs**] [**-interesting**]

Parameters

-all_vrfs	(Optional) Displays SLB statistics for all VRFs.
-interesting	(Optional) Displays only counters with a non-zero value.

Defaults

If no option is specified, all counters for the current VRF context are displayed.

Mode

All command modes.

Usage

This command displays statistics for both IPv4 and IPv6 as a combined value.

Example

This example shows how to display server load balancing connection statistics:

```
S Chassis(rw)->show ipv6 slb statistics
NOTE: This command displays statistics combined from both IPv4 and IPv6 LSNAT.

LSNAT Statistics
                Current    High       Deleted    Total
Bindings        38365      65536      65906      104271
Sticky Entries  16         16         0          16

Resources
Bindings Exhausted:       180        No Real Available:        0
Sticky Entries Exhausted  0          No FTP ALG Available:     0
No Portmap Port:          0
No IPv6 Portmap Port:     0

Vservers Active:          4          Vservers Active High:     4
Serverfarms Active:       2          Serverfarms Active High:  2
Reals Active:             10         Reals Active High:        10

Counters Last Cleared: MON JUL 16 15:19:28 2012

LSNAT Extended Statistics (Normalized for 5 seconds)
Bindings Per Sec:         20
S Chassis(rw)->
```

show ipv6 slb statistics

Use this command to display SLB statistics.

Syntax

show ipv6 slb statistics [**-all_vrfs**] [**-interesting**]

Parameters

-all_vrfs	(Optional) Displays SLB statistics for all VRFs.
-interesting	(Optional) Displays only counters with a non-zero value.

Defaults

If no option is specified, all counters for the current VRF context are displayed.

Mode

All command modes.

Usage

This command displays statistics for both IPv4 and IPv6 as a combined value.

Example

This example shows how to display server load balancing connection statistics:

```
S Chassis(rw)->show ip slb statistics
NOTE: This command displays statistics combined from both IPv4 and IPv6 LSNAT.

LSNAT Statistics
                Current    High       Deleted    Total
Bindings        38365      65536      65906      104271
Sticky Entries  16         16         0          16

Resources
Bindings Exhausted:       180        No Real Available:        0
Sticky Entries Exhausted  0          No FTP ALG Available:     0
No Portmap Port:          0
No IPv6 Portmap Port:     0

Vservers Active:          4          Vservers Active High:     4
Serverfarms Active:       2          Serverfarms Active High:  2
Reals Active:             10         Reals Active High:        10

Counters Last Cleared: MON JUL 16 15:19:28 2012

LSNAT Extended Statistics (Normalized for 5 seconds)
Bindings Per Sec:         20
S Chassis(rw)->
```

show ip slb info

Use this command to display global IPv4 SLB information.

Syntax

show ip slb info

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display IPv4 server load balancing information:

```
S Chassis(rw)->show ip slb info

Object               System Max    Avail VRF Used
-------------------------------------------------
Virtual-IPs                1000      996        4
Reals                       800      790       10
Sfarms                      400      398        2
Vservers                    500      496        4

FTP Control Port:    21
TFTP Control Port:   69
FIN/RST Timeout:     Disabled
Real-Server Access:  Restricted
Real-Server Access Tcp Reset: Disabled
Real-Server Access Acl: Not Set
TCP Half-Close uses FIN/RST Timeout: Disabled
S Chassis(rw)->
```

show ipv6 slb info

Use this command to display global IPv6 SLB information.

Syntax

show ipv6 slb info

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display IPv6 server load balancing information:

```
S Chassis(rw)->show ipv6 slb info
Object               System Max    Avail VRF Used
-------------------------------------------------
Virtual-IPs                1000      996        4
```

```
Reals                          800      790       10
Sfarms                         400      398        2
Vservers                       500      496        4

TFTP Control Port:   69
FIN/RST Timeout:     Disabled
Real-Server Access:  Restricted
Real-Server Access Tcp Reset: Disabled
Real-Server Access Acl: Not Set
TCP Half-Close uses FIN/RST Timeout: Disabled
S Chassis(rw)->
```

show ip slb sticky

Use this command to display IPv4 server load balancing active sticky connections.

Syntax

show ip slb sticky {**match** *sip sport dip dport* [**detail**]| **id** *id* | **summary**}

Parameters

match *sip sport dip dport*	Display sticky entries matching the specified source ip address, source IP port, destination IP address and destination port. Using the '*' character for any match field means match any for that field.
detail	(Optional) Display a detailed level of information for the **match** option.
id *id*	Displays the sticky entry information for the specified ID.
summary	Displays all sticky entries summary information.

Defaults

If **detail** is not specified for the **match** option, a standard level of information will display.

Mode

All command modes**.**

Examples

This example shows how to display all server load balancing active sticky connections.

```
S Chassis(rw)->show ip slb sticky summary

LSNAT Sticky Summary

Id     Source          Destination           Bindings   Hits
-------------------------------------------------------------------
65520  1.0.0.5         5.5.5.1:80            5229       5229
65521  1.0.0.5         5.5.5.2:80            5229       5229
65522  1.0.0.4         5.5.5.1:80            5236       5236
65523  1.0.0.4         5.5.5.2:80            5237       5237
```

```
65532  1.0.0.3         5.5.5.2:80            0          7856
65533  1.0.0.2         5.5.5.2:80            0          7857
65534  1.0.0.3         5.5.5.1:80            0          7885
65535  1.0.0.2         5.5.5.1:80            0          7885

Number of entries displayed: 8
S Chassis(rw)->
```

This example show how to display SLB active sticky connections for ID 65520:

```
S Chassis(rw)->show ip slb sticky id 65520

Id:                65520 (SIP,DIP,DPORT)
Addresses:
 Source:            1.0.0.5
 Destination:       5.5.5.1:80
Vserver:           http-lsnat44
Serverfarm:        http-farm
Real Server:       2.0.0.2:51
Hits:              5363
Created Date:      MON JUL 16 16:41:51 2012
Expire Date:       MON JUL 16 19:17:36 2012  (Timeout: 7200s)
Current Bindings:  5363
S Chassis(rw)->
```

show ipv6 slb sticky

Use this command to display IPv6 server load balancing active sticky connections.

Syntax

show ipv6 slb sticky {**match** *sip sport dip dport* [**detail**]| **id** *id* | **summary**}

Parameters

match *sip sport dip dport*	Display sticky entries matching the specified source ip address, source IP port, destination IP address and destination port. Using the '*' character for any match field means match any for that field.
detail	(Optional) Display a detailed level of information for the **match** option.
id *id*	Displays the sticky entry information for the specified ID.
summary	Displays all sticky entries summary information.

Defaults

If **detail** is not specified for the **match** option, a standard level of information will display.

Mode

All command modes.

Examples

This example shows how to display all IPv6 server load balancing active sticky connections.

```
S Chassis(rw)->show ipv6 slb sticky summary
LSNAT Sticky Summary

       Source                                              Current
Id     Destination                                         Bindings   Hits
-------------------------------------------------------------------------------
65524  2111::5
       2555::1:80                                          5392       5482
65525  2111::5
       2555::2:80                                          5392       5482
65526  2111::4
       2555::1:80                                          5392       5487
65527  2111::4
       2555::2:80                                          5392       5487
65528  2111::3
       2555::2:80                                          0          7819
65529  2111::2
       2555::2:80                                          0          7819
65530  2111::3
       2555::1:80                                          0          7837
65531  2111::2
       2555::1:80                                          0          7837

Number of entries displayed: 8
S Chassis(rw)->
```

This example show how to display IPv6 SLB active sticky connections for ID 65524:

```
S Chassis(rw)->show ipv6 slb sticky id 65524

Id:                65524 (SIP,DIP,DPORT)
Addresses:
 Source:            2111::5
 Destination:       2555::1
Vserver:           http-lsnat64
Serverfarm:        http-farm
Real Server:       2.0.0.6:51
Hits:              5519
Created Date:      MON JUL 16 16:41:47 2012
Expire Date:       MON JUL 16 19:18:34 2012  (Timeout: 7200s)
Current Bindings:  5429
S Chassis(rw)->
```

show ip slb statistics-sticky

Use this command to display IPv4 SLB sticky statistics.

Syntax

show ip slb statistics-sticky

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display all IPv4 server load balancing sticky statistics.

```
S Chassis(rw)->show ip slb statistics-sticky
LSNAT Sticky Statistics

Total Entries Created:    16
Total Bindings Stuck:     103116
Current Bindings Stuck:   39951
Active Entries:           16
Active Entries (High):    16
Entries Exhausted:        0
S Chassis(rw)->
```

show ipv6 slb statistics-sticky

Use this command to display IPv6 SLB sticky statistics.

Syntax

show ipv6 slb statistics-sticky

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display all IPv6 server load balancing sticky statistics.

```
S Chassis(rw)->show ipv6 slb statistics-sticky
LSNAT Sticky Statistics

Total Entries Created:    16
Total Bindings Stuck:     103116
Current Bindings Stuck:   39951
Active Entries:           16
Active Entries (High):    16
Entries Exhausted:        0
S Chassis(rw)->
```

show ip slb bindings

Use this command to display SLB bindings.

Syntax

show ip slb bindings {**summary** | **id** *id* | **match** {*sip* | *****} {*sport* | *****} {*dip* | *****} {*dport* | *****} [**detail**]

Parameters

summary	Displays a summary level of information for all bindings.
id *id*	Displays the specified bindings detailed information.
match *sip* | * *sport* | * *dip* | * *dport* | *	Display SLB bindings for the specified source and destination addresses and ports or all using * to match anything for the specified parameter.
detail	(Optional) Specifies that a detailed level of information should be displayed.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to display a summary of SLB bindings for this system:

```
S Chassis(rw)->show ip slb bindings summary

LSNAT Binding Summary

Id     Source                Destination           Direction Hw Conns
-------------------------------------------------------------------------
32675  134.141.94.133:1168   10.21.130.54:161      Forward          0
```

```
       172.21.1.5:161        134.141.94.133:1168   Reverse

Number of bindings displayed: 1
S Chassis(rw)->
```

This example show how to display SLB binding information for a specified ID:

```
S Chassis(rw)->show ip slb bindings id 32675

Id:                32675 (ESTABLISHED)
Sticky:            NO
Forward Addresses:
 Source:            134.141.94.133:1168
 Destination:       10.21.130.54:161
Reverse (NAT) Addresses:
 Source:            172.21.1.5:161
 Destination:       134.141.94.133:1168
Vserver:           snmp
Serverfarm:        snmpfarm
Real Server:       172.21.1.5:0
IP Protocol:       UDP
Created Date:      FRI JUN 05 09:50:39 2009
Expire Date:       FRI JUN 05 09:54:40 2009 (Timeout: 240s, Expires: 12s, Idle:
228s)
Hardware Conns:    0
```

This example show how to display SLB information matching all address and port criteria:

```
S Chassis(rw)->show ip slb bindings match * * * *

LSNAT Binding Summary

Id     Source                Destination           Direction Hw Conns
-------------------------------------------------------------------------
32673  134.141.94.133:1168   10.21.130.54:161      Forward          1
       172.21.1.5:161        134.141.94.133:1168   Reverse
32674  134.141.94.133:2359   10.21.130.54:161      Forward          2
       172.21.1.5:161        134.141.94.133:2359   Reverse

Number of bindings displayed: 2
S Chassis(rw)->
```

show ipv6 slb bindings

Use this command to display SLB bindings.

Syntax

show ipv6 slb bindings {**summary** | **id** *id* | **match** {*sip* | *****} {*sport* | *****} {*dip* | *****} {*dport* | *****} [**detail**]

Parameters

summary	Displays a summary level of information for all bindings.
id *id*	Displays the specified bindings detailed information.
match *sip* | * *sport* | * *dip* | * *dport* | *	Display SLB bindings for the specified source and destination addresses and ports or all using * to match anything for the specified parameter.
detail	(Optional) Specifies that a detailed level of information should be displayed.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to display a summary of SLB bindings for this system:

```
S Chassis(rw)->show ipv6 slb bindings summary
LSNAT Binding Summary
       Source
Id     Destination                                      Direction Hw Conns

-------------------------------------------------------------------------------
37113  2111::3:46996                                    FORWARD          1
       2555::2:80
       2222::5:51                                       REVERSE
       2444::6071:22336
37115  2111::2:46995                                    FORWARD          1
       2555::2:80
       2222::3:51                                       REVERSE
       2444::6072:22335
37117  2111::3:46994                                    FORWARD          0
       2555::1:80
       2.0.0.3:51                                       REVERSE
       4.4.160.213:22333
.
.
.
Number of bindings displayed: 1761
S Chassis(rw)->
```

This example show how to display SLB binding information for a specified ID:

```
S Chassis(rw)->show ipv6 slb bindings id 37115

Id:               37115 (ESTABLISHED)
```

```
Sticky:            YES
Forward Addresses:
 Source:            2111::2:46995
 Destination:       2555::2:80
Reverse (NAT) Addresses:
 Source:            2222::3:51
 Destination:       2444::6072:22335
Vserver:           http-lsnat66
Serverfarm:        http-farm-ipv6
Real Server:       2222::3:51
IP Protocol:       TCP
Created Date:      MON JUL 16 16:06:39 2012
Expire Date:       TUE JUL 17 10:18:49 2012  (Timeout: 65535s, Expires: 64984s,
Idle: 551s)
Hardware Conns:    0
```

clear ip slb

Use this command to clear sticky entries or to remove bindings.

Syntax

clear ip slb {**sticky** | **bindings**} {**all** | **id** *id* | **match** {*sip* | *****} {*sport* | ***} {*dip* | *****} {dport | *****}}

Parameters

sticky	Clear SLB sticky entries.
bindings	Clear SLB bindings
all	Clears all of the sticky or binding entries.
match *sip* | * *sport* | ***** *dip* | * *dport* | *****	Clears SLB bindings or sticky entries for the specified source and destination address and ports or for all (*****).
id *id*	Clears the specified item.

Defaults

None.

Mode

All command modes**.**

Examples

This example shows how to remove all sticky entries:

```
S Chassis(rw-router)->clear ip slb sticky all
```

This example shows how to remove all server load balancing bindings:

```
S Chassis(rw-router)->clear ip slb bindings all
```

clear ipv6 slb

Use this command to clear IPv6 sticky entries or to remove IPv6 bindings.

Syntax

clear ipv6 slb {**sticky** | **bindings**} {**all** | **id** *id* | **match** {*sip* | *****} {*sport* | **} {*dip* | *****} {dport | *****}}

Parameters

sticky	Clear SLB sticky entries.
bindings	Clear SLB bindings
all	Clears all of the sticky or binding entries.
match *sip* | * *sport* | * *dip* | * *dport* | *	Clears SLB bindings or sticky entries for the specified source and destination address and ports or for all (*).
id *id*	Clears the specified item.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to remove all sticky entries:

```
S Chassis(rw-router)->clear ipv6 slb sticky all
```

This example shows how to remove all server load balancing bindings:

```
S Chassis(rw-router)->clear ipv6 slb bindings all
```

clear ip slb statistics

Use this command to clear SLB counters.

Syntax

clear ip slb statistics

Parameters

None.

Defaults

None.

Mode

All configuration command modes.

Example

This example shows how to remove all server load balancing statistics:

```
S Chassis(rw-router)->clear ip slb statistics
```

clear ipv6 slb statistics

Use this command to clear IPv6 SLB counters.

Syntax

clear ipv6 slb statistics

Parameters

None.

Defaults

None.

Mode

All configuration command modes.

Example

This example shows how to remove all server load balancing statistics:

```
S Chassis(rw-router)->clear ipv6 slb statistics
```

70

Transparent Web Cache Balancing (TWCB) Commands

This chapter describes the Transparent Web Cache Balancing (TWCB) set of commands and how to use them. For information about configuring TWCB, refer to the "Transparent Web Cache Balancing (TWCB) Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
ip twcb wcserverfarm	70-2
ipv6 twcb wcserverfarm	70-3
description	70-3
predictor	70-4
cache	70-5
weight	70-6
faildetect probe	70-7
faildetect app-port	70-8
faildetect type	70-9
faildetect reset	70-10
maxconns	70-11
inservice	70-12
this	70-13
ip twcb webcache	70-14
ipv6 twcb webcache	70-14
destination ip	70-15
idle timeout	70-16
serverfarm	70-17
source nat pool	70-17
bypass-list	70-19
host redirect	70-20
ip twcb redirect out	70-21
ipv6 twcb redirect out	70-22
show ip twcb wcserverfarms	70-22

For information about...	Refer to page...
show ipv6 twcb wcserverfarms	70-23
show ip twcb webcaches	70-24
show ipv6 twcb webcaches	70-25
show ip twcb info	70-26
show ipv6 twcb info	70-26
show ip twcb caches	70-27
show ipv6 twcb caches	70-29
show ip twcb bindings	70-31
show ipv6 twcb bindings	70-32
show ip twcb statistics	70-34
show ipv6 twcb statistics	70-35
clear ip twcb	70-36
clear ipv6 twcb	70-36

ip twcb wcserverfarm

Use this command to create a web cache server farm.

Syntax

ip twcb wcserverfarm *serverfarm-name*

no ip twcb wcserverfarm *serverfarm-name*

Parameters

serverfarm-name	Specifies a server farm name of up to 63 characters in length.

Defaults

None.

Mode

Configuration command mode

Usage

Executing this command enters server farm configuration command mode for an IPv4 server farm.

Example

This example creates the IPv4 **s1Server** web cache server farm:

```
S Chassis(rw-config)->ip twcb wcserverfarm s1Server
S Chassis(rw-config-twcb-wcsfarm)->
```

ipv6 twcb wcserverfarm

Use this command to create an IPv6 web cache server farm.

Syntax

ipv6 twcb wcserverfarm *serverfarm-name*

no ipv6 twcb wcserverfarm *serverfarm-name*

Parameters

serverfarm-name	Specifies a server farm name of up to 63 characters in length.

Defaults

None.

Mode

Configuration command mode

Usage

Executing this command enters server farm configuration command mode for an IPv6 server farm.

Example

This example creates the IPv6 **s2Server** web cache server farm:

```
S Chassis(rw-config)->ipv6 twcb wcserverfarm s2Server
S Chassis(rw-config-twcb-wcsfarm)->
```

description

Use this command to configure a description for the IPv4 or IPv6 TWCB server farm, cache server, or web cache server.

Syntax

description *description*

no description

Parameters

description	Specifies a description of up to 63 characters in length for the server farm, cache server, or web cache server. If spaces are used, the description must be enclosed in double quotes (“”).

Defaults

None.

Mode

Configuration command, TWCB Server Farm Configuration mode.
Configuration command, TWCB Cache Server Configuration mode.
Configuration command, TWCB web cache Server Configuration mode.

Usage

The "no" form of this command deletes the description for this server farm context.

Examples

This example shows how to set the description for the IPv4 **s1Server** web cache server farm to **"2nd floor documentation"**:

```
S Chassis(rw-config)->ip twcb wcserverfarm s1Server
S Chassis(rw-config-twcb-wcsfarm)->description "2nd floor documentation"
```

This example shows how to set the description for the IPv6 **s2Server** web cache server farm to **"2nd floor documentation"**:

```
S Chassis(rw-config)->ipv6 twcb wcserverfarm s2Server
S Chassis(rw-config-twcb-wcsfarm)->description "2nd floor documentation"
```

predictor

Use this command to set the IPv4 or IPv6 cache server selection algorithm within the server farm.

Syntax

predictor {**dest-ip-hash** | **roundrobin** {*ipv4-address-begin ipv4-address-end* | *acl-list*}}

no predictor roundrobin

Parameters

dest-ip-hash	Specifies that the destination IP hash method will be the used as the cache server selection algorithm.
round-robin	Specifies that round robin method will be used as the cache server selection algorithm.
ipv4-address-begin	The beginning IP address of a list of destination IP addresses for which the cache servers within this server farm will be selected by the round-robin algorithm (IPv4 TWCB server farm only).
ipv4-address-end	The ending IP address of a list of destination IP addresses for which the cache servers within this server farm will be selected by the round-robin algorithm (IPv4 TWCB server farm only).
acl-list	An IPv4 or IPv6 ACL list containing IP address permit statements for cache servers that will be selected using the round robin predictor.

Defaults

The TWCB predictor defaults to the destination IP hash method for the cache server selection algorithm.

Mode

Configuration command, TWCB Server Farm Configuration mode.

Usage

The predictor setting determines the cache server selection algorithm within the server farm. Predictor can be set to an internal IP destination address hash or a round robin algorithm.

By default, the router will select a cache server based on a hash of the destination IP address of the web site being accessed. If a web site is accessed frequently, the cache server serving requests for this destination IP address may become overloaded with user requests. Using the round robin predictor type, traffic to a particular range of destination IP addresses can be balanced between caches on the server farm.

In an IPv6 TWCB server farm round robin context, you must use an IPv6 access list to define the cache servers used by the round robin. In an IPv4 TWCB server farm round robin context, you can either use an IPv4 access list or specify a beginning and end IP address for a range of cache servers.

The "no" form of this command resets the predictor to the default value of the destination IP address selection method.

Use the "cache" on page 70-5 command to assign a round-robin weight to a cache server when the round-robin predictor is configured.

Examples

This example configures a predictor round-robin for the IPv4 web cache server farm **s1Server** specifying that the end users with IP addresses from **10.10.10.05** through **10.10.10.25** should be selected on a round-robin basis for caching on cache servers belonging to this server farm:

```
S Chassis(rw-config)->ip twcb wcserverfarm s1Server
S Chassis(rw-config-twcb-wcsfarm)->predictor roundrobin 10.10.10.05 10.10.10.25
```

This example configures a round robin predictor for the IPv6 web cache server farm **s2Server** specifying **ipv6cache1** as the IPv6 ACL list containing the list of cache server IP addresses to be used by the predictor:

```
S Chassis(rw-config)->ip twcb wcserverfarm s2Server
S Chassis(rw-config-twcb-wcsfarm)->predictor roundrobin ipv6cache1
```

cache

Use this command to create an IPv4 or IPv6 cache server based upon the supplied IP address.

Syntax

cache *ip-address*

no cache *ip-address*

Parameters

ip-address	Specifies the IPv4 or IPv6 IP address of the cache server to be created.

Defaults

None.

Mode

Configuration command, TWCB Server Farm Configuration mode

Usage

Executing this command enters cache server configuration command mode.

Examples

This example configures IP address **186.89.10.51** as a cache server on the **s1Server** server farm:

```
S Chassis(rw-config)->ip twcb wcserverfarm s1Server
S Chassis(rw-config-twcb-wcsfarm)->cache 186.89.10.51
S Chassis(rw-config-twcb-cache)->
```

This example configures IP address **2001:abcd::5** as a cache server on the **s1Server** server farm:

```
S Chassis(rw-config)->ip twcb wcserverfarm s1Server
S Chassis(rw-config-twcb-wcsfarm)->cache 2001:abcd::5
S Chassis(rw-config-twcb-cache)->
```

weight

Use this command to apply a cache weight value to IPv4 or IPv6 cache servers in a web cache server farm.

Syntax

weight *weight*

no weight

Parameters

weight	Specifies the weight assigned to an IPv4 or IPv6 cache server. Valid value range of **1**-**155**. Default: **1**.

Defaults

The cache server weight defaults to 1.

Mode

Configuration command, Cache Server Configuration mode.

Usage

The weight value only applies to caches being balanced via the round robin predictor type as described in “predictor” on page 70-4.

Weighted round robin is a round robin algorithm that takes into account a weight assigned to each cache server. Weight is a way of accounting for the resource differences between servers. If a server has the capacity to handle twice the number of sessions as another server, its weight ratio to the other server can be set to 2:1. The default weight for all cache servers is **1**. When all cache servers are configured with the default weight, each cache server is treated equally. When a non-default weight is applied to any cache servers in the web cache server farm, the algorithm takes that weight into account when assigning sessions to the cache servers.

Consider the following example. A server farm contains three cache servers with the following weights: server A has a weight of **1**, server B has a weight of **2**, and server C has a weight of **3**. For each six (the sum of the three weights) active sessions, server A will be assigned 1 session, server B will be assigned 2 sessions, and server C will be assigned 3 sessions in a round robin fashion. For this example, the weight ratio between the three servers would be 1:2:3.

Example

This example configures the cache server **186.89.10.51** on the **s1Server** server farm with a weight of **2**:

```
S Chassis(rw-config)->ip twcb wcserverfarm s1Server
S Chassis(rw-config-twcb-wcsfarm)->cache 186.89.10.51
S Chassis(rw-config-twcb-cache)->weight 2
S Chassis(rw-config-twcb-cache)->
```

This example configures the cache server **2001:abcd::5** on the **s2Server** server farm with a weight of **3**:

```
S Chassis(rw-config)->ip twcb wcserverfarm s2Server
S Chassis(rw-config-twcb-wcsfarm)->cache 2001:abcd::5
S Chassis(rw-config-twcb-cache)->weight 3
S Chassis(rw-config-twcb-cache)->
```

faildetect probe

Use this command to assign up to two probes to the IPv4 or IPv6 TWCB cache server faildetect configuration.

Syntax

faildetect probe {**one** | **two**} *probe-name*

no faildetect probe {**one** | **two**} *probe-name*

Parameters

one | **two**	Specifies probe label the named probe is assigned to for this cache server.
probe-name	Specifies the name of the probe to be assigned to monitor this cache server.

Defaults

The faildetect probe one defaults to $twcb_default. Faildetect probe two is unconfigured.

Mode

Configuration command, TWCB Cache Server Configuration mode**.**

Usage

The TWCB fail detection feature supports the assigning of up to two probes per cache server. A probe can be assigned to probe **one** or **two**. By default the probe **$twcb_default** is assigned to probe **one**. If you do not wish any faildetect monitoring to occur for this cache server, set the faildetect type to **none**, using "faildetect type" on page 70-9.

Use "faildetect app-port" on page 70-8 to assign the port the specified probe will monitor.

Use the **no faildetect probe** command to remove the specified probe for this real server context.

Examples

This example shows how to create a TCP probe named **TCP-HTTP** and assign it to probe one of the **101.10.1.251** on server farm **s1Server** and **2001:abcd::5** port **80** cache servers on the server farm **s2Server**:

```
S Chassis(su)->configure
S Chassis(su-config)->probe TCP-HTTP tcp
S Chassis(su-config-probe)->inservice
S Chassis(su-config-probe)->exit
S Chassis(su-config)->ip twcb serverfarm s1Server
S Chassis(su-config-twcb-wcsfarm)->cache 101.10.1.251
S Chassis(su-config-twcb-cache)->faildetect probe one TCP-HTTP
S Chassis(su-config-twcb-cache)->inservice
S Chassis(su-config-twcb-cache)->exit
S Chassis(su-config-twcb-wcsfarm)->exit
S Chassis(su-config)->ip twcb serverfarm s2Server
S Chassis(su-config-twcb-wcsfarm)->cache 2001:abcd::5
S Chassis(su-config-twcb-cache)->faildetect probe one TCP-HTTP
S Chassis(su-config-twcb-cache)->inservice
S Chassis(su-config-twcb-cache)->
```

faildetect app-port

Use this command to set the port number the assigned probe will monitor for an IPv4 or IPv6 TWCB cache server context.

Syntax

faildetect app-port *port-number*

no faildetect app-port *port-number*

Parameters

port-number	Specifies the port the probe assigned to this cache server context will monitor. The default value is port **80**.

Defaults

The faildetect application port defaults to 80.

Mode

Configuration command, TWCB Cache Server Configuration mode**.**

Usage

TWCB fail detection sets the application port to 80 by default. Use this command to set the TCP port on the cache server to a value other than 80 if required.

Use the **no faildetect app-port** command to reset the TCP application port to the default value of **80**.

Example

This example shows how to assign the TCP probe **TCP-HTTP** to the **101.10.1.251** port 8080 cache server on the server farm s1Server and **2001:abcd::5** port **8080** cache server on the server farm **s2Server**:

```
S Chassis(su-config)->ip twcb serverfarm s1Server
S Chassis(su-config-twcb-wcsfarm)->cache 101.10.1.251
S Chassis(su-config-twcb-cache)->faildetect probe one TCP-HTTP
S Chassis(su-config-twcb-cache)->faildetect app-port 8080
S Chassis(su-config-twcb-cache)->inservice
S Chassis(su-config-twcb-cache)->exit
S Chassis(su-config-twcb-wcsfarm)->exit
S Chassis(su-config)->ip twcb serverfarm s2Server
S Chassis(su-config-twcb-wcsfarm)->cache 2001:abcd::5
S Chassis(su-config-twcb-cache)->faildetect probe one TCP-HTTP
S Chassis(su-config-twcb-cache)->faildetect app-port 8080
S Chassis(su-config-twcb-cache)->inservice
S Chassis(su-config-twcb-cache)->
```

faildetect type

Use this command to set whether fail detection is active or inactive for an IPv4 or IPv6 cache server configuration context.

Syntax

faildetect type {**none** | **probe**}

no faildetect type

Parameters

none	Specifies that fail detection is inactive and TWCB sets the cache server's operational state to UP, regardless of the actual operational state of the cache server.
probe	Specifies that fail detection is active. Fail detection monitors the cache server in accordance with its configuration. The default faildetect type is **probe**.

Defaults

The faildetect type defaults to **probe**.

Mode

Configuration command, TWCB Cache Server Configuration mode**.**

Usage

The **faildetect type** configuration determines whether fail detection is active or inactive for an IPv4 or IPv6 cache server context.

The **no faildetect type** command resets the fail detection type to the default value of **probe**.

Examples

This example shows how to set the faildetect type to **none** for cache server **101.10.1.251** port **80** of the **s1Server** server farm and **2001:abcd::5** port **80** of the **s2Server** server farm:

```
S Chassis(su-config)->ip slb serverfarm s1Server
S Chassis(su-config-twcb-wcsfarm)->cache 101.10.1.251
S Chassis(su-config-twcb-cache)->faildetect type none
S Chassis(su-config-twcb-cache)->inservice
S Chassis(su-config-twcb-cache)->exit
S Chassis(su-config-twcb-wcsfarm)->exit
S Chassis(su-config)->ip slb serverfarm s2Server
S Chassis(su-config-twcb-wcsfarm)->cache 2001:abcd::5
S Chassis(su-config-twcb-cache)->faildetect type none
S Chassis(su-config-twcb-cache)->inservice
S Chassis(su-config-twcb-cache)->
```

faildetect reset

Use this command to reset an IPv4 or IPv6 TWCB cache server faildetect configuration to its application default settings.

Syntax

faildetect reset

Parameters

None.

Defaults

None.

Mode

Configuration command, TWCB Cache Server Configuration mode**.**

Usage

The **faildetect reset** command in a cache server configuration context does the following:

- Sets the faildetect type to the default value of **probe**
- Sets the probe for faildetect probe **one** to **$twcb_default**
- Removes any configured probe for faildetect probe **two**

Example

This example shows how to reset all faildetect configuration to the factory default settings for the **101.10.1.251** cache server on server farm **s1Server** and **2001:abcd::5** cache server on the server farm **s2Server**:

```
S Chassis(su-config)->ip slb serverfarm s1Server
S Chassis(su-config-twcb-wcsfarm)->cache 101.10.1.251
S Chassis(su-config-twcb-cache)->faildetect reset
S Chassis(su-config-twcb-cache)->inservice
S Chassis(su-config-twcb-cache)->exit
S Chassis(su-config-twcb-wcsfarm)->exit
S Chassis(su-config)->ip slb serverfarm s2Server
S Chassis(su-config-twcb-wcsfarm)->cache 2001:abcd::5
S Chassis(su-config-twcb-cache)->faildetect reset
S Chassis(su-config-twcb-cache)->inservice
S Chassis(su-config-twcb-cache)->
```

maxconns

Use this command to limit the maximum number of connections to an IPv4 or IPv6 cache server.

Syntax

maxconns *number*

no maxconns

Parameters

number	Specifies the maximum number of connections allowed for this server. Values range from **0** to **65535**. Default value of no limit (**0**).

Defaults

None.

Mode

Configuration command, Cache Server Configuration mode.

Usage

Specifying **0** sets maximum connections to no limit.

The "no" form resets the maximum connections to the default value of **0** (unlimited).

Examples

This example sets the maximum number of connections for cache servers **186.89.10.51** and **2001:abcd::5** to **1000**:

```
S Chassis(rw-config)->ip twcb wcserverfarm s1Server
S Chassis(rw-config-twcb-wcsfarm)->cache 186.89.10.51
S Chassis(rw-config-twcb-cache)->maxconns 1000
S Chassis(rw-config-twcb-cache)->inservice
```

```
S Chassis(rw-config-twcb-cache)->exit
S Chassis(rw-config-twcb-wcsfarm)->exit
S Chassis(rw-config)->ipv6 twcb wcserverfarm s2Server
S Chassis(rw-config-twcb-wcsfarm)->cache 2001:abcd::5
S Chassis(rw-config-twcb-cache)->maxconns 1000
S Chassis(rw-config-twcb-cache)->inservice
S Chassis(rw-config-twcb-cache)->
```

inservice

Use this command to activate an IPv4 or IPv6 web cache, server farm, or cache server.

Syntax

inservice

no inservice

Parameters

None.

Defaults

None.

Mode

Configuration command, Cache Server Configuration.
Configuration command, Web Cache Configuration mode.
Configuration command, Web Cache Server Farm Configuration mode.

Usage

Enter the **inservice** command after all other parameters are configured for the server farm cache server or web cache context. For a web cache or cache server the default is **no inservice**. A web cache server farm is **inservice** by default.

Examples

This example sets the maximum number of connections for cache server **186.89.10.51** to **100** and activates the server:

```
S Chassis(rw-config)->ip twcb wcserverfarm s1Server
S Chassis(rw-config-twcb-wcsfarm)->cache 186.89.10.51
S Chassis(rw-config-twcb-cache)->maxconns 100
S Chassis(rw-config-twcb-cache)->inservice
```

This example adds the serverfarm farm **s1Server** to the web cache **cache1** and activates the web cache:

```
S Chassis(rw-config)->ip twcb webcache cache1
S Chassis(rw-config-twcb-webcache)->serverfarm s1Server
S Chassis(rw-config-twcb-webcache)->inservice
```

This example sets the maximum number of connections for cache server **2001:abcd::5** to **100** and activates the server:

```
S Chassis(rw-config)->ipv6 twcb wcserverfarm s2Server
S Chassis(rw-config-twcb-wcsfarm)->cache 2001:abcd::5
S Chassis(rw-config-twcb-cache)->maxconns 100
S Chassis(rw-config-twcb-wcsfarm)->inservice
```

this

Use this command to display web cache, server farm, or cache server information when within the configuration command mode for each entity.

Syntax

this

Parameters

None.

Defaults

None.

Mode

Configuration command, Cache Server Configuration.
Configuration command, Web Cache Configuration mode.
Configuration command, Web Cache Server Farm Configuration mode.

Example

This example displays information for the s1Server from within the s1Server configuration command mode:

```
S Chassis(rw-config)->ip twcb wcserverfarm s1Server
S Chassis(rw-config-twcb-wcsfarm)->this
Server-Farm: s1Server (DOWN)
   Predictor:               DEST-IP-HASH Connections:                    0
   Caches Configured:                  0 Hits:                           0
   Caches Up:                          0 State Changes:                  0
   WebCaches Using:                    0

Serverfarms in active state: 0
S Chassis(rw-config-twcb-wcsfarm)->
```

ip twcb webcache

Use this command to create a web cache using the specified name.

Syntax

ip twcb webcache *webcache-name*

no ip twcb webcache *webcache-name*

Parameters

webcache-name	Specifies the name of the web cache to be created. The name may be up to 63 characters in length.

Defaults

None.

Mode

Configuration command mode.

Usage

Up to 10 web caches can be configured on a device. Use the **show limit** command to determine the number of web caches supported on the device. A web cache supports a single protocol port such as port 80, 443 or 8080. A web cache can be configured per protocol port for each VRF segment configured on the device.

At least one cache server must be active before a web cache server can become active.

Executing this command enters web cache configuration command mode.

The "no" form of this command removes the specified web cache from the configuration.

Example

This example creates an IPv4 web cache named **cache1**:

```
S Chassis(rw-config)->ip twcb webcache cache1
S Chassis(rw-config-twcb-webcache)->
```

ipv6 twcb webcache

Use this command to create an IPv6 web cache using the specified name.

Syntax

ipv6 twcb webcache *webcache-name*

no ipv6 twcb webcache *webcache-name*

Parameters

webcache-name	Specifies the name of the web cache to be created. The name may be up to 63 characters in length.

Defaults

None.

Mode

Configuration command mode.

Usage

Up to 10 web caches can be configured on a device. Use the **show router limit** command to determine the number of web caches supported on the device. A web cache supports a single protocol port such as port 80, 443 or 8080. A web cache can be configured per protocol port for each VRF segment configured on the device.

At least one cache server must be active before a web cache server can become active.

Executing this command enters web cache configuration command mode.

The "no" form of this command removes the specified web cache from the configuration.

Example

This example creates an IPv6 web cache named **cache2**:

```
S Chassis(rw-config)->ipv6 twcb webcache cache2
S Chassis(rw-config-twcb-webcache)->
```

destination ip

Use this command to assign the access list containing public facing TWCB router web cache destination IP addresses.

Syntax

destination ip *access-list*

no destination ip *access-list*

Parameters

access-list	Specifies the IPv4 or IPv6 standard access list containing destination IP addresses for the TWCB router web cache.

Defaults

None.

Mode

Configuration command, web cache Configuration mode.

Usage

This command configures the TWCB destination NAT component of the TWCB source and destination NAT feature. The configuration of TWCB source and destination NAT allows the client, TWCB router, and web cache server to reside anywhere in the network and still provide for the forwarding of an HTTP request from the client to the web cache server. TWCB source and destination NAT also provides for the reverse forwarding from the web cache server to the client, assuring that the packet flow will pass through the TWCB router.

Destination IP addressing provides a public facing address, owned by the TWCB router, that the client making an HTTP request can use to reach the web cache server from anywhere in the network. The public web cache addresses are defined in a standard access list that is assigned to a web cache configuration using this command. TWCB forwards the HTTP request to the appropriate web cache server for processing.

Before TWCB forwards the HTTP request to the web cache server, it first selects a source NAT address from the IPv4 source NAT pool or IPv6 source NAT address range defined using "source nat pool" on page 70-17. Using this public facing source NAT address assures that the web cache server reverse packet flow will pass through the TWCB router on its way back to the client.

Example

This example configures the IPv4 web cache **cache1** with destination addresses contained in the access list **acl1** and IPv6 web cache **cache2** with destination addresses contained in the access list **acl2**:

```
S Chassis(rw-config)->ip twcb webcache cache1
S Chassis(rw-config-twcb-webcache)->destination ip acl1
S Chassis(rw-config-twcb-webcache)->exit
S Chassis(rw-config)->ipv6 twcb webcache cache2
S Chassis(rw-config-twcb-webcache)->destination ip acl2
```

idle timeout

Use this command to specify the number of seconds an IPv4 or IPv6 binding remains idle before being deleted.

Syntax

idle timeout *seconds*

no idle timeout

Parameters

seconds	Specifies the number of seconds a binding remains idle before being deleted. Valid values: **41** - **65535** seconds. Default value: **240** seconds.

Defaults

None.

Mode

Configuration command, Web Cache Configuration mode.

Usage

The "no" form of this command resets the idle-timeout value to its default value of **240** seconds.

Example

This example sets the idle timeout for web caches cache1 and cache2 to 6 minutes:

```
S Chassis(rw-config)->ip twcb webcache cache1
S Chassis(rw-config-twcb-webcache)->idle timeout 360
S Chassis(rw-config-twcb-webcache)->exit
```

```
S Chassis(rw-config)->ipv6 twcb webcache cache2
S Chassis(rw-config-twcb-webcache)->idle timeout 360
```

serverfarm

Use this command to add the specified server farm to this IPv4 or IPv6 web cache.

Syntax

serverfarm *serverfarm-name*

no serverfarm *serverfarm-name*

Parameters

serverfarm-name	Specifies the name of up to 63 characters in length of the server farm to add to this web cache.

Defaults

None.

Mode

Configuration command, Cache Server Configuration mode

Usage

The “no” form of this command removes the specified server farm from the web cache.

Example

This example adds the server farm **s1Server** to the **cache1** web cache and s2Server to the **cache2** web cache:

```
S Chassis(rw-config)->ip twcb webcache cache1
S Chassis(rw-config-twcb-webcache)->serverfarm s1Server
S Chassis(rw-config-twcb-webcache)->exit
S Chassis(rw-config)->ipv6 twcb webcache cache2
S Chassis(rw-config-twcb-webcache)->serverfarm s2Server
```

source nat pool

Use this command to configure the overloaded IPv4 address or an IPv6 range to which the web cache client will be natted.

Syntax

source nat pool {*ipv4-nat-pool* | *ipv6-address/prefix-len*}

no source nat pool {*ipv4-nat-pool* | *ipv6-address/prefix-len*}

Parameters

ipv4-nat-pool	Specifies an IPv4 NAT pool containing one or more overloaded external IP addresses web cache clients will use for natting their internal IP address.
ipv6-address/prefix-len	Specifies an IPv6 external IP address and prefix length web cache clients will use for natting their internal IP address.

Defaults

None.

Mode

Configuration command, Web-cache Configuration mode

Usage

This command configures the TWCB source NAT pool component of the TWCB source and destination NAT feature. The configuration of TWCB source and destination NAT allows the client, TWCB router, and web cache server to reside anywhere in the network and still provide for the forwarding of an HTTP request from the client to the web cache server. TWCB source and destination NAT also provides for the reverse forwarding from the web cache server to the client, assuring that the packet flow will pass through the TWCB router.

Standard TWCB operation requires that a cache server have a route back to the client through the TWCB router. Client addresses are often unknown to the cache server. The TWCB source and destination NAT feature addresses these two issues. TWCB source NAT, configured using this command, provides a TWCB public facing source address as the TWCB router forwards the packet on to the web cache server, assuring that the web cache server will reverse flow the packet back through the TWCB router. Destination NAT provides a public facing TWCB router web cache address from the perspective of the client and is configured using “destination ip” on page 70-15.

First configure destination NAT by assigning an access list containing a range of public facing IP addresses the client will use to reach the TWCB router web cache. See “destination ip” on page 70-15 for destination NAT configuration details.

When the HTTP request reaches the TWCB router, TWCB determines the web cache server that will process the request. Before it forwards the packet on to the web cache server, it selects a public facing source address configured using this command. When the web cache server forwards the reverse flow back to the client, it uses this public source NAT address as its destination. When the reverse packet arrives at the TWCB router, it uses the original client request’s destination IP address as the packet source and forwards the server response to the client.

By default, source natting of a TWCB router web cache address does not occur.

For IPv4, one or more overloaded public facing IP addresses are assigned to a NAT pool, allowing multiple clients to use the same external address, with NAPT assigning an unused port to differentiate between clients. For IPv6 clients, an IPv6 address and prefix length is specified providing a range of external IP addresses.

The IPv6 address definition requires a prefix length of 111 or less in order to account for the checksum-neutral calculation of the IPv6 client address.

The “no” form of this command removes the specified web cache IPv4 source NAT pool or IPv6 source NAT IP address and prefix length.

Example

This example assigns the **ipv4twcb_pool** to web cache **cache1** and the IPv6 **4000:1:2::/111** address range to web cache **cach2**:

```
S Chassis(rw-config)->ip twcb webcache cache1
S Chassis(rw-config-twcb-webcache)->source nat pool ipv4twcb_pool
S Chassis(rw-config-twcb-webcache)->exit
S Chassis(rw-config)->ipv6 twcb webcache cache2
S Chassis(rw-config-twcb-webcache)->source nat pool 4000:1:2::/111
```

bypass-list

Use this command to specify web sites for which HTTP requests are not redirected to the cache servers.

Syntax

bypass-list {**range** *begin-ip-address end-ip-address* | **aclName** *access-list*}

no bypass-list {**range** *begin-ip-address end-ip-address* | **aclName** *access-list*}

Parameters

begin-ip-address	Specifies an IPv4 address that begins a range of IPv4 addresses of sites for which HTTP requests are not redirected to the cache servers.
end-ip-address	Specifies an IPv4 address that ends a range of IPv4 addresses of sites for which HTTP requests are not redirected to the cache servers.
aclName *access-list*	Specifies an IPv4 or IPv6 ACL list containing permit statements specifying web sites for which HTTP requests are not redirected to the cache servers.

Defaults

None.

Mode

Configuration command, Web Cache Configuration mode.

Usage

Some web site hosts require source IP address authentication for user access. HTTP requests for these sites can not be redirected to the cache servers. This command provides for the creation of lists of IP addresses that need to bypass the cache servers.

Up to 10 ranges can be configured for IPv4 web caches. Both IPv4 and IPv6 web caches can use the ACL list option. IPv6 web caches must use the ACL list option.

The “no” form of this command deletes the specified range of IP addresses or ACL list.

Examples

This example creates a bypass list for IPv4 web cache **cache1** for IP address range **50.10.10.30** to **50.10.10.43**:

```
S Chassis(rw-config)->ip twcb webcache cache1
S Chassis(rw-config-twcb-webcache)->bypass-list range 50.10.10.30 50.10.10.43
```

This example creates a bypass list for IPv6 web cache **cache2** for the IPv6 range specified in bypass1_acl:

```
S Chassis(rw-config)->ipv6 twcb webcache cache2
S Chassis(rw-config-twcb-webcache)->bypass-list bypass1_acl
```

host redirect

Use this command to explicitly permit or deny redirection of HTTP requests for the list of end users to this web cache.

Syntax

host {**permit** | **deny** | **aclName** *access-list*} **redirect** {**range** *begin-ip-address end-ip-address*}

no host {**permit** | **deny** | **aclName** *access-list*} **redirect** {**range** *begin-ip-address end-ip-address*}

Parameters

permit | **deny**	Specifies whether the IPv4 or IPv6 IP addresses configured will be allowed or disallowed for host redirection.
aclName *access-list*	Specifies an IPv4 or IPv6 ACL list containing permit or deny statements for the IP addresses that will be allowed or disallowed for host redirection.
range	Specifies a range of IPv4 IP addresses.
begin-ip-address	Specifies an IPv4 address that begins a range to explicitly permit or deny redirection of HTTP requests from these end users to this web cache.
end-ip-address	Specifies an IPv4 address that ends a range to explicitly permit or deny redirection of HTTP requests from these end users to this web cache.

Defaults

None.

Mode

Configuration command, Cache Server Configuration mode.

Usage

You can explicitly specify end user clients whose HTTP requests are or are not redirected to the cache servers. If you do not explicitly specify such addresses, HTTP requests from all end users are redirected to the cache server.

Up to 10 IPv4 ranges can be configured. An IPv4 or IPv6 ACL list can be specified. IPv6 addresses must be specified as an IPv6 ACL list.

The “no” form of this command removes all or optionally the specified IPv4 range of host redirection configuration.

Examples

This example configures a **deny** list for end users **10.10.10.26** through **10.10.10.50**; HTTP traffic from these source IP addresses will not be redirected to the caches:

```
S Chassis(rw-config)->ip twcb webcache cache1
S Chassis(rw-config-twcb-webcache)->host deny redirect range 10.10.10.26
10.10.10.50
```

This example configures a **deny** list for end users specified in the **cache2deny** for **cache2**; HTTP traffic from these source IPv6 addresses will not be redirected to the caches:

```
S Chassis(rw-config)->ipv6 twcb webcache cache2
S Chassis(rw-config-twcb-webcache)->host deny redirect aclName cache2deny
```

ip twcb redirect out

Use this command to specify that HTTP traffic egressing the router from this VLAN should be evaluated to see if it needs to be redirected to the specified IPv4 web cache.

Syntax

ip twcb *ipv4-webcache-name* **redirect out**

no ip twcb *ipv4-webcache-name*

Parameters

webcache-name	Specifies the name of the IPv4 web cache to redirect outbound HTTP traffic to.

Defaults

None.

Mode

Configuration command, Interface Configuration mode.

Usage

The outbound interface is typically an interface that connects to the Internet. The outbound interface can be a VLAN, L3 tunnel, or L2 tunnel. Associate the specified IPv4 web cache to the indicated interface for redirection of HTTP traffic. Up to 3 interfaces can be associated with an IPv4 or IPv6 web cache.

You can configure up to 10 web caches on an interface.

Multiple web caches can be specified in a single command if the prefix characters for the caches are unique to all caches to be configured. For example, if three web caches were named: **wc_one**, **wc_two**, and **wc_three**, all three web caches could be configured for redirect out in a single command by specifying **wc_** as the *webcache-name*. Or **wc_two** and **wc_three** could be configured for redirect out in a single command line by specifying **wc_t** as the *webcache-name*.

Example

This example associates the **cache1** IPv4 web cache with **vlan 1** for the redirection of HTTP traffic:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 1
```

```
S Chassis(rw-config-intf-vlan.0.1)->ip twcb cache1 redirect out
```

ipv6 twcb redirect out

Use this command to specify that HTTP traffic egressing the router from this VLAN should be evaluated to see if it needs to be redirected to the specified IPv6 web cache.

Syntax

ip twcb *ipv6-webcache-name* **redirect out**

no ip twcb *ipv6-webcache-name*

Parameters

webcache-name	Specifies the name of the IPv6 web cache to redirect outbound HTTP traffic to.

Defaults

None.

Mode

Configuration command, Interface Configuration mode.

Usage

The outbound interface is typically an interface that connects to the Internet. The outbound interface can be a VLAN, L3 tunnel, or L2 tunnel. Associate the specified IPv6 web cache to the indicated interface for redirection of HTTP traffic. Up to 3 interfaces can be associated with an IPv4 or IPv6 web cache.

You can configure up to 10 web caches on an interface.

Multiple web caches can be specified in a single command if the prefix characters for the caches are unique to all caches to be configured. For example, if three web caches were named: **wc_one**, **wc_two**, and **wc_three**, all three web caches could be configured for redirect out in a single command by specifying **wc_** as the *webcache-name*. Or **wc_two** and **wc_three** could be configured for redirect out in a single command line by specifying **wc_t** as the *webcache-name*.

Example

This example associates the **cache2** IPv6 web cache with **vlan 1** for the redirection of HTTP traffic:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ipv6 twcb cache2 redirect out
```

show ip twcb wcserverfarms

Use this command to display information for the specified or all IPv4 server farms.

Syntax

show ip twcb wcserverfarms [*serverfarm-name*] [**detail**]

Parameters

serverfarm-name	(Optional) Specifies the server farm for the display of information.
detail	(Optional) Specifies that a detailed level of information should display.

Defaults

If a *serverfarm-name* is not specified, displays a summary of information for all configured server farms.

Mode

All command modes.

Example

This example displays information for the configured server farms:

```
S Chassis(rw)->show ip twcb wcserverfarms
                                          cache cache
wcserverfarm                    status    cfg   up    conns hits
-----------------------------------------------------------------
v4_farm                         DISABLED 9     0     0     0

Serverfarms in active state: 0
S Chassis(rw)->
```

show ipv6 twcb wcserverfarms

Use this command to display information for the specified or all IPv6 server farms.

Syntax

show ipv6 twcb wcserverfarms [*serverfarm-name*] [**detail**]

Parameters

serverfarm-name	(Optional) Specifies the server farm for the display of information.
detail	(Optional) Specifies that a detailed level of information should display.

Defaults

If a *serverfarm-name* is not specified, displays a summary of information for all configured server farms.

Mode

All command modes.

Example

This example displays information for the configured server farms:

```
S Chassis(rw)->show ipv6 twcb wcserverfarms
                                          cache cache
wcserverfarm                    status    cfg   up    conns hits
-----------------------------------------------------------------
v6_farm                         DOWN      1     0     0     0

Serverfarms in active state: 0
S Chassis(rw)->
```

show ip twcb webcaches

Use this command to display information associated with the specified or all IPv4 web caches.

Syntax

show ip twcb webcaches [*webcache-name* | **detail**]

Parameters

webcache-name	(Optional) Specifies the name of the web cache for the display of information.
detail	(Optional) Specifies that a detailed level of information should display.

Defaults

If no parameter is specified, detailed information for all web caches is displayed.

Mode

All command modes.

Example

This example displays detailed information about all configured web caches.:

```
S Chassis(rw)->show ip twcb webcaches detail
WebCache: v4_cache (DOWN) (IPv4)
   Current Conns:                      0 Hits:                          0
   Idle Timeout:                     240 State Changes:                 0
   Http-Port:                         80
   Source NAT Pool:              Not Set
   Destination IP:               Not Set

   Last state change:             TUE JUL 17 12:53:22 2012
   Last state change reason:      SERVERFARM changed state

   Serverfarms(1):
     v4_farm
```

```
   Bypass List Acl:              Not Set
   Host Acl:                     Not Set

Webcaches in active state: 0
S Chassis(rw)->
```

show ipv6 twcb webcaches

Use this command to display information associated with the specified or all IPv6 web caches.

Syntax

show ipv6 twcb webcaches [*webcache-name* | **detail**]

Parameters

webcache-name	(Optional) Specifies the name of the web cache for the display of information.
detail	(Optional) Specifies that a detailed level of information should display.

Defaults

If no parameter is specified, detailed information for all web caches is displayed.

Mode

All command modes.

Example

This example displays detailed information about all configured web caches.:

```
S Chassis(rw)->show ipv6 twcb webcaches detail
WebCache: v6_cache (DOWN) (IPv6)
   Current Conns:                    0 Hits:                          0
   Idle Timeout:                   240 State Changes:                 0
   Http-Port:                       80
   Source NAT Pool:              Not Set
   Destination IP:               Not Set

   Last state change:             TUE JUL 17 12:53:22 2012
   Last state change reason:      SERVERFARM changed state

   Serverfarms(1):
     v6_farm
   Bypass List Acl:              Not Set
   Host Acl:                     Not Set

Webcaches in active state: 0
S Chassis(rw)->
```

show ip twcb info

Use this command to display IPv4 and IPv6 cache, server farm and web cache resources used and available for this system.

Syntax

show ip twcb info

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

Firmware does not make a distinction between resources available to IPv4 and IPv6 TWCB components. This command and "show ipv6 twcb info" on page 70-26 display identical information.

Example

This example displays TWCB resource information for this system:

```
S Chassis(rw)->show ip twcb info

Object               System Max    Avail VRF Used
-------------------------------------------------
Caches                        500      490       10
Wcsfarm                        50       48        2
Webcache                       50       48        2
S Chassis(rw)->
```

show ipv6 twcb info

Use this command to display IPv6 cache, server farm and web cache resources used and available for this system.

Syntax

show ipv6 twcb info

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

Firmware does not make a distinction between resources available to IPv4 and IPv6 TWCB components. This command and “show ip twcb info” on page 70-26 display identical information.

Example

This example displays IPv6 TWCB resource information for this system:

```
S Chassis(rw)->show ipv6 twcb info

Object                System Max    Avail VRF Used
-------------------------------------------------
Caches                       500      490       10
Wcsfarm                       50       48        2
Webcache                      50       48        2
S Chassis(rw)->
```

show ip twcb caches

Use this command to display cache information associated with the specified or all IPv4 server farms.

Syntax

show ip twcb caches [*serverfarm-name*] [**detail**]

Parameters

serverfarm-name	(Optional) Specifies the name of the server farm for the display of cache information.
detail	(Optional) Specifies a detailed level of information should display.

Defaults

If no parameter is specified, information for all web caches is displayed.

Mode

All command modes.

Examples

This example displays information for all caches for this system:

```
S Chassis(rw)->show ip twcb caches
                                          fail      max   curr
cache               |ins|wcserverfarm     |type |wgt|conns|conns|hits
-------------------------------------------------------------------------------
2.1.10.2            |DIS|v4_farm          |Probe|1  |10   |0    |0
2.1.10.3            |DIS|v4_farm          |Probe|1  |10   |0    |0
2.1.10.4            |DIS|v4_farm          |Probe|1  |0    |0    |0
2.1.10.5            |DN |v4_farm          |Probe|1  |0    |0    |0
2.1.10.6            |DN |v4_farm          |Probe|1  |0    |0    |0
2.1.10.7            |DN |v4_farm          |Probe|1  |0    |0    |0
2.1.10.8            |DN |v4_farm          |Probe|1  |0    |0    |0
2.1.10.9            |DN |v4_farm          |Probe|1  |0    |0    |0
2.1.10.10           |DN |v4_farm          |Probe|1  |0    |0    |0

Caches in active state: 0
S Chassis(rw)->
```

This example displays detailed information for the v4_farm server farm cache:

```
S Chassis(rw)->show ip twcb caches v4_farm detail
WcServerfarm: v4_farm
  Cache Server: 2.1.10.2 (DISABLED) (IPv4)
    Fail-Detect:                    Probe Connections:                    0
    Weight:                             1 Hits:                           0
    Max Conns:                         10 State Changes:                  4
    App Port:                          80
    Probe One:   Not Set (default: "$twcb_default")
    Probe Two:   Not Set
    Last state change:   TUE JUL 17 10:31:09 2012
WcServerfarm: v4_farm
  Cache Server: 2.1.10.3 (DISABLED) (IPv4)
    Fail-Detect:                    Probe Connections:                    0
    Weight:                             1 Hits:                           0
    Max Conns:                         10 State Changes:                  4
    App Port:                          80
    Probe One:   Not Set (default: "$twcb_default")
    Probe Two:   Not Set
    Last state change:   TUE JUL 17 10:31:13 2012
.
.
.
S Chassis(rw)->
```

Table 70-1 provides an explanation of the command output.

Table 70-1 show ip twcb caches Output Display

Output...	What it displays...
cache	Specifies the IP address of the TWCB cache.
ins	Specifies the service state: • **UP** – TWCB cache is in service and available • **DN** – TWCB cache is in service and not available • **DIS** – TWCB cache is not in service
wcserverfarm	Specifies the server farm this real server belongs to.
fail type	Specifies the faildetection type configured for this real server: • **None** – Faildetect is not active on this device • **Probe** – Faildetect is active on this device
wgt	Specifies the weight configured for this TWCB cache.
max conns	Specifies the maximum number of connections allowed for this TWCB cache.
curr conns	Specifies the current number of connections in use for this TWCB cache.
hits	Specifies the total number of connections used since the last time statistics were cleared.

show ipv6 twcb caches

Use this command to display cache information associated with the specified or all IPv6 server farms.

Syntax

show ipv6 twcb caches [*serverfarm-name*] [**detail**]

Parameters

serverfarm-name	(Optional) Specifies the name of the server farm for the display of cache information.
detail	(Optional) Specifies a detailed level of information should display.

Defaults

If no parameter is specified, information for all web caches is displayed.

Mode

All command modes.

Examples

This example displays information for all caches for this system:

```
S Chassis(rw)->show ipv6 twcb caches
                                                fail      max   curr
cache                |ins|wcserverfarm      |type |wgt|conns|conns|hits
-------------------------------------------------------------------------------
2001:10::2           |DN |v6_farm           |Probe|1  |0    |0    |0

Caches in active state: 0
S Chassis(rw)->
```

This example displays detailed information for the v6_farm server farm cache:

```
S Chassis(rw)->show ipv6 twcb caches v6_farm detail
WcServerfarm: v6_farm
  Cache Server: 2001:10::2 (DOWN) (IPv6)
    Fail-Detect:                    Probe Connections:                    0
    Weight:                             1 Hits:                           0
    Max Conns:                   No Limit State Changes:                  2
    App Port:                          80
    Probe One:   Not Set (default: "$twcb_default")
    Probe Two:   Not Set
    Last state change:   TUE JUL 17 10:32:12 2012

Caches in active state: 0
S Chassis(rw)->
```

Table 70-1 provides an explanation of the command output.

Table 70-2 show ipv6 twcb caches Output Display

Output...	What it displays...
cache	Specifies the IP address of the TWCB cache.
ins	Specifies the service state: • **UP** – TWCB cache is in service and available • **DN** – TWCB cache is in service and not available • **DIS** – TWCB cache is not in service
wcserverfarm	Specifies the server farm this real server belongs to.
fail type	Specifies the faildetection type configured for this real server: • **None** – Faildetect is not active on this device • **Probe** – Faildetect is active on this device
wgt	Specifies the weight configured for this TWCB cache.
max conns	Specifies the maximum number of connections allowed for this TWCB cache.
curr conns	Specifies the current number of connections in use for this TWCB cache.

Table 70-2 show ipv6 twcb caches Output Display

Output...	What it displays...
hits	Specifies the total number of connections used since the last time statistics were cleared.

show ip twcb bindings

Use this command to display IPv4 TWCB bindings for this system.

Syntax

show ip twcb bindings {**summary** | **id** *id* | **match** {*sip* | ***}** {*dip* | ***}** [**detail**]}

Parameters

summary	Specifies a summary level of information for all bindings will display.
id *id*	Specifies the ID of the binding to display.
match *sip dip*	Specifies the source and destination IP addresses of the binding to display. An * can be used in each case to specify all IP addresses for that context.
detail	Specifies that a detailed level of information should display for the **match** option.

Defaults

If **detail** is not specified, summary information is displayed for the **match** option.

Mode

All command modes.

Usage

This command is used to show information about the active IPv4 TWCB bindings. In the output of this command, an * in the port field of the source IP address indicates all ports.

Examples

This example displays the IPv4 bindings summary for this device:

```
S Chassis(rw)->show ip twcb bindings summary

TWCB Binding Summary

Id     Source                Destination           Direction Hw Conns
-------------------------------------------------------------------------
131062 2.1.49.188:*          2.1.51.188:80         Forward          1
       2.1.51.188:80         2.1.49.188:*          Reverse
131063 2.1.49.192:*          2.1.51.188:80         Forward          1
       2.1.51.188:80         2.1.49.192:*          Reverse
131064 2.1.49.191:*          2.1.51.188:80         Forward          1
       2.1.51.188:80         2.1.49.191:*          Reverse
```

```
131065 2.1.49.190:*          2.1.51.188:80         Forward          1
       2.1.51.188:80         2.1.49.190:*          Reverse
131066 2.1.49.189:*          2.1.51.188:80         Forward          1
       2.1.51.188:80         2.1.49.189:*          Reverse

Number of bindings displayed: 5
S Chassis(rw)->
```

This example displays the IPv4 binding ID **131063**:

```
S Chassis(rw)->show ip twcb bindings id 131063

Id:                131063 (ESTABLISHED)
Forward Addresses:
Source:            2.1.49.192:*
Destination:       2.1.51.188:80
Reverse Addresses:
 Source:            2.1.51.188:80
 Destination:       2.1.49.192:*
Webcache:          v4_cache
Serverfarm:        v4_farm
Wcreal Server:     2.1.10.3
Created Date:      TUE JUL 17 13:55:43 2012
Expire Date:       TUE JUL 17 14:09:05 2012  (Timeout: 240s)
Hardware Conns:    1

Number of bindings displayed: 1
S Chassis(rw)->
```

show ipv6 twcb bindings

Use this command to display IPv6 TWCB bindings for this system.

Syntax

show ipv6 twcb bindings {**summary** | **id** *id* | **match** {*sip* | *****} {*dip* | *****} [**detail**]}

Parameters

summary	Specifies a summary level of information for all bindings will display.
id *id*	Specifies the ID of the binding to display.
match *sip dip*	Specifies the source and destination IP addresses of the binding to display. An * can be used in each case to specify all IP addresses for that context.
detail	Specifies that a detailed level of information should display for the **match** option.

Defaults

If **detail** is not specified, summary information is displayed for the **match** option.

Mode

All command modes.

Usage

This command is used to show information about the active IPv6 TWCB bindings. In the output of this command, an * in the port field of the source IP address indicates all ports.

Examples

This example displays the IPv6 bindings summary for this device:

```
S Chassis(rw)->show ipv6 twcb bindings summary

TWCB Binding Summary

       Source
Id     Destination                                          Direction Hw Conns
-------------------------------------------------------------------------------
131061 2001:49::188:*                                       FORWARD          1
       2001:51::188:80
       2001:51::188:80                                      REVERSE
       2001:49::188:*

Number of bindings displayed: 1
S Chassis(rw)->
```

This example displays the IPv6 binding ID **131063**:

```
S Chassis(rw)->show ipv6 twcb bindings id 131061

Id:                131061 (ESTABLISHED)
Forward Addresses:
Source:            2001:49::188:*
Destination:       2001:51::188:80
Reverse Addresses:
 Source:            2001:51::188:80
 Destination:       2001:49::188:*
Webcache:          v6_cache
Serverfarm:        v6_farm
Wcreal Server:     2001:10::2
Created Date:      TUE JUL 17 14:13:45 2012
Expire Date:       TUE JUL 17 14:19:50 2012  (Timeout: 240s)
Hardware Conns:    1
S Chassis(rw)->
```

show ip twcb statistics

Use this command to display TWCB statistics data.

Syntax

show ip twcb statistics [**-interesting**] [**-all_vrfs**]

Parameters

-interesting	(Optional) Displays only counters with non-zero values.
-all_vrfs	(Optional) Displays statistics for all VRFs.

Defaults

If no option is specified, all statistics for the current VRF context display.

Mode

All command modes.

Usage

TWCB statistics display as a combined IPv4 and IPv6 counter value.

Example

This example displays TWCB statistics data:

```
S Chassis(rw)->show ip twcb statistics

NOTE: This command displays statistics combined from both IPv4 and IPv6 TWCB.

TWCB Statistics

                Current    High       Deleted    Total
Bindings        0          0          0          0

Resources
Bindings Exhausted:       0          No Caches:                0
No IPv6 Portmap Port:     0

Webcaches Active:         0          Webcaches Active High:    0
Serverfarms Active:       0          Serverfarms Active High:  0
Caches Active:            0          Caches Active High:       0

Counters Last Cleared: TUE JUL 17 12:53:22 2012

TWCB Extended Statistics (Normalized for 5 seconds)
Bindings Per Sec:         0

S Chassis(rw)->
```

show ipv6 twcb statistics

Use this command to display TWCB statistics data.

Syntax

show ipv6 twcb statistics [**-interesting**] [**-all_vrfs**]

Parameters

-interesting	(Optional) Displays only counters with non-zero values.
-all_vrfs	(Optional) Displays statistics for all VRFs.

Defaults

If no option is specified, all statistics for the current VRF context display.

Mode

All command modes.

Usage

TWCB statistics display as a combined IPv4 and IPv6 counter value.

Example

This example displays TWCB statistics data:

```
S Chassis(rw)->show ipv6 twcb statistics

NOTE: This command displays statistics combined from both IPv4 and IPv6 TWCB.

TWCB Statistics

                Current    High       Deleted    Total
Bindings        0          0          0          0

Resources
Bindings Exhausted:       0          No Caches:                0
No IPv6 Portmap Port:     0

Webcaches Active:         0          Webcaches Active High:    0
Serverfarms Active:       0          Serverfarms Active High:  0
Caches Active:            0          Caches Active High:       0

Counters Last Cleared: TUE JUL 17 12:53:22 2012

TWCB Extended Statistics (Normalized for 5 seconds)
Bindings Per Sec:         0
```

```
S Chassis(rw)->
```

clear ip twcb

Use this command to reset the statistical data or bindings for an IPv4 web cache.

Syntax

clear ip twcb {**statistics** | **bindings** {**all** | *id* | **match** {*sip* | ***}}

Parameters

statistics	Clears all statistics for this web cache.
bindings	Specifies the bindings to be cleared as follows: • **all** - Clear all items • *id* - Clear a particular item • **match** - Clear the specified source IP address (sip) or all source IP addresses (*)

Defaults

None

Mode

All command modes.

Usage

The firmware tracks IPv4 and IPv6 TWCB statistics as a combined value. Both this command and "clear ipv6 twcb" on page 70-36 clear all TWCB statistics when specifying the **statistics** option.

Example

This example clears statistics for all IPv4 web caches, web cache server farms and cache servers:

```
S Chassis(rw)->clear ip twcb statistics
```

clear ipv6 twcb

Use this command to reset the statistical data or bindings for an IPv6 web cache.

Syntax

clear ipv6 twcb {**statistics** | **bindings** {**all** | *id* | **match** {*sip* | ***}}

Parameters

statistics	Clears all statistics for this web cache.
bindings	Specifies the bindings to be cleared as follows: • **all** - Clear all items • *id* - Clear a particular item • **match** - Clear the specified source IP address (sip) or all source IP addresses (*)

Defaults

None

Mode

All command modes.

Usage

The firmware tracks IPv4 and IPv6 TWCB statistics as a combined value. Both this command and “clear ip twcb” on page 70-36 clear all TWCB statistics when specifying the **statistics** option.

Example

This example clears statistics for all web caches, web cache server farms and cache servers:

```
S Chassis(rw)->clear ipv6 twcb statistics
```

71

RIP Commands

This chapter describes the RIP set of commands and how to use them. For information about configuring RIP, refer to the "Routing Information Protocol (RIP) Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
router rip	71-1
network	71-2
distance	71-3
ip rip offset	71-4
timers	71-4
key chain	71-5
key	71-6
key-string	71-6
accept-lifetime	71-7
send-lifetime	71-8
ip rip authentication keychain	71-9
ip rip authentication mode	71-10
passive-interface	71-10
redistribute	71-11
show ip protocols	71-12

router rip

Use this command to enable or disable RIP configuration mode.

Syntax

```
router rip
no router rip
```

Parameters

None.

Defaults

None.

Mode

Configuration command mode**.**

Usage

You must execute the **router rip** command to enable the protocol before completing many RIP-specific configuration tasks.

Use the **show running-config rip** command to display RIP configuration.

The "no" form of this command disables RIP.

Example

This example shows how to enable RIP:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router rip
S Chassis(rw-config-rip)->
```

network

Use this command to attach a network of directly connected networks to a RIP routing process, or to remove a network from a RIP routing process.

Syntax

network *ip-address wild-card-bits*

no network *ip-address wild-card-bits*

Parameters

ip-address	Specifies the IP address of a directly connected network that RIP will advertise to its neighboring routers.
wild-card-bits	Specifies a mask for the directly connected network.

Defaults

None.

Mode

Configuration command, RIP configuration command mode**.**

Usage

RIP network wildcard masks are reverse networks. This means that wherever there is a 1 in a regular netmask, use a 0 in a wildcard mask. For example, if the network mask is 255.255.255.0 (/24), specify a wildcard mask of 000.000.000.255.

The "no" form of this command removes the network from the RIP routing process.

Example

This example shows how to attach network 192.168.1.0 to the RIP routing process:

```
S Chassis(rw-config)->router rip
S Chassis(rw-config-rip)->network 192.168.1.0 0.0.0.255
```

distance

Use this command to configure the administrative distance for RIP routes.

Syntax

distance *weight*

no distance [*weight*]

Parameters

weight	Specifies an administrative distance for RIP routes. Valid values are **1**-**255**.

Defaults

None.

Mode

RIP configuration command mode**.**

Usage

If several routes (coming from different protocols) are presented to the Extreme Networks S-Series Route Table Manager (RTM), the protocol with the lowest administrative distance will be chosen for route installation. By default, RIP administrative distance is set to 120. The **distance** command can be used to change this value, resetting RIP's route preference in relation to other routes as shown in the table below.

Route Source	Default Distance
Connected	0
Static	1
OSPF	110
RIP	120

The "no" form of this command resets RIP administrative distance to the default value of 120.

Example

This example shows how to change the default administrative distance for RIP to 150:

```
S Chassis(rw-config)->router rip
S Chassis(rw-config-rip)->distance 150
```

ip rip offset

Use this command to add or remove an offset to the hop metric of an incoming or outgoing RIP route.

Syntax

ip rip offset {**in** | **out**} *value*

no ip rip offset {**in** | **out**}

Parameters

in	Applies the hop offset to incoming metrics.
out	Applies the hop offset to outgoing metrics.
value	Specifies a positive offset to be applied to routes learned via RIP. Valid values are from **0** to **16**. If the value is 0, no action is taken.

Defaults

None.

Mode

Interface configuration command mode.

Usage

Adding an offset on an interface is used for the purpose of making an interface a backup.

The "no" form of this command removes an offset.

Example

The following example shows how to add an offset of 1 to incoming RIP metrics on VLAN 1:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip rip offset in 1
```

timers

Use this command to adjust RIP routing timers determining the frequency of routing updates, the length of time before a route becomes invalid, and the interval during which routing information regarding better paths is suppressed.

Syntax

timers basic *update-seconds invalid-seconds flush-seconds*

no timers basic

Parameters

basic	Specifies a basic configuration for RIP routing timers.
update-seconds	Specifies the interval (seconds between updates) at which routing updates are sent. Valid values are **1** to **255**. Default: **30** seconds.

invalid-seconds	Specifies the interval (in seconds) from the point of the last update after which a route times out and is marked as expired. Valid values are **1** to **255**. Default: **180** seconds.
flush-seconds	Specifies the interval (in seconds) from the point of a routes expiration after which a route is deleted from the routing table. Valid values are **1** to **255**. Default: **120** seconds.

Defaults

None.

Mode

RIP configuration command mode. Read-Write

Usage

Use the **show ip protocols** command to display RIP timers configuration.

The "no" form of this command clears RIP timer parameters.

Example

This example shows how to set RIP timers to a 25 second update time, a 150 second invalid interval, and a 100 second flush time:

```
S Chassis(rw-config)->router rip
S Chassis(rw-config-rip)->timers basic 25 150 100
```

key chain

Creates or deletes a key chain used globally for RIP authentication.

Syntax

key chain *name*

no key chain *name*

Parameters

name	Specifies a name for the key chain.

Defaults

None.

Mode

Configuration command, Global configuration**.**

Usage

This command places you in key chain configuration command mode.

The "no" form of this command deletes the specified key chain.

Example

This example shows how to create a RIP authentication key chain called “md5key”:

```
S Chassis(rw-config)->key chain md5key
S Chassis(rw-config-keychain)->
```

key

Use this command to identify a RIP authentication key on a key chain.

Syntax

key *key-id*

no key *key-id*

Parameters

key-id	Specifies an authentication number for a key. Valid number are from **1** to **255**. Only one key is supported per key chain in this Extreme Networks S-Series release.

Defaults

None.

Mode

Configuration command, key chain configuration**.**

Usage

This release of the Extreme Networks S-Series firmware supports only **one** key per key chain.

This command places you in key configuration command mode.

The “no” form of this command removes the key from the key chain.

Example

This example shows how to create authentication key 3 within the key chain called “md5key”:

```
S Chassis(rw-config)->key chain md5key
S Chassis(rw-config-keychain)->key 3
```

key-string

Use this command to specify a RIP authentication string for a key. Once configured, this string must be sent and received in RIP packets in order for them to be authenticated.

Syntax

key-string *text*

no key-string *text*

Parameters

text	Specifies the authentication string that must be sent and received in RIP packets. The string can contain from 1 to 16 uppercase and lowercase alphanumeric characters, except that the first character cannot be a number.

Defaults

None.

Mode

Configuration command, key configuration**.**

Usage

The "no" form of this command removes the authentication string.

Example

This example shows how to create an authentication string called "password" for key 3 in the "md5key" key chain:

```
S Chassis(rw-config)->key chain md5key
S Chassis(rw-config-keychain)->key 3
S Chassis(rw-config-keychain-key)->key-string password
```

accept-lifetime

Use this command to specify the time period during which an authentication key on a key chain is valid to be received.

Syntax

accept-lifetime *start-time* {*month date year | date month year*} {**duration** *seconds | end-time* | **infinite**}

no accept-lifetime *start-time month date year*

Parameters

start-time	Specifies the time of day the authentication key will begin to be valid to be received. Valid input is hours:minutes:seconds (*hh:mm:ss*).
month	Specifies the month the authentication key will begin to be valid to be received. Valid input is the first three letters of the month.
date	Specifies the day of the month the authentication key will begin to be valid to be received. Valid values, depending on the length of the month, are **1** - **31**.
year	Specifies the year the authentication key will begin to be valid to be received. Valid input is four digits up to **2035**.
duration *seconds*	Length of time (in seconds) the key is valid to be received. Valid values are **1** - **4294967295**.

end-time	Specifies the hours, minutes and seconds (*hh:mm:ss)* and the *month*, *date* and *year* from the start-time the key is valid to be received.
infinite	Specifies that the key is valid to be received from the start-time on.

Defaults

None.

Mode

Configuration command, key configuration**.**

Usage

The "no" form of this command removes the accept-lifetime configuration for an authentication key.

Examples

This example shows how to allow the "password" authentication key to be received as valid on its RIP-configured interface beginning at 2:30 on November 30, 2002 with no ending time (infinitely):

```
S Chassis(rw-config)->key chain md5key
S Chassis>Router(config-keychain)->key 3
S Chassis>Router(config-keychain-key)->key-string password
S Chassis>Router(config-keychain-key)->accept-lifetime 02:30:00 nov 30 2002
infinite
```

send-lifetime

Use this command to specify the time period during which an authentication key on a key chain is valid to be sent.

Syntax

send-lifetime *start-time month date year* {**duration** *seconds* | *end-time* | **infinite**}

no send-lifetime [*start-time month date year*]

Parameters

start-time	Specifies the time of day the authentication key will begin to be valid to be sent. Valid input is hours:minutes:seconds (*hh:mm:ss*).
month	Specifies the month the authentication key will begin to be valid to be sent. Valid input is the first three letters of the month.
date	Specifies the day of the month the authentication key will begin to be valid to be sent. Valid values, depending on the length of the month, are **1** - **31**.
year	Specifies the year the authentication key will begin to be valid to be sent. Valid input is four digits up to **2035**.
duration *seconds*	Length of time (in seconds) the key is valid to be sent. Valid values are **1** - **4294967295**.

end-time	Specifies the hours, minutes and seconds (*hh:mm:ss)* and the *month*, *date* and *year* from the start-time the key is valid to be sent.
infinite	Specifies that the key is valid to be sent from the start-time on.

Defaults

None.

Mode

Configuration command, Key chain key configuration**.**

Usage

The "no" form of this command removes the send-lifetime configuration for an authentication key. Start time can be specified, but is not mandatory.

Example

This example shows how to allow the "password" authentication key to be sent as valid on its RIP-configured interface beginning at 2:30 on November 30, 2002 with no ending time (infinitely):

```
S Chassis(rw-config)->key chain md5key
S Chassis(rw-config-keychain)->key 3
S Chassis(rw-config-keychain-key)->key-string password
S Chassis(rw-config-keychain-key)->send-lifetime 02:30:00 nov 30 2002 infinite
```

ip rip authentication keychain

Use this command to enable or disable a RIP authentication key chain for use on an interface.

Syntax

ip rip authentication keychain *name*

no ip rip authentication keychain *name*

Parameters

name	Specifies the key chain name to enable or disable for RIP authentication.

Defaults

None.

Mode

Interface configuration command mode.

Usage

Both a RIP authentication keychain must be enabled and the RIP authentication mode ("ip rip authentication mode" on page 71-10) must be configured before authentication will be active.

The "no" form of this command prevents RIP from using authentication.

Examples

This example shows how to set the RIP authentication key chain to "password" on VLAN 1:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip rip authentication keychain password
```

ip rip authentication mode

Use this command to set the authentication mode when a key chain is present.

Syntax

ip rip authentication mode {**text** | **md5**}

no ip rip authentication mode

Parameters

text	Initiates text-only authentication.
md5	Initiates MD5 authentication.

Defaults

None.

Mode

Interface configuration command mode.

Usage

The RIP authentication keychain must be enabled as described in "ip rip authentication keychain" on page 71-9 before RIP authentication mode can be configured.

The "no" form of this command suppresses the use of authentication.

Example

This example shows how to set the authentication mode for VLAN 1 as **text**:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip rip authentication mode text
```

passive-interface

Use this command to prevent RIP from transmitting update packets on an interface.

Syntax

passive-interface vlan *vlan-id*

no passive-interface vlan *vlan-id*

Parameters

vlan *vlan-id*	Specifies the number of the VLAN to make a passive interface. This VLAN must be configured for IP routing.

Defaults

None.

Mode

RIP configuration command mode**.**

Usage

This command does not prevent RIP from monitoring updates on the interface.

The "no" form of this command disables passive interface.

Example

This example shows how to set VLAN 2 as a passive interface. No RIP updates will be transmitted on VLAN 2:

```
S Chassis(rw-config)->router rip
S Chassis(rw-config-rip)->passive-interface vlan 2
```

redistribute

Use this command to allow routing information discovered through non-RIP protocols to be distributed in RIP update messages.

Syntax

redistribute {**connected** | **ospf** *process-id* | **static**} [**metric** *metric-value*]

no redistribute {**connected** | **ospf** *process-id* | **static**}

Parameters

connected	Specifies that non-RIP routing information discovered via directly connected interfaces will be redistributed.
ospf	Specifies that OSPF routing information will be redistributed in RIP.
process-id	Specifies the process ID, an internally used identification number for each instance of the OSPF routing process run on a router. Valid values are **1** to **65535**.
static	Specifies that non-RIP routing information discovered via static routes will be redistributed. Static routes are those created using the **ip route** command detailed in "ip route" on page 56-5.
metric *metric-value*	(Optional) Specifies a metric for the connected, OSPF or static redistribution route. This value should be consistent with the designation protocol.

Defaults

If *metric- value* is not specified, 1 will be applied.

Mode

RIP configuration command mode.

Usage

The “no” form of this command clears redistribution parameters.

Example

This example shows how to redistribute routing information discovered through OSPF process ID 1 non-subnetted routes into RIP update messages:

```
S Chassis(rw-config)->router rip
S Chassis(rw-config-rip)->redistribute ospf 1
```

show ip protocols

Use this command to display information about RIP and OSPF IP protocols running on the device, or under a topology.

Syntax

show ip protocols [topology <*topology-name*>] [summary]

Parameters

topology <*topology-name*>	(Optional) Specifies the name of the topology for which to display IP protocols.
summary	(Optional) Displays summary protocol information.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display IP protocol information:

```
S Chassis(rw)->show ip protocols

Routing Protocol is RIP
  Triggered Updates always
  Sending Updates every 30 seconds
  Invalid after 180 seconds
  Flush after 120 seconds
  Redistributing:
  Send and Receive version 2 only
                       Offset Offset
  Flag      Interface  In     Out    Key-chain
  -----     ---------- ---    ---    ----------
  Routing For Networks:
  Routing Information Sources:
  Distance: (default is 120)
```

```
Routing Protocol is OSPF
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing:  ospf 1
  Routing Information Sources:
199.113.113.0     0.0.0.255
```

72

Border Gateway Protocol Commands

This chapter describes the Border Gateway Protocol (BGP) set of commands and how to use them. For information about configuring BGP, refer to the "Border Gateway Protocol (BGP) Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
BGP Configuration Commands	72-1
Route Flap Damping Commands	72-62
Querying and Clearing Commands	72-68

BGP Configuration Commands

For information about...	Refer to page...
router bgp	72-3
bgp address-family	72-4
aggregate-address	72-5
bgp aggregate-med	72-7
bgp always-compare-med	72-8
bgp automatic-route-refresh	72-9
bgp cluster-id	72-9
bgp confederation-id	72-10
bgp deterministic-med	72-11
bgp distance	72-11
bgp orf comm-filter	72-12
bgp orf extcomm-filter	72-13
bgp orf prefix-filter	72-14
bgp graceful-restart	72-15
bgp local-pref	72-16
bgp max-ebgp-ecmp-routes	72-16
bgp max-ibgp-ecmp-routes	72-17
bgp restart-defer	72-18

For information about...	Refer to page...
bgp restart-time	72-19
bgp restart-timeout	72-19
bgp router-id	72-20
bgp stale-path-time	72-21
bgp strict-confeds	72-22
bgp trap	72-22
enable	72-23
ip prefix-list	72-24
ipv6 prefix-list	72-25
log-up-down	72-27
network	72-27
redistribute blackhole	72-30
redistribute connected	72-31
redistribute rip	72-32
redistribute static	72-33
redistribute ospf	72-34
redistribute isis	72-35
neighbor advertisement-interval	72-36
neighbor advertise-map	72-37
neighbor activate	72-39
neighbor aggregate-confed	72-39
neighbor as-origination-interval	72-40
neighbor check-next-hop	72-41
neighbor clear-counters	72-42
neighbor confed-member	72-42
neighbor connect-retry-interval	72-43
neighbor default-originate	72-44
neighbor enable	72-45
neighbor idle-hold-interval	72-45
neighbor ignore-leading-as	72-46
neighbor maximum-orf	72-47
neighbor maximum-prefix	72-48
neighbor next-hop-peer	72-49
neighbor next-hop-self	72-49
neighbor open-delay	72-50
neighbor passive	72-51

For information about...	Refer to page...
neighbor peer-group	72-52
neighbor peer-type	72-53
neighbor peering-type	72-53
neighbor remote-as	72-54
neighbor remove-private-as	72-55
neighbor route-map	72-56
neighbor route-reflector-client	72-57
neighbor route-withdraw-interval	72-58
neighbor soft-reconfiguration	72-58
neighbor timers	72-59
neighbor ttl	72-60
neighbor update-source	72-61

router bgp

This command enables BGP on a router and specifies the router's Autonomous System (AS) number.

Syntax

router bgp *as-number*

no router bgp *as-number*

Parameters

as-number	Specifies the AS number for this router. Valid values are **1** - **4294967295**.

Defaults

None.

Mode

Global Configuration.

Usage

The **router bgp** command enables BGP on a router. Because there is no default AS number, an autonomous system number must also be specified.

The **no router bgp** command disables BGP on a router.

Example

The following example configures the router to be a BGP speaker in AS number **65151**.

```
S Chassis(su)->configure
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->
```

bgp address-family

This command enters address family mode and configures Address Family Indicator (AFI) and Subsequent Address Family Indicator (SAFI) modes for BGP peers.

Syntax

```
bgp address-family [ipv4 | ipv6] [unicast | multicast]
no address-family {ipv4 | ipv6} {unicast | multicast}
```

Parameters

ipv4	(Optional) Specifies that the AFI mode is configured for IPv4 for this address family (default).
ipv6	(Optional) Specifies that the AFI mode is configured for IPv6 for this address family.
unicast | multicast	(Optional) Specifies that the SAFI mode is configured for either unicast or multicast for this address family. The default value is unicast.

Defaults

If no option is specified, the AFI mode is IPv4 unicast.

Mode

BGP Router Configuration.

Usage

By default BGP peers are enabled for carrying ipv4 unicast routes. For all other AFI/SAFI's a given peer must be "activated" for carrying routes of that type.

Use this command to enter the address family configuration mode for IPv4 unicast, IPv6 unicast, IPv4 multicast, or IPv6 multicast. Within the appropriate mode:

- Activate BGP neighbors using "neighbor activate" on page 72-39
- Configure BGP administrative distance for this address family context using "bgp distance" on page 72-11
- Redistribute routes for this address family context using the appropriate redistribution command:
  - "redistribute connected" on page 72-31
  - "redistribute rip" on page 72-32
  - "redistribute static" on page 72-33
  - "redistribute ospf" on page 72-34
  - "redistribute isis" on page 72-35
  - "redistribute blackhole" on page 72-30

Before configuring an IPv4 or IPv6 multicast address family, a multicast toplogy for that address family must be configured in the global configuration address family using "topology" on page 52-2. Enter the IPv4 or IPv6 multicast address family in global configuration mode using "address-family" on page 52-1, and configure the address family context with a topology before attempting to configure a BGP IPv4 or IPv6 multicast address family.

To disable a peer from carrying ipv4/unicast routes a BGP route-map is required.

The **no address-family** removes the configuration for the specified address family context.

Example

The following example enters the address family configuration mode for AFI/SAFI mode IPv6 unicast:

```
S Chassis(su-config-bgp)->address-family ipv6 unicast
S Chassis(su-config-bgp-af)->
```

The following example removes all address-family configuration for IPv6 unicast:

```
S Chassis(su-config-bgp)->no address-family ipv6 unicast
S Chassis(su-config-bgp)->
```

The following example configures an IPv4 multicast address family topology named MultiIPv4 and enters the IPv4 BGP multicast address family configuration mode:

```
S Chassis(su-config)->address-family ipv4 multicast
S Chassis(su-config-af)->topology MultiIPv4
S Chassis(su-config-af)->exit
S Chassis(su-config)->router bgp 1
S Chassis(su-config-bgp)->address-family ipv4 multicast
S Chassis(su-config-bgp-af)->
```

aggregate-address

This command creates an aggregate by combining the characteristics of multiple routes so that a single route is advertised.

Syntax

aggregate-address *prefix/length* [**summary**] [**as-set**] [**summary-and-as-set**] [**suppress-map** *route-map*] [**advertise-map** *route-map*] [**attribute-map** *route-map*]

no aggregate-address *prefix/length* [**summary**] [**as-set**] [**summary-and-as-set**] [**suppress-map** *route-map*] [**advertise-map** *route-map*] [**attribute-map** *route-map*]

Parameters

prefix/length	Specifies the prefix and length of the aggregate-address.
summary	(Optional) Specifies that BGP will suppress the advertisement of specified routes to all neighbors.
as-set	(Optional) Specifies that an aggregate entry AS path attribute contains an AS-SET which includes all the AS numbers contained in the contributor routes.
summary-and-as-set	(Optional) Specifies that both the **summary** and **as-set** options are enabled for this aggregate.
suppress-map *route-map*	(Optional) Specifies that match clauses for the specified route-map selectively suppress contributor routes from being advertised.
advertise-map *route-map*	(Optional) Specifies that match clauses for the specified route-map selectively advertise contributor routes.

attribute-map *route-map*	(Optional) Specifies that set clauses for the specified route-map set the attributes in the aggregated routes.

Defaults

- If the **summary** option is not specified, BGP will not suppress the advertisement of the contributor routes to neighbors.
- If the **as-set** option is not specified, aggregate entries do not inherit the AS path of the more specific routes in the routing updates.
- If the **summary-and-as-set** option is not specified, **summary** and **as-set** option settings are used to determine the behavior of those options.
- If the **suppress-map** option is not specified, routes specified in the aggregate route are advertised, unless the **summary** option is specified.
- If the **advertise-map** option is not specified, all routes specified in the aggregate route are advertised.
- If the **attribute-map** option is not specified, no modifications to the route attributes are made for the aggregate route.

Mode

BGP Router Configuration.

Usage

Route aggregation provides for the aggregating of one or more specific routes into a single aggregate route. Aggregate routes are only created if a more specific route of the aggregate route exists in the BGP routing table.

The **summary** option creates and advertises the aggregate route while at the same time suppressing the advertisement of all the more specific routes for this aggregate.

The **as-set** option retains the advertisement of the AS-Path information for the specific routes of the aggregate. The default behavior for an aggregate route is to suppress the AS-Path information for the specific routes of the aggregate. It may be desirable to retain AS-Path information for routes in the aggregate that belong to an AS outside of the AS in which the aggregate is created.

The **summary-and-as-set** option enables both the **summary** and **as-set** options using a single command option.

The **suppress-map** option creates and advertises an aggregate while at the same time suppressing only those specific routes that match clauses in the specified route-map. Prefixes contained in the aggregate route that are not specifically matched in the route-map are not suppressed. Do not use the **suppress-map** option in conjunction with the **summary** option.

The **advertise-map** option, when used in conjunction with the **as-set** option, creates and advertises an aggregate, while at the same time allows for specifying in a route-map which AS path information is retained in the aggregate. Do not use the **advertise-map** option in conjunction with the **summary** option.

The **attribute-map** option, creates and advertises an aggregate, while at the same time allows for the modifying of aggregate route attributes specified in the route-map.

The **no aggregate-address** command removes the specified aggregate.

Examples

The following example creates and advertises aggregate route 200.51.0.0/22 and suppresses the advertisement of all the more specific routes for this aggregate:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->aggregate-address 200.51.0.0/22 summary
S Chassis(su-config-bgp)->
```

The following example sets the MED attribute to 50 for routes in aggregate route **200.51.0.0/22** using route-map **attrmap1**:

```
S Chassis(su-config)->route-map bgp attrmap1 permit 10
S Chassis(su-config-route-map-bgp)->set med 50
S Chassis(su-config-route-map-bgp)->exit
S Chassis(su-config)->show route-map attrmap1
 route-map bgp attrmap1 permit 10
  set med 50
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->aggregate-address 200.51.0.0/22 attribute-map attrmap1
S Chassis(su-config-bgp)->
```

The following example retains AS-path information for routes **200.51.1.0/24** using route-map **advmap1** in aggregate route 200.51.0.0/22:

```
S Chassis(su-config)->ip prefix-list advlist1 permit seq 1 200.51.1.0/24
S Chassis(su-config)->route-map bgp advmap1
S Chassis(su-config-route-map-bgp)->match prefix-list advlist1
S Chassis(su-config-route-map-bgp)->exit
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->aggregate-address 200.51.0.0/22 as-set advertise-map
advmap1
S Chassis(su-config-bgp)->
```

bgp aggregate-med

This command enables aggregation of routes independent of the route Multi-Exit Discriminator (MED) value.

Syntax

bgp aggregate-med

no bgp aggregate-med

Parameters

None.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **no bgp aggregate-med** command resets the BGP MED aggregation capability to the default value of **disabled**.

Example

The following example enables BGP MED aggregation for BGP router 65151:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp aggregate-med
S Chassis(su-config-bgp)->
```

bgp always-compare-med

This command specifies whether to compare MEDs when multiple routes with differing MEDs are received from peers in different Autonomous Systems.

Syntax

bgp always-compare-med

no bgp always-compare-med

Parameters

None.

Defaults

None.

Mode

BGP Router Configuration.

Usage

MEDs are used when an AS has multiple connections to another AS. Routes are advertised on both connections with different MEDs to specify a preferred path, typically for purposes of load balancing. Typically, the MED for routes from different Autonomous Systems to the same destination are not compared. When two routes to the same destination are received from peers in different Autonomous Systems, the **bgp always-compare-med** command allows you to specify whether to compare those MEDs. When choosing between these routes, assuming that nothing else makes one preferable to the other (such as a configured policy), the values of the differing MEDs are used to choose the route to use. In this comparison, the route with the lowest MED is preferred.

Routes without MEDs are treated as having the best possible MED.

The **no bgp always-compare-med** command resets the always compare MED feature to the default value of disabled.

Example

The following example enables the comparison of MEDs from different ASs:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp always-compare-med
S Chassis(su-config-bgp)->
```

bgp automatic-route-refresh

This command enables the automatic sending of route-refresh messages on inbound policy changes.

Syntax

bgp automatic-route-refresh

no bgp automatic-route-refresh

Parameters

None.

Defaults

None.

Mode

BGP Router Configuration.

Usage

BGP automatic route refresh is enabled by default.

The **no automatic-route-refresh** command disables BGP automatic route refresh.

Example

The following example disables BGP automatic route refresh for BGP router 65151:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->no bgp automatic-route-refresh
S Chassis(su-config-bgp)->
```

bgp cluster-id

This command specifies the route reflection cluster ID for BGP.

Syntax

bgp cluster-id *cluster-id*

no bgp cluster-id *cluster-id*

Parameters

cluster-id	Specifies a cluster-ID in dotted-quad format used by route reflectors to prevent route propagation loops within the cluster.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **bgp cluster-id** command specifies the route reflection cluster ID for BGP. The cluster ID defaults to be the same as the router ID. If a router is to be a route reflector, then a single cluster ID should be selected and configured on all route reflectors in the cluster. If there is only one route reflector in the cluster, the cluster ID setting can be omitted because the default will suffice. The only constraints on the choice of cluster ID are the following:

- IDs of clusters within an AS must be unique within that AS.
- The cluster ID must not be 0.0.0.0

Example

The following example configures a cluster ID of 1.2.3.4 for AS 65151:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 151.1.1.9
S Chassis(su-config-bgp)->bgp cluster-id 1.2.3.4
S Chassis(su-config-bgp)->
```

bgp confederation-id

This command configures the BGP router to be a member of a BGP confederation.

Syntax

bgp confederation identifier *confed-id*

no bgp confederation identifier *confed-id*

Parameters

confed-id	Specifies a confederation identifier value. Valid values are **1** - **65535**.

Defaults

None.

Mode

BGP Router Configuration.

Usage

A BGP router can be configured to be a member of a BGP confederation when an AS is large and you wish to break it up into smaller groupings or where the network is subdivided into several AS's and you want to group members of multiple ASs. When configured as a confederation member, the router represents itself as the configured AS number to confederation peers and as the configured confederation identifier to non-confederation peers.

The **no bgp confederation identifier** command removes the configured confederation peer identifier for this router.

Example

The following example configures the BGP router to be a member of BGP confederation **100**:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 151.1.1.9
```

```
S Chassis(su-config-bgp)->bgp confederation-id 100
S Chassis(su-config-bgp)->
```

bgp deterministic-med

This command enables deterministic processing of MEDs.

Syntax

bgp deterministic-med

no bgp deterministic-med

Parameters

None.

Defaults

None.

Mode

BGP Router Configuration.

Usage

When BGP deterministic MED is enabled, BGP sorts paths based on the neighbor AS and MED so that paths are sorted the same way every time. This results in a deterministic best-path selection.

BGP deterministic MED is enabled by default.

The **no bgp deterministic-med** command disables BGP deterministic MED.

Example

The following example disables BGP deterministic MED for BGP router **65151**:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->no bgp deterministic-med
S Chassis(su-config-bgp)->
```

bgp distance

This command specifies the route selection priority given to internal or external BGP routes compared to other protocols for this router.

Syntax

bgp distance {**internal** | **external**} *distance*

no bgp distance {**internal** | **external**}

Parameters

internal *distance*	Specify a distance for routes internal to the AS. Valid values are **1** - **255**. Default value is **200**.
external *distance*	Specify a distance for routes external to the AS. Valid values are **1** - **255**. Default value is **20**.

Defaults

None.

Mode

BGP Router Configuration or BGP address family configuration mode.

Usage

The distance command specifies how active routes that are learned from BGP will be selected, compared to other protocols. When a route has been learned from more than one protocol, the active route will be selected from the protocol with the lowest distance (or preference).

The **no bgp distance** command resets the specified BGP protocol type to the default value. Internal BGP distance defaults to **200**. External BGP distance defaults to **20**.

Examples

The following example configures the distance (preference) for routes internal to the AS to be 113.

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 1.2.3.4
S Chassis(su-config-bgp)->bgp distance internal 113
```

The following example resets the distance (preference) distance for routes internal to the AS to the default value of 200.

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->no bgp distance internal
```

bgp orf comm-filter

This command specifies whether the Outbound Route Filtering (ORF) capability for community filtering is to be sent to the BGP peer, received from the BGP peer, or both.

Syntax

bgp orf {**ipv4** | **ipv6**} **unicast comm-filter** {**send** | **receive** | **both**}

no bgp orf {**ipv4** | **ipv6**} **unicast comm-filter** {**send** | **receive** | **both**}

Parameters

ipv4 | **ipv6 unicast**	Specifies the ORF configuration applies to IPv4 unicast or IPv6 addresses.
send	Specifies that the ORF capability for community filtering is sent to the BGP peer.
receive	Specifies that the ORF capability for community filtering is received from the BGP peer.
both	Specifies that the ORF capability for community filtering is both sent to and received from the BGP peer.

Defaults

None.

Mode

BGP Router Configuration.

Usage

This command is used to reduce the number of BGP community filtering advertisements the BGP speaker sends or receives from a peer router.

Most configurations will configure BGP to advertise both send and receive ORF community filtering capabilities. This feature can be configured in a single direction between two routers with one router configured to send and the other router configured to receive the ORF community filtering capability.

The **bgp orf comm-filter** command sets whether the ORF capability for community filtering will be sent to a BGP peer, received from a BGP peer, or both.

The **no bgp orf commfilter** command removes the configured ORF capability.

Example

This example specifies that BGP will send the ORF capability for community filtering for IPv4 unicast to the peer:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 151.1.1.9
S Chassis(su-config-bgp)->bgp orf ipv4 unicast comm-filter send
S Chassis(su-config-bgp)->
```

bgp orf extcomm-filter

This command specifies whether the Outbound Route Filtering (ORF) capability for extended community filtering is to be sent to the BGP peer, received from the BGP peer, or both.

Syntax

```
bgp orf {ipv4 | ipv6} unicast extcomm-filter {send | receive | both}
no orf {ipv4 | ipv6} unicast extcomm-filter {send | receive | both}
```

Parameters

ipv4 | ipv6 unicast	Specifies the ORF configuration applies to IPv4 unicast or IPv6 addresses.
send	Specifies that the ORF capability for extended community filtering is sent to the BGP peer.
receive	Specifies that the ORF capability for extended community filtering is received from the BGP peer.
both	Specifies that the ORF capability for extended community filtering is both sent to and received from the BGP peer.

Defaults

None.

Mode

BGP Router Configuration.

Usage

This command is used to reduce the number of BGP extended community filtering advertisements the BGP speaker sends or receives from a peer router.

Most configurations will configure BGP to advertise both send and receive ORF extended community filtering capabilities. This feature can be configured in a single direction between two routers with one router configured to send and the other router configured to receive the ORF extended community filtering capability.

The **bgp orf extcomm-filter** command specifies whether the ORF capability for extended community filtering is to be sent to a BGP peer, received from a BGP peer, or both.

The **no bgp orf extcomm-filter** command removes the configured ORF capability.

Example

This example specifies BGP to send the ORF capability for extended community filtering for IPv4 unicast to the peer:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 151.1.1.9
S Chassis(su-config-bgp)->bgp orf ipv4 unicast extcomm-filter send
S Chassis(su-config-bgp)->
```

bgp orf prefix-filter

This command specifies whether the Outbound Route Filtering (ORF) capability for prefix filtering is to be sent to the BGP peer, received from the BGP peer, or both.

Syntax

```
bgp orf {ipv4 | ipv6}unicast prefix-filter {send | receive | both}
no bgp orf {ipv4 | ipv6} unicast prefix-filter {send | receive | both}
```

Parameters

ipv4 | ipv6 unicast	Specifies the ORF configuration applies to IPv4 unicast or IPv6 addresses.
send	Specifies that the ORF capability for prefix filtering is sent to the BGP peer.
receive	Specifies that the ORF capability for prefix filtering is received from the BGP peer.
both	Specifies that the ORF capability for prefix filtering is both sent to and received from the BGP peer.

Defaults

None.

Mode

BGP Router Configuration.

Usage

This command is used to reduce the number of BGP prefix filtering advertisements the BGP speaker sends or receives from a peer router.

Most configurations will configure BGP to advertise both send and receive ORF prefix filtering capabilities. This feature can be configured in a single direction between two routers with one router configured to send and the other router configured to receive the ORF prefix filtering capability.

The **bgp orf prefix-filter** commands specifies whether the ORF capability for prefix filtering will be sent to a BGP peer, received from a BGP peer, or both.

The **no bgp orf prefixfilter** command removes the configured ORF capability.

Example

This example specifies BGP to send the ORF capability for prefix filtering to the BGP peer for IPv4 unicast:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 151.1.1.9
S Chassis(su-config-bgp)->bgp orf ipv4 unicast prefix-filter send
S Chassis(su-config-bgp)->
```

bgp graceful-restart

This command enables graceful restart on this router.

Syntax

bgp graceful-restart

no bgp graceful-restart

Parameters

None.

Defaults

None.

Mode

BGP Router Configuration.

Usage

With BGP graceful restart enabled, the data-forwarding plane of a router will continue to process and forward packets even if the control plane fails.

When the router restarts its BGP process, normally peer routers clear all routes associated with the restarting router. When graceful restart is enabled on a router, the peer router marks all routes as “stale” and continues to forward packets based on the expectation that the restarting router will reestablish the BGP session within a reasonable period of time. During the period of the restart, the restarting router continues to forward packets based upon routing state at the time of the restart. Peers refresh the restarting router with RIB updates. When the restarting router completes its restart and RIB update, it in turn updates its peers with any new updates.

The **no graceful-restart** command resets graceful restart to the default setting of **disabled**.

Example

The following example enables graceful restart on router 151.1.1.9

```
S Chassis(su-config-bgp)->bgp router 65151
S Chassis(su-config-bgp)->bgp router-id 151.1.1.9
S Chassis(su-config-bgp)->bgp graceful-restart
S Chassis(su-config-bgp)->
```

bgp local-pref

This command sets the local-preference for advertised routes.

Syntax

bgp local-pref *pref-value*

no bgp local-pref *pref-value*

Parameters

pref-value	Specifies the local-preference value for advertised routes. Valid values are **1** - **4294967295**. Default value is **100**.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The higher the local-preference value, the more preferred the route is. The local preference value is only applicable within the local AS.

Example

The following example sets the router local-preference for advertised routes to 150:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 151.1.1.9
S Chassis(su-config-bgp)->bgp local-pref 150
S Chassis(su-config-bgp)->
```

bgp max-ebgp-ecmp-routes

This command configures the maximum number of external BGP ECMP routes.

Syntax

bgp max-ebgp-ecmp-routes *value*

no bgp max-ebgp-ecmp-routes *value*

Parameters

value	Specifies the maximum number of EBGP ECMP routes configurable on this router. Valid values are **1** - **8**. Default value is **1**.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **no max-ebgp-ecmp-routes** command resets the maximum number of external BGP ECMP routes to the default value of **1**.

Example

The following example configures the maximum number of external BGP ECMP routes to 5:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 151.1.1.9
S Chassis(su-config-bgp)->bgp max-ebgp-ecmp-routes 5
S Chassis(su-config-bgp)->
```

bgp max-ibgp-ecmp-routes

This command configures the maximum number of internal BGP ECMP routes.

Syntax

bgp max-ibgp-ecmp-routes *value*

no bgp max-ibgp-ecmp-routes *value*

Parameters

value	Specifies the maximum number of IBGP ECMP routes configurable on this router. Valid values are **1** - **8**. Default value is **1**.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **no max-ibgp-ecmp-routes** command resets the maximum number of internal BGP ECMP routes to the default value of **1**.

Example

The following example configures the maximum number of internal BGP ECMP routes to **5**:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 151.1.1.9
S Chassis(su-config-bgp)->bgp max-ibgp-ecmp-routes 5
S Chassis(su-config-bgp)->
```

bgp restart-defer

This command configures the time to defer route selection after gracefully restarting.

Syntax

bgp restart-defer *time-seconds*

no bgp restart-defer

Parameters

time-seconds	Specifies the number of seconds to defer route selection after gracefully restarting the router. Valid values are **1** - **3600** seconds. Default value is **120** seconds.

Defaults

None.

Mode

BGP Router Configuration.

Usage

When BGP is restarting, the value configured for this defer timer is the upper bound (in seconds) on the amount of time route selection will be deferred. The value specified should be large enough to provide all peers with enough time to send all their routes. The value must be greater than or equal to the restart timeout setting.

Graceful restart must be enabled for the defer timer setting to be relevant.

The **no bgp restart-defer** command resets the defer timer value to the default value of **120** seconds.

Example

The following example configures the defer timer to 150 seconds:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 151.1.1.9
S Chassis(su-config-bgp)->bgp restart-defer 150
S Chassis(su-config-bgp)->
```

bgp restart-time

This command configures the maximum time to wait for a graceful restart capable peer to come back after a restart.

Syntax

bgp restart-time *time-seconds*

no bgp restart-time *time-seconds*

Parameters

time-seconds	Specifies the maximum amount of time in seconds this router will wait for a gracefully restarting peer to come back up. Valid values are **1** - **3600** seconds. Default value is **120** seconds.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **bgp restart-time** command configures the maximum time (in seconds) to wait for a graceful restart capable peer to come back after a restart. This value will be used instead of the restart timeout value advertised by the peer in its OPEN message, if the OPEN message value exceeds this restart timer value

Graceful restart must be enabled for the restart timer setting to be relevant.

The **no bgp restart-time** command resets the restart timer value to the default value of **120** seconds.

Example

The following example configures the restart time to be 100 seconds:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->bgp restart-time 100
S Chassis(su-config-bgp)->
```

bgp restart-timeout

This command configures the estimated time advertised to peers in the OPEN message for the session to be reestablished after a graceful restart.

Syntax

bgp restart-timeout *time-seconds*

no bgp restart-timeout

Parameters

time-seconds	Specifies the number of seconds advertised to peers for the session to be reestablished after a graceful restart. Valid values are from **1** - **3600**. The default value is **120** seconds.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **bgp restart-timeout** command specifies the interval which BGP advertises to its peers as the estimated time (in seconds) it will take for the BGP session to be re-established after a restart. This can be used to speed up routing convergence by its peer in case the BGP speaker does not come back after a restart.

Following a local restart, BGP will impose the restart timeout value as the upper bound on the length of time permitted for BGP to restart. If BGP fails to restart within the restart timeout period, the route selection process will commence immediately thereby overriding the defer timer.

This field is also the time BGP will wait for a failed stub to re-join. If the stub does not come back within this time, BGP will deactivate.

Graceful restart must be enabled for restart-timeout to be relevant.

The **no bgp restart-timeout** command resets the restart timeout value to the default value of **120** seconds.

Example

The following example configures the restart-timeout to be 150 seconds:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->bgp restart-timeout 150
```

bgp router-id

This command configures a BGP-specific router ID.

Syntax

bgp router-id *router-id*

no bgp router-id *router-id*

Parameters

router-id	Specifies a 32-bit integer in dotted-quad notation to be used as the BGP router ID. The default value is **0.0.0.0**.

Defaults

None.

Mode

BGP Router Configuration.

Usage

BGP router IDs must be unique.

The **no bgp router-id** resets the router ID to the default value of **0.0.0.0**.

Example

The following example configures the BGP Router ID to be 159.1.1.9:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->
```

bgp stale-path-time

This command configures the maximum time following a graceful restart before removing stale routes from the the peer.

Syntax

bgp stale-path-time *time-seconds*

no bgp stale-path-time

Parameters

time-seconds	Specifies the number of seconds to wait following a restart before removing stale routes from the the peer. Valid values are from **1** - **3600**. The default value is **150** seconds.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **bgp stale-path-time** setting must be greater than or equal to the configured restart time.

Graceful restart must be enabled for the stale path time setting to be relevant.

The **no bgp stale-path-time** command resets the stale path time value to the default value of **120** seconds.

Example

The following example configures the stale-path-time to be 130 seconds:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->bgp restart-timeout 130
```

bgp strict-confeds

This command enables BGP to drop AS-Paths with non-standard confederation segments.

Syntax

bgp strict-confeds

no bgp strict-confeds

Parameters

None.

Defaults

None.

Mode

BGP Router Configuration.

Usage

BGP strict-confeds is disabled by default.

The **no bgp strict-confeds** command resets the BGP strict-confeds setting to the default value of disabled.

Example

The following example enables the strict-confeds feature on this router:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp strict-confeds
S Chassis(su-config-bgp)->
```

bgp trap

This command enables the sending of BGP traps when a peer transitions to the Established state or a lower state.

Syntax

bgp trap {**peer-established** | **peer-degraded**}

no bgp trap {**peer-established** | **peer-degraded**}

Parameters

peer-established	Specifies that a trap is sent when a peer transitions to the Established state.
peer-degraded	Specifies that a trap is sent when a peer transitions to any lower state.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **no bgp trap** command resets the sending of peer transition traps to the default value of disabled.

Example

The following example enables the sending of traps when a peer transitions to the Established state:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp trap peer-established
S Chassis(su-config-bgp)->
```

enable

This command enables BGP.

Syntax

enable

no enable

Parameters

None.

Defaults

None.

Mode

BGP Router Configuration.

Usage

BGP is enabled when entering BGP configuration mode using the **router bgp** command. The only time you would need to administratively enable BGP is when you have disabled BGP using the **no enable** command.

The **enable** command enables BGP configuration on a router.

The **no enable** command disables BGP on a router.

Example

The following example disables BGP on the router:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->no enable
```

ip prefix-list

This command creates an IPv4 prefix list.

Syntax

```
ip prefix-list name [seq seq-value] {deny | permit} {prefix/length}
[source-address] [next-hop] [ge length] [le length] [nlri]
```

```
no ip prefix-list name [seq seq-value] {deny | permit} {network/masklen}
[ge length] [le length]
```

Parameters

name	Specifies the name of the prefix list as a string of characters.
seq *seq-value*	(Optional) Specifies the prefix list entry as an integer between **1** and **65535**, inclusive.
deny | **permit**	Specifies that matching prefixes for the specified source address or next hop are denied or permitted.
deny	Specifies that matching prefixes for the specified source address or next hop are denied.
prefix/length	Specifies a valid IPv4 prefix and length.
source-address	(Optional) Specifies that the configured parameters are matched against the IPv4 source address
next-hop	(Optional) Specifies that configured parameters are matched against the next hop attribute.
ge *length*	(Optional) Specifies that the IPv4 address matches (prefix, length) pairs with exactly the same prefix address and length that are greater than or equal to the value of the **ge** command. This value can be in the range of 0 to 32, but it must be at least the value of *length* and no greater than the value of **le**.
le *length*	(Optional) Specifies that the IPv4 address matches (prefix, length) pairs with exactly the same prefix address and length that are less than or equal to the value of the **le** command. This value can be in the range of 0 to 32, but it must be at least the value of length and no less than the value of **ge**.
nlri	(Optional) Specifies that the configured parameters are matched against the Network Layer Reachability Information (NLRI).

Defaults

- If the **seq** option is not specified, sequence number is generated automatically in increments of 5, starting with 0.
- If the **source-address** option is not specified, the match is not based upon the source address for this prefix.
- If the **next-hop** option is not specified, the match is not based upon the next hop attribute for this prefix.
- If the **ge** and **le** options are not specified, an exact match is assumed.
- If the **ge** option is not specified and the **le** option is, the range is assumed to be less than or equal to the **le** length.

- If the **le** option is not specified and the **ge** option is, then the range is assumed to be from the specified **ge** length to 32.

Mode

Router global configuration.

Usage

Prefix lists simulate a sequential lookup and return the first matched entry as the true match. The entries are ordered according to the sequential value. Sequence numbers are generated automatically in increments of **5** starting with **0**, unless the sequence option is specified.

The optional **ge** and **le** commands can be used to specify the range of the prefix length to be matched for prefixes that are more specific than a network and netmask value.

Configured prefix lists are used in BGP route-maps. A configured prefix-list is associated with a BGP route-map using the **match prefix-list** command in a BGP route-map configuration context.

The deny prefix-list match type should only be used for prefix-lists referenced by BGP route-maps with the ORF association set to local. Otherwise the permit/deny type of the route-map is used.

The **no prefix-list** command deletes all entries or specified entries in a prefix list. One way to remove a specific entry from a prefix list is to specify all parameters that were specified when the entry was created. Another way is to specify the sequence number of the entry.

Examples

The following example configures a prefix list "abc" that permits all prefixes in 128.0.0.0/8 with a prefix length of 24.

```
S Chassis(su-config)->ip prefix-list abc permit 128.0.0.0/8 ge 24 le 24
```

The following example configures a prefix list "abc" and permits all routes matching 10.0.0.0/24 with prefix length greater than or equal to 16:

```
S Chassis(su-config)->ip prefix-list abc seq 10 permit 10.0.0.0/24 ge 16
```

ipv6 prefix-list

This command creates an IPv6 prefix list.

Syntax

ipv6 prefix-list *name* [**seq** *seq_value*] {**deny** | **permit**} {*prefix/length*} [source-address] [next-hop] [**ge** length] [**le** length] [**nlri**]

no ipv6 prefix-list *name* [**seq** *seq_value*] {**deny** | **permit**} {*network/masklen*} [**ge** length] [**le** length]

Parameters

name	Specifies the name of the prefix list as a string of characters.
seq *seq_value*	Specifies the prefix list entry as an integer between 0 and 65535, inclusive.
permit	Specifies that matching IPv6 prefixes for the specified source address or next hop are permitted.
deny	Specifies that matching IPv6 prefixes for the specified source address or next hop are denied.

prefix/length	Specifies a valid IPv6 prefix and length.
source-address	(Optional) Specifies that the configured parameters are matched against the IPv6 source address
next-hop	(Optional) Specifies that configured parameters are matched against the next hop attribute.
ge *length*	(Optional) Specifies that the IPv6 address matches (prefix, length) pairs with exactly the same prefix address and length that are greater than or equal to the value of the **ge** command. This value can be in the range of 0 to 64, but it must be at least the value of *length* and no greater than the value of **le**.
le *length*	(Optional) Specifies that the IPv6 address matches (prefix, length) pairs with exactly the same prefix address and length that are less than or equal to the value of the **le** command. This value can be in the range of 0 to 64, but it must be at least the value of length and no less than the value of **ge**.
nlri	(Optional) Specifies that the configured parameters are matched against the Network Layer Reachability Info (NLRI).

Defaults

- If the **seq** option is not specified, sequence number is generated automatically in increments of 5, starting with 0.
- If the **source-address** option is not specified, the match is not based upon the source address for this prefix.
- If the **next-hop** option is not specified, the match is not based upon the next hop attribute for this prefix.
- If the **ge** and **le** options are not specified, an exact match is assumed.
- If the **ge** option is not specified and the **le** option is, the range is assumed to be less than or equal to the **le** length.
- If the **le** option is not specified and the **ge** option is, then the range is assumed to be from the specified **ge** length to 64.

Mode

Router global configuration.

Usage

Prefix lists simulate a sequential lookup and return the first matched entry as the true match. The entries are ordered according to the sequential value. Sequence numbers are generated automatically in increments of **5** starting with **0**, unless the sequence option is specified.

The optional **ge** and **le** commands can be used to specify the range of the prefix length to be matched for prefixes that are more specific than a network and netmask value.

Configured prefix lists are used in BGP route maps. A configured prefix-list is associated with a BGP route map using the **match prefix-list** command in a BGP route map configuration context.

The deny prefix-list match type should only be used for prefix-lists referenced by BGP route-maps with the ORF association set to local. Otherwise the permit/deny type of the route-map is used.

The **no prefix-list** command deletes all entries or specific entries in a prefix list. One way to remove a specific entry from a prefix list is to specify all parameters that were specified when the entry was created. Another way is to specify the sequence number of the entry.

Examples

The following example configures a prefix list “abc” that permits all prefixes in **2001::/8** with a prefix length of 24.

```
S Chassis(su-config)->ip prefix-list abc permit 2001::/8 ge 24 le 24
```

The following example configures a prefix list “abc” and permits all routes matching **2001::/24** with prefix length range of 16 to 64:

```
S Chassis(su-config)->ip prefix-list abc seq 10 permit 2001::/24 ge 16
```

log-up-down

This command causes a message to be logged via the syslog mechanism whenever a BGP peer enters or leaves the established state.

Syntax

log-up-down

no log-up-down

Parameters

None.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **log-up-down** command specifies whether a message will be logged via the syslog mechanism whenever a BGP peer enters or leaves the Established state. When the **log-up-down** command is enabled, it is specified in the running-config, even though the command is enabled by default.

The **no log-up-down** command disables logging a message via the syslog mechanism whenever a BGP peer enters or leaves the Established state.

Example

The following example causes a message to be logged in syslog whenever this peer leaves or enters the Established state:

```
S Chassis(su-config)->bgp router 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->log-up-down
```

network

This command specifies prefixes to be imported into BGP.

Syntax

network *prefix/length* [**route-map** *name*][**aspath-limit** *limit*] [**origin** *code*] [**med** *value*] [**local-pref** *value*]

no network *prefix/length* [**route-map** *name*][**aspath-limit** *limit*] [**origin** *code*] [**med** *value*] [**local-pref** *value*]

Parameters

prefix/length	Sets an IPv4 or IPv6 prefix and length of the network to be imported into BGP.
route-map *name*	(Optional) Specifies a route-map to be applied to this network when importing into BGP.
aspath-limit *limit*	(Optional) Specifies the upper limit on AS-path length. Valid values are **0** - **255**. Default value is **1**.
origin *code*	(Optional) Specifies the origin process attribute. Valid values are: **0** - IGP **1** - EGP **2** - Incomplete Default value is **0**.
med *value*	(Optional) Specifies the multi-exit discriminator value for this route. Valid values are **0** - **4294967295**. Default value is **0**.
local-pref *value*	(Optional) Specifies a route selection value for this route when the same prefix is learned from multiple peers. Valid values are **1** - **4294967295** seconds. Default value is **100**.

Defaults

- If a **route-map** is not specified, no route-map is applied.
- If an **aspath-limit** is not specified, the aspath-limit is not included in the update.
- If an **origin** code is not specified, the origin is set to the default value of **0** (IGP).
- If a **med** is not specified, the MED value is not included in the update and MED is treated as though it were set to **0**.
- If **local-pref** is not specified, the local-pref is set to the default value of **100**.

Mode

BGP Router Configuration.

Usage

The **network** command is used to specify prefixes that should be imported into BGP.

Note: When configuring an optional network parameter, the configured value is applied to all matching routes. It may be preferable to modify these parameters within a route-map to specify the routes to be matched. For the **network** command, use a redistribution route-map.

The **no network** command removes the specified network prefixes.

Examples

The following example imports the network 10.1.0.0 with a prefix length of 24 into BGP. Additionally, this network range will be advertised to other peers.

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->network 10.1.0.0/24
```

The following example imports the prefix 2001::/64 into BGP. This network will be advertised based upon the **routes1** route-map contents with origin set to IGP.

```
S Chassis(su-config)->router bgp 65151
S Chassis(config-router-bgp)-> bgp router-id 1.2.3.4
S Chassis(config-router-bgp)-> network 2001::/64 route-map routes1 origin 0
```

redistribute bgp

This command specifies that BGP routes are exported into BGP.

Syntax

redistribute bgp [[**global** [**aspath-limit** *limit*] [**origin** *code*] [**med** *value*] [**local-pref** *value*] [**route-map** *name*]]

no redistribute bgp [[**global** [**aspath-limit** *limit*] [**origin** *code*] [**med** *value*] [**local-pref** *value*] [**route-map** *name*]]

Parameters

global	(Optional) Specifies that BGP prefixes should be redistributed from the global VRF router. Defaults to the current VRF context.
aspath-limit *limit*	(Optional) Specifies the upper limit on AS-path length. Valid values are **0** - **255**. Default value is **1**.
origin *code*	(Optional) Specifies the origin process attribute. Valid values are: **0** - IGP **1** - EGP **2** - Incomplete Default value is **2**.
med *value*	(Optional) Specifies the multi-exit discriminator value for this route. Valid values are **0** - **4294967295**. Default value is **0**.
local-pref *value*	(Optional) Specifies a route selection value for this route when the same prefix is learned from multiple peers.
route-map *name*	(Optional) A route-map name to apply to these routes.

Defaults

If a **route-map** is not specified, no route-map is applied.

Mode

BGP Router Configuration or BGP address family configuration mode.

Usage

The **redistribute bgp** command provides for the exporting of BGP routes into BGP.

The **no redistribute bgp** command removes redistribution of BGP route configuration from the router.

Examples

In the following example BGP is configured to redistribute all BGP routes with the local preference set for 100.

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->redistribute bgp local-pref 100
```

redistribute blackhole

This command specifies that blackhole routes are exported into BGP.

Syntax

redistribute blackhole [**aspath-limit** *limit*] [**origin** *code*] [**med** *value*] [**local-pref** *value*] [**route-map** *name*]

no redistribute blackhole [**aspath-limit** *limit*] [**origin** *code*] [**med** *value*] [**local-pref** *value*] [**route-map** *name*]

Parameters

aspath-limit *limit*	(Optional) Specifies the upper limit on AS-path length. Valid values are **0** - **255**. Default value is **1**.
origin *code*	(Optional) Specifies the origin process attribute. Valid values are: **0** - IGP **1** - EGP **2** - Incomplete Default value is **2**.
med *value*	(Optional) Specifies the multi-exit discriminator value for this route. Valid values are **0** - **4294967295**. Default value is **0**.
local-pref *value*	(Optional) Specifies a route selection value for this route when the same prefix is learned from multiple peers.
route-map *name*	(Optional) A route-map name to apply to these routes.

Defaults

- If a **route-map** is not specified, no route-map is applied.
- If an **aspath-limit** is not specified, the aspath-limit is not included in updates.
- If an **origin** code is not specified, the origin is set to the default value of **2** (incomplete).
- If a **med** is not specified, the MED attribute is not included in updates. When MED is not included in an update, MED is treated as though it were set to **0**.

- If **local-pref** is not specified, the local-pref is set to the default value of **100**.

Mode

BGP Router Configuration or BGP address family configuration mode.

Usage

The **redistribute blackhole** command provides for the exporting of blackhole routes into BGP.

The **no redistribute blackhole** command removes redistribution of blackhole route configuration from the router.

Examples

In the following example BGP is configured to redistribute all blackhole routes with the local preference set for 100.

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->redistribute blackhole local-pref 100
```

redistribute connected

This command specifies that connected routes are exported into BGP.

Syntax

redistribute connected [**aspath-limit** *limit*] [**origin** *code*] [**med** *value*] [**local-pref** *value*] [**route-map** *name*]

no redistribute connected [**aspath-limit** *limit*] [**origin** *code*] [**med** *value*] [**local-pref** *value*] [**route-map** *name*]

Parameters

aspath-limit *limit*	(Optional) Specifies the upper limit on AS-path length. Valid values are **0** - **255**. Default value is **1**.
origin *code*	(Optional) Specifies the origin process attribute. Valid values are: **0** - IGP **1** - EGP **2** - Incomplete Default value is **2**.
med *value*	(Optional) Specifies the multi-exit discriminator value for this route. Valid values are **0** - **4294967295**. Default value is **0**.
local-pref *value*	(Optional) Specifies a route selection value for this route when the same prefix is learned from multiple peers.
route-map *name*	(Optional) A route-map name to apply to these routes.

Defaults

- If a **route-map** is not specified, no route-map is applied.
- If an **aspath-limit** is not specified, the aspath-limit is not included in updates.
- If an **origin** code is not specified, the origin is set to the default value of **2** (incomplete).

- If a **med** is not specified, the MED attribute is not included in updates. When MED is not included in an update, MED is treated as though it were set to **0**.
- If **local-pref** is not specified, the local-pref is set to the default value of **100**.

Mode

BGP Router Configuration or BGP address family configuration mode.

Usage

The redistribute connected command provides for the exporting of connected routes into BGP.

The **no redistribute connected** command removes redistribution of connected route configuration from the router.

Examples

In the following example BGP is configured to redistribute connected routes that match the contents of the **connRoute** route-map:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->redistribute connected route-map connRoute
```

redistribute rip

This command specifies that RIP routes are exported into BGP.

Syntax

redistribute rip [**aspath-limit** *limit*] [**origin** *code*] [**med** *value*] [**local-pref** *value*] [**route-map** *name*]

no redistribute rip [**aspath-limit** *limit*] [**origin** *code*] [**med** *value*] [**local-pref** *value*] [**route-map** *name*]

Parameters

aspath-limit *limit*	(Optional) Specifies the upper limit on AS-path length. Valid values are **0** - **255**. Default value is **1**.
origin *code*	(Optional) Specifies the origin process attribute. Valid values are: **0** - IGP **1** - EGP **2** - Incomplete Default value is **2**.
med *value*	(Optional) Specifies the multi-exit discriminator value for this route. Valid values are **0** - **4294967295**. Default value is **0**.
local-pref *value*	(Optional) Specifies a route selection value for this route when the same prefix is learned from multiple peers.
route-map *name*	(Optional) A route-map name to apply to these routes.

Defaults

- If a **route-map** is not specified, no route-map is applied.
- If an **aspath-limit** is not specified, the aspath-limit is not included in updates.

- If an **origin** code is not specified, the origin is set to the default value of **2** (incomplete).
- If a **med** is not specified, the MED attribute is not included in updates. When MED is not included in an update, MED is treated as though it were set to **0**.
- If **local-pref** is not specified, the local-pref is set to the default value of **100**.

Mode

BGP Router Configuration or BGP address family configuration mode.

Usage

The **redistribute rip** command provides for the exporting of RIP routes into BGP.

The **no redistribute rip** command removes redistribution of RIP route configuration from the router.

Examples

In the following example BGP is configured to redistribute all RIP routes with the local preference set for 100.

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->redistribute rip local-pref 100
```

redistribute static

This command specifies that static routes are exported into BGP.

Syntax

redistribute static [**aspath-limit** *limit*] [**origin** *code*] [**med** *value*] [**local-pref** *value*] [**route-map** *name*]

no redistribute static [**aspath-limit** *limit*] [**origin** *code*] [**med** *value*] [**local-pref** *value*] [**route-map** *name*]

Parameters

aspath-limit *limit*	(Optional) Specifies the upper limit on AS-path length. Valid values are **0** - **255**. Default value is **1**.
origin *code*	(Optional) Specifies the origin process attribute. Valid values are: **0** - IGP **1** - EGP **2** - Incomplete Default value is **2**.
med *value*	(Optional) Specifies the multi-exit discriminator value for this route. Valid values are **0** - **4294967295**. Default value is **0**.
local-pref *value*	(Optional) Specifies a route selection value for this route when the same prefix is learned from multiple peers.
route-map *name*	(Optional) A route-map name to apply to these routes.

Defaults

- If a **route-map** is not specified, no route-map is applied.

- If an **aspath-limit** is not specified, the aspath-limit is not included in updates.
- If an **origin** code is not specified, the origin is set to the default value of **2** (incomplete).
- If a **med** is not specified, the MED attribute is not included in updates. When MED is not included in an update, MED is treated as though it were set to **0**.
- If **local-pref** is not specified, the local-pref is set to the default value of **100**.

Mode

BGP Router Configuration or BGP address family configuration mode.

Usage

The **redistribute static** command provides for the exporting of static routes into BGP.

The **no redistribute static** command removes redistribution of static route configuration from the router.

Examples

In the following example BGP is configured to redistribute all static routes with the local preference set for 100.

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->redistribute static local-pref 100
```

redistribute ospf

Syntax

redistribute ospf *proc-id* [**aspath-limit** *limit*] [**origin** *code*] [**med** *value*] [**local-pref** *value*] [**route-map** *name*]

no redistribute ospf [**aspath-limit** *limit*] [**origin** *code*] [**med** *value*] [**local-pref** *value*] [**route-map** *name*]

Parameters

proc-id	Specifies an OSPF process ID.
aspath-limit *limit*	(Optional) Specifies the upper limit on AS-path length. Valid values are **0** - **255**. Default value is **1**.
origin *code*	(Optional) Specifies the origin process attribute. Valid values are: **0** - IGP **1** - EGP **2** - Incomplete Default value is **2**.
med *value*	(Optional) Specifies the multi-exit discriminator value for this route. Valid values are **0** - **4294967295**. Default value is **0**.
local-pref *value*	(Optional) Specifies a route selection value for this route when the same prefix is learned from multiple peers.
route-map *name*	(Optional) A route-map name to apply to these routes.

Defaults

- If a **route-map** is not specified, no route-map is applied.
- If an **aspath-limit** is not specified, the aspath-limit is not included in updates.
- If an **origin** code is not specified, the origin is set to the default value of **2** (incomplete).
- If a **med** is not specified, the MED attribute is not included in updates. When MED is not included in an update, MED is treated as though it were set to **0**.
- If **local-pref** is not specified, the local-pref is set to the default value of **100**.

Mode

BGP Router Configuration or BGP address family configuration mode.

Usage

The **redistribute ospf** command provides for the exporting of OSPF routes into BGP.

The **no redistribute ospf** command removes redistribution of OSPF route configuration from the router.

Examples

In the following example BGP is configured to redistribute OSPF routes that match the contents of the **OSPFroutes** route-map.

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->redistribute ospf route-map OSPFroutes
```

redistribute isis

This command specifies that IS-IS routes are exported into BGP.

Syntax

redistribute isis [**aspath-limit** *limit*] [**origin** *code*] [**med** *value*] [**local-pref** *value*] [**route-map** *name*] [**match** {**level-1-internal** | **level-1-external** | **level-2-internal** | **level-2-external** | **level-1-2**}

no redistribute isis [**aspath-limit** *limit*] [**origin** *code*] [**med** *value*] [**local-pref** *value*] [**route-map** *name*] [**match** {**level-1-internal** | **level-1-external** | **level-2-internal** | **level-2-external** | **level-1-2**}

Parameters

aspath-limit *limit*	(Optional) Specifies the upper limit on AS-path length. Valid values are **0** - **255**. Default value is **1**.
origin *code*	(Optional) Specifies the origin process attribute. Valid values are: **0** - IGP **1** - EGP **2** - Incomplete Default value is **2**.
med *value*	(Optional) Specifies the multi-exit discriminator value for this route. Valid values are **0** - **4294967295**. Default value is **0**.

local-pref *value*	(Optional) Specifies a route selection value for this route when the same prefix is learned from multiple peers.
route-map *name*	(Optional) A route-map name to apply to these routes.
match	(Optional) Redistribute the specified IS-IS route type only.
level-1-internal	Match ISIS level-1 internal routes.
level-1-external	Redistribute ISIS level-1 external routes.
level-2-internal	Redistribute ISIS level-2 internal routes.
level-2-external	Redistribute ISIS level-2 external routes.
level-1-2	Redistribute ISIS level-1 and level-2 routes.

Defaults

- If a **route-map** is not specified, no route-map is applied.
- If an **aspath-limit** is not specified, the aspath-limit is not included in updates.
- If an **origin** code is not specified, the origin is set to the default value of **2** (incomplete).
- If a **med** is not specified, the MED attribute is not included in updates. When MED is not included in an update, MED is treated as though it were set to **0**.
- If **local-pref** is not specified, the local-pref is set to the default value of **100**.
- If an IS-IS route **match** type is not specified, all IS-IS route types are redistributed.

Mode

BGP Router Configuration or BGP address family configuration mode.

Usage

The **redistribute isis** command provides for the exporting of IS-IS routes into BGP.

The **no redistribute isis** command removes redistribution of IS-IS route configuration from the router.

Examples

In the following example BGP is configured to redistribute all IS-IS routes with the local preference set for 100.

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->redistribute isis local-pref 100
```

neighbor advertisement-interval

This command sets the minimum interval between the sending of EBGP routing updates.

Syntax

neighbor *ip-address* **advertisement-interval** *interval*

no neighbor *ip-address* **advertisement-interval**

Parameters

ip-address	Specifies a BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.
interval	Specifies the interval in seconds between the sending of BGP routing updates. Valid values are **1** - **65535** seconds. The default value is **30** seconds.

Defaults

None.

Mode

BGP Router Configuration.

Usage

BGP sends an UPDATE or WITHDRAWN message whenever an advertised EBGP route changes unless a minimum EBGP advertisement-interval setting is set. The flapping of an EBGP route can cause the flooding of UPDATE and WITHDRAWN messages. The EBGP advertisement-interval setting determines the frequency of EBGP updates regardless of changes to advertised EBGP routes.

The **no neighbor advertisement-interval** command resets the BGP advertisement-interval to the default value of **30** seconds.

Example

The following example sets the BGP advertisement interval for neighbor 9.1.2.1 to 35 seconds:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->neighbor 9.1.2.1 advertisement-interval 35
S Chassis(su-config-bgp)->
```

neighbor advertise-map

This command provides for conditional advertisement of routes for this neighbor.

Syntax

neighbor {*ip-address* | *groupID*} **advertise-map** *adv-map* **non-exist-map** *non-exit-map*

no neighbor {*ip-address* | *groupID*} **advertise-map** *adv-map* **non-exist-map** *non-exit-map*

Parameters

ip-address	Specifies a BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.
groupID	Specifies a BGP peer group name as a character string. If an invalid IP address is specified (for example, 256.1.1.1), it will be read as a group name.

adv-map	Specifies the BGP route-map containing the prefix to be added to the RIB for this neighbor, only if there is no route in the local RIB that matches a route in the non-exist-map.
non-exist-map	Specifies the BGP route-map containing the prefix that if not found in the local RIB will cause the prefix in the advertise map to be advertised.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **neighbor advertise-map** command provides for conditional advertisement of routes for this neighbor using advertise-map and non-exist-map route-maps. Configure prefix-list match clauses in the non-exist-map route-map with prefixes that should exist and be advertised to the peer under normal operational conditions. Should any prefix in the non-exist-map route-map fail (no longer exist), then the router will start advertising the prefixes in the advertise-map route-map, which are alternate routes to the preferred routes in the non-exist-map route-map.

Prefix-lists are assigned to route-maps associated with this command using "route-map bgp" on page 85-31.

The **no neighbor advertise-map** command deletes the conditional advertisement configuration for the specified neighbor.

Example

The following example:

- Configures an advertise-map prefix-list named **adv-list1** and assigns it to BGP route-map **adv-map1**, specifying prefix **155.25.1.0/24** as the prefix to be advertised if the prefix in the non-exist-map route-map is not available
- Configures a non-exist-map prefix-list named **non-exist-list1** and assigns it to BGP route-map **non-exist-map1**, specifying prefix **200.51.1.0/24** as the advertised prefix, unless it is not available (does not exist)
- Configures a BGP advertise-map for neighbor **9.1.2.1** that assigns **adv-map1** as the advertise map route-map and **non-exist-map1** as the non-exist-map route-map

```
S Chassis(su-config)->ip prefix-list adv-list1 permit seq 1 155.25.1.0/24
S Chassis(su-config)->route-map bgp adv-map1
S Chassis(su-config-route-map-bgp)->match adv-list1 adv-map1
S Chassis(su-config-route-map-bgp)->exit
S Chassis(su-config)->ip prefix-list non-exist-list1 permit seq 1 200.51.1.0/24
S Chassis(su-config)->route-map bgp non-exist-map1
S Chassis(su-config-route-map-bgp)->match non-exist-list1 non-exist-map1
S Chassis(su-config-route-map-bgp)->exit
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->neighbor 9.1.2.1 advertise-map adv-map1 non-exist-map
non-exist-map1
S Chassis(su-config-bgp)->
```

neighbor activate

This command activates the specified BGP peer for the current address family context.

Syntax

neighbor *ip-address* **activate**

no neighbor *ip-address* **activate**

Parameters

ip-address	Specifies a BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.

Defaults

None.

Mode

BGP Address Family Configuration.

Usage

The **neighbor activate** command must be applied to any IPv6 peers, but does not need to be applied to an IPv4 peer.

The **no neighbor activate** command disables activation of the specified BGP neighbor for the current address family context.

Example

The following example activates neighbor **fe80:0:0:0:21f:45ff:fe3d:21** within the IPv6 unicast address family context:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->neighbor fe80:0:0:0:21f:45ff:fe3d:21be remote-as 5
S Chassis(su-config-bgp)->address-family ipv6 unicast
S Chassis(su-config-bgp-af)->neighbor fe80:0:0:0:21f:45ff:fe3d:21be activate
```

neighbor aggregate-confed

This command enables the inclusion of confederation information in the AS paths sent to this router's peers.

Syntax

neighbor {*ip-address* | *groupID*} **aggregate-confed**

no neighbor {*ip-address* | *groupID*} **aggregate-confed**

Parameters

ip-address	Specifies a BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.

groupID	Specifies a BGP peer group name as a character string. If an invalid IP address is specified (for example, 256.1.1.1), it will be read as a group name.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The inclusion of confederation information in the AS paths sent to this router's peers is enabled by default.

The **no neighbor aggregate-confed** command disables the inclusion of confederation information in the AS paths sent to this router's peers.

Example

The following example disables the inclusion of confederation information in the AS paths sent to the specified peer for this router:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->no neighbor 200.51.1.1 aggregate-confed
S Chassis(su-config-bgp)->
```

neighbor as-origination-interval

This command sets the interval between successive update messages for route prefixes that originate in the local AS.

Syntax

neighbor *ip-address* **as-origination-interval** *interval*

no neighbor *ip-address* **as-origination-interval**

Parameters

ip-address	Specifies a BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.
interval	Specifies the interval in seconds between successive update messages for route prefixes that originate in the local AS. Valid values are **1** - **65535** seconds. The default value is **15** seconds.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **no neighbor as-origination-interval** command resets the as-origination-interval to the default value of **15** seconds.

Example

The following example sets the BGP as-origination-interval for neighbor 9.1.2.1 to 18 seconds:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->neighbor 9.1.2.1 as-origination-interval 18
S Chassis(su-config-bgp)->
```

neighbor check-next-hop

This command enables checking to see if the next hop is the peer's address and does not send routes if it is.

Syntax

neighbor *ip-address* **check-next-hop**

no neighbor *ip-address* **check-next-hop**

Parameters

ip-address	Specifies a BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.

Defaults

None.

Mode

BGP Router Configuration.

Usage

Checking to see whether the next hop is the peer's address is enabled by default.

The **no neighbor check-next-hop** command disables checking to see whether the next hop is the peer's address.

Example

The following example disables checking to see whether the next hop for neighbor 200.51.1.1 is the peer's address:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->no neighbor 200.51.1.1 check-next-hop
S Chassis(su-config-bgp)->
```

neighbor clear-counters

This command clears all BGP counters for this peer.

Syntax

neighbor *ip-address* **clear-counters**

Parameters

ip-address	Specifies a BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.

Defaults

None.

Mode

BGP Router Configuration.

Example

The following example clears all the counters on neighbor 200.51.1.1:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->neighbor 200.51.1.1 clear-counters
S Chassis(su-config-bgp)->
```

neighbor confed-member

This command configures the specified neighbor as a member of the router's confederation.

Syntax

neighbor *ip-address* **confed-member**

Parameters

ip-address	Specifies a BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.

Defaults

None.

Mode

BGP Router Configuration.

Usage

By default, a neighbor is not a member of the router’s confederation.

The **no neighbor confed-member** command removes this neighbor as a member of the router’s confederation.

Example

The following example configures neighbor 200.51.1.1 as a member of this router's confederation:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->bgp confederation-id 100
S Chassis(su-config-bgp)->neighbor 200.51.1.1 confed-member
S Chassis(su-config-bgp)->
```

neighbor connect-retry-interval

This command sets the amount of time between attempts to reestablish a connection to configured peers that are currently no longer available.

Syntax

neighbor *ip-address* **connect-retry-interval** *interval*

no neighbor *ip-address* **connect-retry-interval** *interval*

Parameters

ip-address	Specifies a BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.
interval	Specifies the interval in seconds between attempts to reestablish a connection to configured peers that are no longer available. Valid values are **1** - **65535** seconds. The default value is **120** seconds.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **no neighbor connect-retry-interval** command resets the BGP connect-retry-interval to the default value of **120** seconds.

Example

The following example sets the BGP connect-retry-interval for neighbor 9.1.2.1 to 125 seconds:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->neighbor 9.1.2.1 connect-retry-interval 125
S Chassis(su-config-bgp)->
```

neighbor default-originate

This command to advertise the default route regardless of whether the default route is present in the local routing table.

Syntax

neighbor *ip-address* **default-originate** [**route-map** *name*]

no neighbor *ip-address* **default-originate** [**route-map** *name*]

Parameters

ip-address	Specifies a BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.
route-map *name*	Specifies a route-map containing routes that, at least one of which, must be present for the default route to be advertised.

Defaults

None.

Mode

BGP Router Configuration, BGP IPV6/Unicast address-family, BGP IPV4/Multicast address-family, or BGP IPV6/Multicast address-family mode.

Usage

With a redistribute static command that is referencing a route-map in the bgp config a **network 0.0.0.0/0** command will not result in the default route being advertised. The **neighbor default-originate** command causes the BGP peer to advertise the default route under the current address-family regardless of whether the default route is present in the local router's routing table.

Using the route-map option results BGP advertising the default route if at least one prefix, matching the route-map match criteria, is present in the BGP RIB under the current address-family. While other matching criteria are possible, the most common use of the route-map for this application is with a prefix-list.

This command will not apply a default route within an L3VPN configuration context.

The **no neighbor default-originate** command removes the default-originate configuration for this neighbor.

Example

The following example configures BGP to advertise the default route if at least one prefix matching the match criteria present in **map1** is present in the BGP RIB:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 192.1.1.9
S Chassis(su-config-bgp)->neighbor 192.168.12.112 default-originate route-map
map1
S Chassis(su-config-bgp)->
```

neighbor enable

This command enables a BGP peer.

Syntax

neighbor *ip-address* **enable**

no neighbor *ip-address* **enable**

Parameters

ip-address	A BGP peer specified as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.

Defaults

None.

Mode

BGP Router Configuration.

Usage

A configured BGP peer is enabled by default. Use this command to administratively enable or disable a peer. The **neighbor enable** command explicitly enables a BGP peer that has been administratively disabled.

The **no neighbor enable** command explicitly disables a peering session. Configuration is retained when disabling a peering session using the **no neighbor enable** command.

Example

The following example enables BGP for peer **125.50.25.5**:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->neighbor 125.50.25.5 enable
```

neighbor idle-hold-interval

This command sets the interval between returning to the idle state and reinitiating a TCP connection for this neighbor.

Syntax

neighbor *ip-address* **idle-hold-interval** *interval*

no neighbor *ip-address* **idle-hold-interval** *interval*

Parameters

ip-address	Specifies a BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.
interval	Specifies the interval in seconds between returning to the idle state and reinitiating a TCP connection. Valid values are **1** - **32767** seconds. The default value is **15** seconds.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **no neighbor idle-hold-interval** command resets the BGP idle-hold-interval to the default value of **15** seconds.

Example

The following example sets the BGP connect-retry-interval for neighbor 9.1.2.1 to 25 seconds:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->neighbor 9.1.2.1 idle-hold-interval 25
S Chassis(su-config-bgp)->
```

neighbor ignore-leading-as

This command configures EBGP peer routes to not contain the specified neighbor's AS.

Syntax

neighbor *ip-address* **ignore-leading-as**

no neighbor *ip-address* **ignore-leading-as**

Parameters

ip-address	Specifies a BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.

Usage

Some routers are capable of propagating routes without appending their own autonomous system number to the AS Path. By default, the S-Series Router will drop such routes. The **neighbor ignore-leading-as** command allows the S-Series Router to keep these routes for EBGP peers. This capability may be needed if the peer has policy that prevents it from pre-pending its own AS number to the AS path.

The **no neighbor ignore-leading-as** command resets this command to the default value of disabled.

Defaults

None.

Mode

BGP Router Configuration.

Example

The following example enables the ignore-leading-as feature:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->neighbor 1.1.1.1 remote-as 5
S Chassis(su-config-bgp)->neighbor 1.1.1.1 ignore-leading-as
```

neighbor maximum-orf

This command sets the maximum number of Outbound Route Filtering (ORF) entries that will be accepted from this neighbor.

Syntax

neighbor *ip-address* **maximum-orf** *num*

no neighbor *ip-address* **maximum-orf** *num*

Parameters

ip-address	Specifies a BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.
num	Specifies the maximum number of ORF entries that will be accepted from this neighbor. Valid values are **1** - **4294967295** entries. The default value is **100000** entries.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The connection will be closed if the configured maximum number of ORF entries is exceeded.

The **no neighbor maximum-orf** command resets the maximum number of ORF entries that will be accepted from this neighbor to the default value of 100k entries.

Example

The following example sets the maximum number of ORF entries that will be accepted from neighbor 9.1.2.1 to 125k:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->neighbor 9.1.2.1 maximum-orf 125000
S Chassis(su-config-bgp)->
```

neighbor maximum-prefix

This command specifies the peak number of prefixes that BGP will accept for installation into the Routing Information Base (RIB).

Syntax

neighbor *ip-address* **maximum-prefix** *num* [**warning-only**]

no neighbor *ip-address* **maximum-prefix** *num* [**warning-only**]

Parameters

ip-address	Specifies a BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.
num	Specifies the maximum number of prefixes that will be installed in the BGP RIB. Valid values are **0** - **4294967295**. Default value is **0** (unlimited).
warning-only	(Optional) Specifies to log a warning message, stop accepting routes, and keep the established peering session.

Defaults

If **warning-only** is not specified, the default action is for the connection to be dropped, if the number of routes installed in the RIB exceeds the maximum allowed.

Mode

BGP Router Configuration.

Usage

The **neighbor maximum-prefix** command configures the maximum number of routes that a peer will accept for installation into the S-Series router BGP RIB. In addition, an action can be configured to occur when this maximum number is exceeded. If **warning-only** is specified, a warning message is logged and additional routes are no longer accepted, but the established peer session is kept. If **warning-only** is not specified, the default action is for the connection to be dropped.

The **no neighbor maximum-prefix** command removes the configured route limit and returns this setting to its default value of unlimited.

Example

The following example causes the S-Series Router to install a maximum of 1000 routes learned from peer 4.3.2.1 into the routing table. If this number is exceeded, then the S-Series Router will log a warning message and stop accepting additional routes.

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->neighbor 4.3.2.1 remote-as 5
S Chassis(su-config-bgp)->neighbor 4.3.2.1 maximum-routes 1000 warning-only
```

neighbor next-hop-peer

This command configures BGP to always set the BGP next hop to the EBGP peer's address, overriding third-party next hops.

Syntax

neighbor {*ip-address* | *groupID*} **next-hop-peer**

no neighbor {*ip-address* | *groupID*} **next-hop-peer**

Parameters

ip-address	Specifies a BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.
groupID	Specifies a BGP peer group.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The next hop of routes received from the EBGP peer is set to the peer's address.

Next-hop-peer behavior is **disabled** by default.

Every prefix that is advertised in BGP contains next hop information. The **no neighbor next-hop-peer** command resets this neighbor's next hop selection to the default next hop behavior of leaving the next hop information for this prefix unchanged.

Example

The following example configures neighbor 200.51.1.1 to set the BGP next hop to the EBGP peer's address:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->neighbor 200.51.1.1 next-hop-peer
S Chassis(su-config-bgp)->
```

neighbor next-hop-self

This command sets this neighbor's next hop as the router's own address on advertisement.

Syntax

neighbor {*ip-address* | *groupID*} **next-hop-self**

no neighbor {*ip-address* | *groupID*} **next-hop-self**

Parameters

ip-address	A BGP peer specified as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.

groupID	A BGP peer group name specified as a string of characters. If an invalid IP address is specified (for example, 256.1.1.1), it will be read as a group name.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **neighbor next-hop-self** command sets the specified peer's nexthop to the router's own address. When routes are learned using EBGP and advertised to an IBGP neighbor, this command sets the next hop information to the IP address of the interface used to communicate with the IBGP neighbor.

Example

The following example specifies that the neighbor will use the router's own address as the next hop.

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->neighbor 1.2.3.4 remote-as 5
S Chassis(su-config-bgp)->neighbor 1.2.3.4 next-hop-self
```

neighbor open-delay

This command sets the interval between the establishment of a TCP connection and the sending of an OPEN message to open a BGP session.

Syntax

neighbor *ip-address* **open-delay** *seconds*

no neighbor *ip-address* **open-delay** *seconds*

Parameters

ip-address	Specifies a BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.
seconds	Specifies the interval, in seconds, between the establishment of a TCP connection and the sending of an OPEN message to open a BGP session. Valid values are **0** - **240** seconds. The default value is **0** seconds (no delay).

Defaults

None.

Mode

BGP Router Configuration.

Usage

The BGP OPEN message is used to open a BGP session, and is sent after the TCP handshake is completed. The delay set by this command allows the remote BGP peer time to send the first OPEN message.

Use the **no neighbor open-delay** command to reset the delay between the TCP handshake completion and the sending of the BGP OPEN message to the default value of **0** seconds (no delay).

Example

The following example sets the delay between TCP handshake completion and the sending of the OPEN message to 3 seconds:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->neighbor 9.1.2.1 open-delay 3
S Chassis(su-config-bgp)->
```

neighbor passive

This command prevents the router from ever trying to open a BGP connection with the specified peer.

Syntax

neighbor *ip-address* **passive**

no neighbor *ip-address* **passive**

Parameters

ip-address	Specifies the BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format .

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **neighbor passive** command prevents the S-Series router from trying to initiate a BGP connection with the specified peer. Instead, the router will wait for the peer to initiate a connection.

This command was introduced to handle a problem in BGP3 and earlier, in which two peers might both attempt to initiate a connection at the same time. This problem has been corrected in the BGP4 protocol, and, thus, this command is not needed with BGP 4 sessions.

Note: If the **neighbor passive** command is applied to both sides of a peering session, the session will never be established. For this reason, and because it is generally not needed for a BGP 4 session, the use of **neighbor passive** is discouraged.

Example

In the following example, BGP will never initiate a connection with peer **1.2.3.4**:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->neighbor 1.2.3.4 remote-as 5
S Chassis(su-config-bgp)->neighbor 1.2.3.4 passive
```

neighbor peer-group

This command creates a BGP peer group and adds a peer group neighbor.

Syntax

neighbor *groupID* **peer-group**

no neighbor *groupID* **peer-group**

neighbor *ip-address* **peer-group** *groupID*

no neighbor *ip-address* **peer-group** *groupID*

Parameters

ip-address	An IPv4 or IPv6 address to add to a peer group. IPv4 addresses are specified in dotted-quad format; IPv6 addresses are specified in colon-separated format.
groupID	Specifies a BGP peer group name as a character string. If an invalid IP address is specified (for example, 256.1.1.1), it will be read as a group name.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **neighbor** *groupID* **peer-group** command creates a peer group. BGP peers can then be added to that group. After this command is issued, peers are added to the group using the **neighbor** *ip-address* **peer-group** command. All members of the peer group must be of the same peer type: IBGP, EBGP or EBGP confederation.

Peer group commands are policy related. If a peer is in a peer group, and both the peer and peer group have policy configured, the peer group's policy takes precedence for route export. The peer's policy takes precedence for route import.

Example

The following example configures peer group **abc** with peers **1.2.3.4** and **4.3.2.1** added to it.

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 1.1.1.1
S Chassis(su-config-bgp)->neighbor 1.2.3.4 remote-as 65151
S Chassis(su-config-bgp)->neighbor 4.3.2.1 remote-as 65151
S Chassis(su-config-bgp)->neighbor abc peer-group
```

```
S Chassis(su-config-bgp)->neighbor 1.2.3.4 peer group abc
S Chassis(su-config-bgp)->neighbor 4.3.2.1 peer-group abc
```

neighbor peer-type

This command specifies the peer type of the peer group.

Syntax

neighbor {*ip-prefix/length* | *groupID*} **peer-type** {**ibgp** | **ebgp** | **ebgp-confed**}

no neighbor {*ip-prefix/length* | *groupID*} **peer-type** {**ibgp** | **ebgp** | **ebgp-confed**}

Parameters

ip-prefix/length	An IPv4 or IPv6 prefix and length.
groupID	Specifies a BGP peer group name as a string of characters. If an invalid IP address is specified (for example, 256.1.1.1), it will be read as a group name.
ibgp	Specifies a peer group peer type as internal BGP.
ebgp	Specifies a peer group peer type as external BGP.
ebgp-confed	Specifies a peer group peer type as an external BGP confederation.

Defaults

None.

Mode

BGP Router Configuration.

Usage

This command applies to peer groups. The default peer type is IBGP.

The **no neighbor peer-type** command resets the peer type to the default value of IBGP for this neighbor.

Example

The following example configures the peer type for neighbors in prefix 10.10.25.1/24 as EBGP:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->neighbor 10.10.25.1/24 peer-type ebgp
S Chassis(su-config-bgp)->
```

neighbor peering-type

This command specifies whether updates for prefixes containing the NOPEER community will be accepted by or sent to this neighbor.

Syntax

neighbor {*ip-address* | *groupID*} **peering-type** {**bilateral** | **unspecified**}

no neighbor {*ip-address* | *groupID*} **peering-type** {**bilateral** | **unspecified**}

Parameters

ip-address	An IPv4 or IPv6 address to add to a peer group. IPv4 addresses are specified in dotted-quad format; IPv6 addresses are specified in colon-separated format.
groupID	Specifies a BGP peer group name as a string of characters. If an invalid IP address is specified (for example, 256.1.1.1), it will be read as a group name.
bilateral	Specifies that for prefixes containing the NOPEER community attribute updates are not accepted or sent.
unspecified	Specifies that updates are accepted or sent for prefixes regardless of whether the prefix contains the NOPEER community attribute. The default value for peering type is **unspecified**.

Defaults

None.

Mode

BGP Router Configuration.

Usage

If the peering type is set to bilateral, EBGP peers will not accept or advertise routes containing the NOPEER community attribute as defined in RFC 3765.

The **neighbor peering-type** command provides for defining the peering type as either bilateral or unspecified for the NOPEER community attribute. If the peering type is specified as **bilateral**, updates for this neighbor are not accepted or sent when the community attribute is NOPEER. If the peering type is specified as **unspecified**, updates for this neighbor are accepted and sent when the community attribute is NOPEER.

The **no neighbor peering-type** command resets the peering type to the default value of **unspecified** for this neighbor.

Example

The following example configures the peering type for neighbor 10.10.25.1 as bilateral:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->neighbor 10.10.25.1 peering-type bilateral
S Chassis(su-config-bgp)->
```

neighbor remote-as

This command configures the remote AS for the specified peer.

Syntax

neighbor *ip-address* **remote-as** *as-num* [**password** *password*]

no neighbor *ip-address* **remote-as** *as-num* [**password** *password*]

Parameters

ip-address	Specifies a BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.
as-num	Specifies the autonomous system (AS) number of the specified BGP peer. Valid values are **1** - **4294967295**.
password *password*	(Optional) Specifies an MD5 password for this peer. Valid values are up to 128 characters.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **neighbor remote-as** command configures the AS of the specified peer.

The **no neighbor remote-as** command removes the AS configuration for the specified peer.

Example

This example configures a BGP peer 1.2.3.4 with an AS number of 5:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->neighbor 1.2.3.4 remote-as 5
```

The following example configures a IPv6 BGP peer address with an AS number of 64600:

```
router(config)->router bgp 65000
router(config-router-bgp)->bgp router-id 159.1.1.9
router(config-router-bgp)->neighbor 2001:0DB8:0:CC00::1 remote-as 64600
```

neighbor remove-private-as

This command specifies whether or not to remove private autonomous system (AS) numbers from outbound updates to an external peer.

Syntax

neighbor {*ip-address* | *groupID*} **remove-private-as**

no neighbor {*ip-address* | *groupID*} **remove-private-as**

Parameters

ip-address	Specifies a BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.
groupID	Specifies a BGP peer group name as a string of characters. If an invalid IP address is specified (for example, 256.1.1.1), it will be read as a group name.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **neighbor remove-private-as** command removes private AS numbers when sending updates to an external peer. When enabled, private AS numbers are removed on outbound updates from any received routes with an AS-path containing private AS numbers.

Example

The following example causes BGP to strip private AS numbers from updates to this peer:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 1.1.1.1
S Chassis(su-config-bgp)->neighbor 1.2.3.4 remote-as 5
S Chassis(su-config-bgp)->neighbor 1.2.3.4 remove-private-as
```

The following example causes BGP to no longer remove private AS numbers:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->no neighbor 1.2.3.4 remove-private-as
```

neighbor route-map

This command specifies a BGP route-map to be used for controlling the import or export of routes to and from the specified peer or group.

Syntax

neighbor {*ip-address* | *groupID*} **route-map** *rm-name* {**in** | **out**}

no neighbor {*ip-address* | *groupID*} **route-map** *rm-name* {**in** | **out**}

Parameters

ip-address	A BGP peer specified as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.
groupID	A BGP peer group name specified as a string of characters. If an invalid IP address is specified (for example, 256.1.1.1), it will be read as a group name.
rm-name	The name of a configured BGP route-map.
in | **out**	Specify whether the route-map should be applied to routes being learned from (**in**) or sent to (**out**) BGP.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **neighbor route-map** command is used to filter routes between BGP peers. Apply the route-map to the redistribute command for the appropriate protocol to filter route redistribution between protocols.

The **neighbor route-map** command specifies a configured route-map to be exported into or out of BGP.

Example

In the following example, the configured route-map **abc** is specified to filter routes exported into BGP:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 1.1.1.1
S Chassis(su-config-bgp)->neighbor 1.2.3.4 remote-as 5
S Chassis(su-config-bgp)->neighbor 1.2.3.4 route-map abc in
```

neighbor route-reflector-client

This command specifies that the router will act as a route reflector for the specified neighbor.

Syntax

neighbor *ip-address* **route-reflector-client**

no neighbor *ip-address* **route-reflector-client**

Parameters

ip-address	A BGP peer specified as a valid IPv4 address in dotted-quad.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **neighbor route-reflector-client** command specifies that the S-Series router will act as a route reflector for this peer.

The **no neighbor route-reflector-client** command removes the specified client from its route reflection group.

Example

The following example configures the neighbor 1.2.3.4 as a route reflector client:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 1.1.1.1
```

```
S Chassis(su-config-bgp)->neighbor 1.2.3.4 remote-as 5
S Chassis(su-config-bgp)->neighbor 1.2.3.4 route-reflector-client
```

neighbor route-withdraw-interval

This command sets the interval between the advertisement and subsequent withdrawal of a route for the specified peer.

Syntax

neighbor *ip-address* **route-withdraw-interval** *interval*

no neighbor *ip-address* **route-withdraw-interval** *interval*

Parameters

ip-address	An IPv4 or IPv6 address specified in dotted-quad format; IPv6 addresses are specified in colon-separated format.
interval	Specifies the amount of time in seconds between the advertisement and subsequent withdrawal of a route from the RIB. Valid values are **0** - **65535** seconds. Default value is **30** seconds.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **no neighbor route-withdraw-interval** resets the route withdrawal interval setting to the default value of 30 seconds.

Example

The following example sets the route withdrawal interval for neighbor 10.10.25.1 to 35 seconds:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->neighbor 10.10.25.1 route-withdraw-interval 35
S Chassis(su-config-bgp)->
```

neighbor soft-reconfiguration

This command enables or disables soft-reconfiguration for a peer or peer group.

Syntax

neighbor {*ip-address* | *groupID*} **soft-reconfiguration**

no neighbor {*ip-address* | *groupID*} **soft-reconfiguration**

Parameters

ip-address	A BGP peer specified as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.
groupID	A BGP peer group name specified as a character string. If an invalid IP address is specified (for example, 256.1.1.1), it will be read as a group name.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The soft reconfiguration capability keeps a local copy of the routes for the specified peer or group. If there is an inbound policy change, the new policy can be reapplied to determine which routes are accepted. The soft reconfiguration capability speeds up the route installation process when a policy change occurs. Soft reconfiguration increases memory usage on the router.

The **no neighbor soft-reconfiguration** command resets the route refresh capability to the default value of **disabled**.

Example

The following example turns on the route refresh capability for peer **10.10.25.1**:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 159.1.1.9
S Chassis(su-config-bgp)->neighbor 10.10.25.1 remote-as 5
S Chassis(su-config-bgp)->neighbor 10.10.25.1 soft-reconfiguration
```

neighbor timers

This command specifies holdtime and keepalive time values for a BGP peer.

Syntax

neighbor *ip-address* **timers** *keepalive-value holdtime-value*

no neighbor *ip-address* **timers** *keepalive-value holdtime-value*

Parameters

ip-address	Specifies a BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.
keepalive-value	Specifies the interval between keepalive messages. Valid values are **0** - **65535** seconds. Default value is **30** seconds.
holdtime-value	Specifies the interval of the BGP hold-timer. Valid values are **0** - **21845** seconds. The Default value is **90** seconds.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The keepalive value specifies the number of seconds that will elapse between keepalive messages. The hold time value specifies the number of seconds to use when negotiating a peering session within this group. If the S-Series router does not receive a keepalive, update, or notification message within the specified period, then the BGP connection will be closed.

The BGP keepalive timer will be set to one-third of the negotiated holdtime by default. If the administrative keepalive time is set to greater than one-third of the hold time, the router will default to one-third of the negotiated hold time.

The negotiated holdtime value is the lesser of the values sent in the exchanged BGP OPEN messages. If a holdtime of zero is specified, no keepalives will be sent. If a holdtime of zero is received from the remote peer, then the holdtime must be configured to be zero in order for the peering session to become established.

Note: You cannot specify a holdtime value of 1 or 2. Attempting to do so will result in an error.

The **no neighbor timers** command removes the configured values and returns this to its default values of 30 seconds for keepalive and 90 seconds for hold time.

Example

This example sets keepalive and holdtime values of 40 and 120 seconds, respectively, for this peer:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 1.1.1.1
S Chassis(su-config-bgp)->neighbor 1.2.3.4 remote-as 5
S Chassis(su-config-bgp)->neighbor 1.2.3.4 timers 40 120
```

neighbor ttl

This command specifies time to live (TTL) value.

Syntax

neighbor *ip-address* **ttl** *ttl-num*

no neighbor *ip-address* **ttl** *ttl-num*

Parameters

ip-address	Specifies a BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.
ttl-num	Specifies the number of hops configured for this neighbors TTL setting. Valid values are 1 - 255. Default value is 0 (Set by the IP stack to **64** hops).

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **no neighbor ttl** command resets the TTL value for this neighbor to the default of **0** (Set by the IP stack to **64**).

Example

The following example configures a TTL value of 5 for this peer.

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 1.1.1.1
S Chassis(su-config-bgp)->neighbor 1.2.3.4 remote-as 5
S Chassis(su-config-bgp)->neighbor 1.2.3.4 ttl 5
```

neighbor update-source

This command specifies the source IP address to be used in all TCP and BGP messages sent to the peer.

Syntax

neighbor *ip-address* **update-source** *source-addr*

no neighbor *ip-address* **update-source** *source-addr*

Parameters

ip-address	Specifies a BGP peer as a valid IPv4 address in dotted-quad format or as a valid IPv6 address in colon-separated format.
source-addr	The local IP interface address.

Defaults

None.

Mode

BGP Router Configuration.

Usage

The **neighbor update-source** command is typically used when peering between IBGP routers that are not directly connected and an alternative route is available or when using virtual interfaces as the peer address. In order to accept a connection, IBGP requires that the source IP address of the received OPEN message match the configured IP address of the peer. By default the source IP address is set to the IP address of the outgoing interface to reach the peer. In the case of a failed direct link, if the peer address is the address of the outgoing interface, peering will not establish.

The **no neighbor update-source** command resets the update source address to the default value of a shared interface address.

Example

The following example causes the TCP session to peer 1.2.3.4 to be established over the interface 4.3.2.1:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->bgp router-id 1.1.1.1
S Chassis(su-config-bgp)->neighbor 1.2.3.4 remote-as 5
S Chassis(su-config-bgp)->neighbor 1.2.3.4 update-source 4.3.2.1
```

The following example causes the TCP session to be established over the outgoing interface to the peer:

```
S Chassis(su-config)->router bgp 65151
S Chassis(su-config-bgp)->no neighbor 1.2.3.4 update-source 4.3.2.1
```

Route Flap Damping Commands

The route flap damping capability treats routes that are being announced and withdrawn (flapping) at a rapid rate as unreachable. If a route flaps at a low rate, it should not be suppressed at all, or suppressed for only a brief period of time. With route flap damping, the suppression of a route or routes occurs in a manner that adapts to the frequency and duration that a particular route appears to be flapping. The more a route flaps during a period of time, the longer it will be suppressed.

Each time a route flap occurs, a penalty of 100 is added to the route. When a route penalty exceeds the suppression threshold, the route is suppressed. The route penalty value decays over time. The half life of a route penalty is configurable for both reachable and unreachable routes. When the penalty falls below the reuse threshold, route dampening no longer suppresses the route. A hold-time value allows for the setting of a maximum time route dampening suppresses a route, regardless of its current route penalty. The amount of time a route flap is kept in memory is also configurable for both reachable and unreachable routes.

BGP route flap damping is defined in RFC 2439, *BGP Route Flap Damping.*

For information about...	Refer to page...
dampen-flap	72-62
cutoff	72-63
half-life-reach	72-64
half-life-unreach	72-64
hold-time	72-65
memory-limit-reach	72-66
memory-limit-unreach	72-67
reuse	72-67

dampen-flap

Use this command to enter the dampen flap command mode for the named dampen flap table.

Syntax

dampen-flap *name*

no dampen-flap *name*

Parameters

name	Specifies the name of the dampen flap table to configure.

Defaults

None.

Mode

Global Configuration.

Usage

The **dampen-flap** command enters the dampen flap table command mode for the named dampen flap table. Route flap damping parameters are configured within the dampen flap command mode.

The "no" form of this command removes the specified dampen flap table.

Example

The following example enters route flap damping command mode for table **rfd1**.

```
S Chassis(su-config)-> dampen-flap rfd1
S Chassis(su-config-dampen-flap)->
```

cutoff

This command specifies the route suppression threshold.

Syntax

cutoff *threshold*

no cut-off

Parameters

threshold	Specifies the route penalty value above which the route is suppressed. Valid values are **1** - **10000**. Default value is **125**.

Defaults

None.

Mode

Dampen Flap Configuration.

Usage

Each route withdrawal adds 100 to the route penalty. For route dampening, the cutoff and reuse thresholds are compared against the route penalty for a particular route. So with the default cutoff threshold of 125, the route dampening suppresses the route after two withdrawals, and the route stays suppressed for approximately 10 minutes (calculated using the half life, an initial penalty of

200, and a reuse threshold of 50). After 15 minutes, should the route still be suppressed due to additional withdrawals, the route will be unsuppressed due to the hold-time setting of 15 minutes.

The "no" form of this command resets the cut-off threshold to its default value of **125**.

Example

The following example configures the cut-off value for the flap table **flap1** as **150**.

```
S Chassis(su-config)->dampen-flap flap1
S Chassis(su-config-dampen-flap)->cutoff 150
```

half-life-reach

This command specifies the time in seconds after which a reachable route's penalty value decays to half of its current value.

Syntax

half-life-reach *seconds*
no half-life-reach

Parameters

seconds	Specifies the number of seconds that will elapse before a reachable route's penalty value decays to half of its current value. Valid values are **0** to **3600** seconds. Default value is **300** seconds.

Defaults

None.

Mode

Dampen Flap Configuration.

Usage

The dampen penalty value assigned to a route decays over time. Use the **half-life-reach** command to specify a time in seconds, after which a reachable route's penalty value decays to half of its current value assuming the route remains stable and reachable.

The half life reach value must be less than the configured memory limit reach value configured using the "memory-limit-reach" on page 72-66 command.

The "no" form of this command resets the half life reach value to its default value of **300** seconds.

Example

The following example configures the half life reachable value to be 250 seconds.

```
S Chassis(su-config)->dampen-flap rfd1
S Chassis(su-config-dampen-flap)->half-life-reach 250
```

half-life-unreach

Use this command to specify the time in seconds after which an unreachable route's penalty value decays to half its current value.

Syntax

half-life-unreach *seconds*
no half-life-unreach

Parameters

seconds	Specifies the number of seconds after which an unreachable route's penalty value decays to half its current value. Valid values are **1** - **3600**. The default value is **900**.

Defaults

None.

Mode

Dampen Flap Configuration.

Usage

The dampen penalty value assigned to a route decays over time. Use the **half-life-unreach** command to specify a time in seconds, after which an unreachable route's penalty value decays to half of its current value, assuming the route remains stable and unreachable.

The half life unreach value must be less than the configured memory limit unreachable value configured using memory-limit-unreach on page 72-67.

The "no" form of this command resets the half life unreachable value to its default value of **900** seconds.

Example

The following example configures the half life unreach value to be 600 seconds.

```
S Chassis(su-config)->dampen-flap rfd1
S Chassis(su-config-dampen-flap)->half-life-unreach 600
```

hold-time

This command specifies the maximum time a route can be suppressed.

Syntax

hold-time *seconds*

no hold-time

Parameters

seconds	Specifies the maximum amount of time in seconds a route can be suppressed (held). Valid values are **1** - **3600**. The default value is **900** seconds.

Defaults

None.

Mode

Dampen Flap Configuration.

Usage

Use the **hold-time** command to specify the maximum duration in seconds that a route can be suppressed.

The “no” form of this command resets the hold-time to the default value of **900** seconds.

Example

The following example configures the hold-time to **1000** seconds:

```
S Chassis(su-config)->dampen-flap rfd1
S Chassis(su-config-dampen-flap)->hold-time 1000
```

memory-limit-reach

This command specifies the decay memory limit for reachable routes.

Syntax

memory-limit-reach *seconds*
no memory-limit-reach

Parameters

seconds	Specifies the number of seconds for the decay memory limit for reachable routes. Valid values are **1** - **3600** seconds. The default value is **900** seconds.

Defaults

None.

Mode

Dampen Flap Configuration.

Usage

The memory limit timers are used by route flap dampening for internal calculations. Half-life timers must be configured to a value less than the corresponding reachable or unreachable memory limit timer. The **memory-limit-reach** command specifies the maximum time in seconds any memory of a previous instability is retained, given the route state is both unchanged and reachable.

The “no” form of this command resets the memory limit reachable setting to the default value of **900** seconds.

Example

The following example configures the keep-history value to be **700** seconds.

```
S Chassis(su-config)->dampen-flap rfd1
S Chassis(su-config-dampen-flap)->memory-limit-reach 700
```

memory-limit-unreach

This command specifies the decay memory limit for unreachable routes.

Syntax

memory-limit-unreach *seconds*
no memory-limit-unreach

Parameters

time-seconds	Specifies the number of seconds for the decay memory limit for unreachable routes. Valid values are **0** - **3600**. The default value is **1800**.

Defaults

None.

Mode

Dampen Flap Configuration.

Usage

The memory limit timers are used by route flap dampening for internal calculations. Half-life timers must be configured to a value less than the corresponding reachable or unreachable memory limit timer. The **memory-limit-unreach** command specifies the maximum time in seconds any memory of a previous instability is retained, given the route state is both unchanged and unreachable.

The "no" form of this command resets the memory limit unreachable value to the default value of **1800**.

Example

The following example configures the keep-history value to be **1600** seconds.

```
S Chassis(su-config)->dampen-flap rfd1
S Chassis(su-config-dampen-flap)->keep-history 1600
```

reuse

Use this command to specify the route penalty value below which a suppressed route is reused.

Syntax

reuse *value*
no reuse

Parameters

value	Specifies the route penalty value below which a suppressed route is reused. Valid values are **1** - **10000**. The default value is **50**.

Defaults

None.

Mode

Dampen Flap Configuration.

Usage

The "no" form of this command resets the reuse value to the default value of **50**.

Example

The following example configures the reuse value to be 75.

```
S Chassis(su-config)->dampen-flap rfd1
S Chassis(su-config-dampen-flap)->reuse 75
```

Querying and Clearing Commands

For information about...	Refer to page...
clear ip bgp	72-68
clear ip bgp flap-all-stats	72-69
clear ip bgp flap-count	72-70
clear ip bgp topology	72-70
show ip bgp	72-71
show ip bgp dampened-routes	72-75
show ip bgp groups	72-76
show ip bgp neighbors	72-77
show ip bgp topology	72-78
show ip bgp summary	72-79
show ipv6 bgp	72-79
show ipv6 bgp neighbors	72-80
show ipv6 bgp summary	72-82

clear ip bgp

This command resets BGP peering sessions and optionally sends route refresh requests.

Syntax

clear ip bgp {*peer-address* [**soft**]| ***** [**soft**]}

Parameters

peer-address	Specifies the IP address of a single BGP peer to clear.
*****	Clears all sessions and peers for the router.
soft	(Optional) Specifies that BGP send a Route Refresh message (if supported by the peer).

Defaults

If the **soft** option is not specified, the connection is torn down and restarted with no Route Refresh message sent to the peer.

Mode

All command modes.

Usage

The **clear ip bgp** command resets BGP peering sessions or sends a Route Refresh request.

When the **soft** option is specified, a route refresh message is triggered and the peering session is not reset.

Example

The following example specifies to clear the BGP peer 1.2.3.4:

```
S Chassis(rw)->clear ip bgp 1.2.3.4
```

The following example clears all BGP peers and send a Route Refresh message.

```
S Chassis(rw)->clear ip bgp * soft
```

clear ip bgp flap-all-stats

This command clears all route flap statistics and state for the specified route prefix.

Syntax

clear ip bgp flap-all-stats *ip-prefix/length*

Parameters

ip-prefix/length	Specifies a route prefix to clear.

Defaults

None.

Mode

All command modes.

Usage

The **clear ip bgp flap-all-stats** command unsuppresses the route, if the route is suppressed when this command is issued.

Example

The following example specifies to clear all BGP route-flap statistics for prefix 3.0.0.0/8:

```
S Chassis(rw)->clear ip bgp flap-all-stats 1.2.3.4/24
S Chassis(rw)->show ip bgp 3.0.0.0/8 detail
Route status codes: > - active

   Network                Next Hop            Rib MED Local-Pref Origin AS Path
```

```
    3.0.0.0/8               192.168.12.111        U   0      100    Inc     10

Community attributes in route:

Extended Community attributes in route:

Route Flap Dampening configuration file name: flap1
Is route suppressed? Yes
Flap penalty: 0, Flap Count 0, Flap time remaining 0 seconds
```

clear ip bgp flap-count

This command clears the route-flap count for the specified route-prefix.

Syntax

clear ip bgp flap-count *ip-prefix/length*

Parameters

ip-prefix/length	Specifies a BGP prefix and length as a valid route.

Defaults

None.

Mode

All command modes.

Example

The following example clears the flap count statistic for route **3.0.0.0/8**:

```
S Chassis(su)->clear ip bgp 3.0.0.0/8
S Chassis(su)->show ip bgp 3.0.0.0/8 detail
Route status codes: > - active

    Network                Next Hop            Rib MED Local-Pref Origin AS Path
    3.0.0.0/8                192.168.12.111        U   0      100    Inc     10

Community attributes in route:

Extended Community attributes in route:

Route Flap Dampening configuration file name: flap1
Is route suppressed? Yes
Flap penalty: 185, Flap Count 0, Flap time remaining 295 seconds
```

clear ip bgp topology

This command resets BGP neighbor session information for a topology.

Syntax

clear ip bgp [topology {* | *topology-name*}]

Parameters

topology-name	Specifies the topology in which session information will be cleared. If * is used instead of *topology-name*, the command clears session and peering information for all topologies.

Defaults

None.

Mode

All command modes.

Usage

When the **topology** option is specified, session information is cleared only in the specified topology. Use the * instead of *topology-name* to clear session information in all topologies.

Example

The following example specifies to clear topology Router3:

```
S Chassis(rw)->clear ip bgp topology Router3
```

show ip bgp

This command displays information about BGP routes installed in the BGP routing information base (RIB).

Syntax

show ip bgp [*ip-address*] [*ip-prefix/mask*] [**longer-prefixes**] [**detail**] [**peer** *ip-addr* {**all-received-routes** | **received-routes** | **advertised-routes**}]

Parameters

ip-address	(Optional) Specifies an IPv4 address for BGP route display.
ip-prefix/mask	(Optional) Specifies an IP prefix and mask for BGP route display
longer-prefixes	(Optional) Specifies that only routes matching the specified IP address or IP prefix/length will display.
detail	(Optional) Displays a detailed level of information including: • Route community attributes • Route Extended Community attributes • Route Target • Route Flap Dampening table name • Flap related counters
peer *ip-addr*	(Optional) Specifies the peer to display route information for.
all-received-routes	Show all received routes for the specified peer.
received-routes	Show received routes from the peer *after* import policies are applied matching prefix and mask (local-rib)

advertised-routes	Show all routes advertised to the peer after export policies have been applied that match a prefix and mask (rib-out).

Defaults

- If a peer IP address, route, or the longer prefix option is not specified, information is displayed for all peers and routes.
- If **detail** is not specified, a standard level of route information displays.

Mode

All command modes.

Usage

To display BGP VPN routes see "show ip bgp vpn" on page 58-20.

Example

The following example returns BGP information for all BGP routes installed in the BGP RIB.

```
S Chassis(rw)->show ip bgp
show ip bgp
Route status codes: > - active

    Network                Next Hop            Rib MED Local-Pref Origin AS Path
>   7.1.1.0/24               192.168.7.112         U   0      100     IGP     7
>   7.1.2.0/24               192.168.7.112         U   0      100     IGP     7
>   7.1.3.0/24               192.168.7.112         U   0      100     IGP     7
>   7.1.4.0/24               192.168.7.112         U   0      100     IGP     7
>   7.1.5.0/24               192.168.7.112         U   0      100     IGP     7
>   7.1.6.0/24               192.168.7.112         U   0      100     IGP     7
>   7.1.7.0/24               192.168.7.112         U   0      100     IGP     7
>   7.1.8.0/24               192.168.7.112         U   0      100     IGP     7
>   7.1.9.0/24               192.168.7.112         U   0      100     IGP     7
>   7.1.10.0/24              192.168.7.112         U   0      100     IGP     7
>   7.1.11.0/24              192.168.7.112         U   0      100     IGP     7
>   7.1.12.0/24              192.168.7.112         U   0      100     IGP     7
>   7.1.13.0/24              192.168.7.112         U   0      100     IGP     7
...
S Chassis(rw)->
```

Table 72-1 table describes the fields that appear in the **show ip bgp** query.

Table 72-1 show ip bgp Output Details

Output...	What it displays...
Network	Specifies the network this route is on.
Next Hop	Specifies the IP address of the nearest gateway used to reach the EBGP peer

Table 72-1 show ip bgp Output Details

Output...	What it displays...
Rib	Specifies whether the route is installed in the unicast or multicast RIB
MED	Specifies the MED value for the route.
Local-Pref	Specifies the Local Preference value for the route.
Origin	Specifies whether the origin of the route is an internal or external protocol.
AS Path	Specifies the route's AS Path.

The following example display advertised routes for peer 192.168.7.112:

```
S Chassis(rw)->show ip bgp peer 192.168.7.112 advertised-routes
Route status codes: adv - advertised, sup - suppressed, pw - pending w/drawal, wd
- w/drawn
Route aggregation codes:
1 - Route is not aggregating or aggregated
2 - Route is aggregating
3 - Route is unsuppressed aggregated
4 - Route is suppressed aggregated

Stat Aggr   Network              Next Hop       Rib MED Local-Pref Origin AS Path
adv  1      8.1.1.0                192.168.7.111    U   0      0      IGP     10 8
adv  1      8.1.2.0                192.168.7.111    U   0      0      IGP     10 8
adv  1      8.1.3.0                192.168.7.111    U   0      0      IGP     10 8
adv  1      8.1.4.0                192.168.7.111    U   0      0      IGP     10 8
adv  1      8.1.5.0                192.168.7.111    U   0      0      IGP     10 8
adv  1      8.1.6.0                192.168.7.111    U   0      0      IGP     10 8
adv  1      8.1.7.0                192.168.7.111    U   0      0      IGP     10 8
adv  1      8.1.8.0                192.168.7.111    U   0      0      IGP     10 8
adv  1      8.1.9.0                192.168.7.111    U   0      0      IGP     10 8
adv  1      8.1.10.0               192.168.7.111    U   0      0      IGP     10 8
adv  1      8.1.11.0               192.168.7.111    U   0      0      IGP     10 8
adv  1      8.1.12.0               192.168.7.111    U   0      0      IGP     10 8
adv  1      8.1.13.0               192.168.7.111    U   0      0      IGP     10 8
adv  1      8.1.14.0               192.168.7.111    U   0      0      IGP     10 8
adv  1      8.1.15.0               192.168.7.111    U   0      0      IGP     10 8
...
S Chassis(rw)->
```

Table 72-2 describes the fields that appear in the **show ip bgp peer** query.

Table 72-2 show ip bgp peer Output Details

Output...	What it displays...
Stat	Specifies the status of the route as follows: • **adv** - advertised • **sup** - suppressed • **pw** - route pending withdrawal • **wd** - route withdrawn
Aggr	Specifies a route aggregation code as follows: • **1** - This route is neither aggregating nor aggregated • **2** - This route is aggregating • **3** - This route is an unsuppressed aggregate • **4** - This route is a suppressed aggregate
Network	Specifies the network this route is on.
Next Hop	Specifies the IP address of the nearest gateway used to reach the EBGP peer
Rib	Specifies whether the route is installed in the unicast or multicast RIB
MED	Specifies the MED value for the route.
Local-Pref	Specifies the Local Preference value for the route.
Origin	Specifies whether the origin of the route is an internal or external protocol.
AS Path	Specifies the route's AS Path.

The following example provides a detailed level of information for routes matching **7.1.1.0/24**:

```
S Chassis(rw)->show ip bgp 7.1.1.0/24 longer-prefixes detail
Route status codes: > - active

    Network                Next Hop            Rib MED Local-Pref Origin AS Path
>   7.1.1.0/24               192.168.7.112         U   0      100    IGP     7

Community attributes in route:
10:700

Extended Community attributes in route:
Route Target: 0:117506304 (0x0002000007010100)

Route Flap Dampening configuration file name: flap1
Is route suppressed? No
Flap penalty: 0, Flap Count 0, Flap time remaining 0 seconds

S Chassis(rw)->
```

show ip bgp dampened-routes

This command displays dampened routes information.

Syntax

```
show ip bgp dampened-routes
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

The following example shows detailed information about all dampened routes in the RIB.

```
S Chassis(su)->show ip bgp dampened-routes
Route status codes: > - active

   Network                Next Hop            Rib MED Local-Pref Origin AS Path
   62.68.32.0/19           1.254.0.1            U   0      100    IGP     65021
6363 2828 2914 15412 21003
   80.96.224.0/23          1.254.0.1            U   0      100    IGP     65021
6363 2828 3257 6663 20668
   81.180.90.0/23          1.254.0.1            U   0      100    IGP     65021
6363 2828 3257 6663 20668
   85.121.164.0/23         1.254.0.1            U   0      100    IGP     65021
6363 2828 3257 6663 20668 35020 35020
   86.105.32.0/20          1.254.0.1            U   0      100    IGP     65021
6363 2828 3257 6663 20668
   95.32.128.0/18          1.254.0.1            U   0      100    IGP     65021
6363 2828 8342 29651 44237 21017
   95.32.192.0/18          1.254.0.1            U   0      100    Inc     65021
6363 2828 8342 29651 44237 21017
   95.171.224.0/24         1.254.0.1            U   0      100    IGP     65021
6363 2828 3549 6854 29648 13105
S Chassis(su)->
```

Table 72-3 table describes the fields that appear in the **show ip bgp dampened-routes** query.

Table 72-3 show ip bgp dampened-routes Output Details

Output...	What it displays...
Network	Specifies the network this dampened route is on.
Next Hop	Specifies the IP address of the nearest gateway used to reach the EBGP peer for this dampened route.

Table 72-3 show ip bgp dampened-routes Output Details

Output...	What it displays...
Rib	Specifies whether the dampened route is installed in the unicast or multicast RIB
MED	Specifies the MED value for the dampened route.
Local-Pref	Specifies the Local Preference value for the dampened route.
Origin	Specifies whether the origin of the dampened route is an internal or external protocol.
AS Path	Specifies the dampened route's AS Path.

show ip bgp groups

This command displays information for BGP peer groups.

Syntax

```
show ip bgp groups
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

The following example shows detailed information about all BGP groups.

```
S Chassis(rw)->show ip bgp groups
BGP peer-group: PG1
  BGP version 4
  Address family IPv4 Unicast
  Peer-group type ebgp
  Peer-group members:
    66.77.122.2
BGP peer-group: PG2
  BGP version 4
  Address family IPv4 Unicast
  Peer-group type ibgp
  Peer-group members:
    192.17.170.16
    192.17.170.80
S Chassis(rw)->
```

show ip bgp neighbors

This command displays information about the state of BGP's IPv4 peering sessions.

Syntax

show ip bgp neighbors [*ip-address*]

Parameters

ip-address	(Optional) Specifies an IPv4 address to view data for only the specified neighbor.

Defaults

Is a peer IP address is not specified, information for all neighbors displays.

Mode

All command modes.

Usage

The **show ip bgp neighbors** query displays detailed data about the state of BGP's peering sessions. You can optionally specify an IPv4 address.

Example

The following example shows detailed information about all BGP peering sessions.

```
S Chassis(rw)->show ip bgp neighbors

BGP neighbor is: 192.168.7.112, remote AS: 7
BGP version is: 4, remote router ID: 113.58.0.1
TTL: 0
Hold Time: 90 (sec), Keepalive Time: 30 (sec)
Restart Time: 120 (sec), Restarting: No
Current state is: ESTABLISHED
Updates received: 6, Updates sent: 5
Total messages received: 206, Total messages sent: 715
Last error code was: 0
Last error sub-code was: 0
Local AS is: 10
Local router ID is: 1.2.3.4
Established Time is: 3184 (sec)
Number of transitions to/from established state is: 4
Soft reset with stored info is: Disabled
Automatic sending of route-refresh messages is: Enabled
Router confederation AS is: 0
Peer is in Router's Confederation? No
Route Reflector ID is: 0.0.0.0
Peer is Route Reflector Client? Non-Client
```

```
BGP neighbor is: 192.168.8.112, remote AS: 8
BGP version is: 4, remote router ID: 113.58.0.2
TTL: 0
Hold Time: 90 (sec), Keepalive Time: 30 (sec)
Restart Time: 120 (sec), Restarting: No
Current state is: ESTABLISHED
Updates received: 5, Updates sent: 24
Total messages received: 439, Total messages sent: 1005
Last error code was: 0
Last error sub-code was: 0
Local AS is: 10
Local router ID is: 1.2.3.4
Established Time is: 3179 (sec)
Number of transitions to/from established state is: 5
Soft reset with stored info is: Disabled
Automatic sending of route-refresh messages is: Enabled
Router confederation AS is: 0
Peer is in Router's Confederation? No
Route Reflector ID is: 0.0.0.0
Peer is Route Reflector Client? Non-Client
S Chassis(rw)->
```

show ip bgp topology

This command displays information for BGP topologies.

Syntax

show ip bgp topology {* | *topology-name*}

Parameters

*	Displays data for all topology instances.
topology-name	(Optional) Specifies a topology to be displayed, by name.

Defaults

All (*) is the default.

Mode

All command modes.

Example

The following example shows detailed information about all BGP topologies.

```
S Chassis(rw)->show ip bgp topology
S Chassis(rw)->
```

show ip bgp summary

This command displays a summary of the BGP configuration.

Syntax

show ip bgp summary

Parameters

None.

Defaults

None.

Mode

User execution

Usage

The **show ip bgp summary** command displays summarized BGP information, including the router ID and the local AS number.

Example

The following example shows a request for summarized BGP information.

```
S Chassis(rw)->show ip bgp summary
BGP router identifier 172.30.10.111, local AS number 10
Neighbor IP       Version       Remote-AS    State        In updates  Out updates  In Service?   Up/Down      last msg rcv
172.30.46.6          4             6         ESTABLISHED      32          31          Yes       0,00:29:18    0,00:00:02
192.168.9.3          4             188       ESTABLISHED      10          20          Yes       0,00:25:49    0,00:00:03
202.2.0.4            4             202       ESTABLISHED      0           35          Yes       0,00:29:58    0,00:00:03
S Chassis(rw)->
```

show ipv6 bgp

This command displays information about IPv6 BGP routes installed in the BGP routing information base (RIB).

Syntax

```
show ipv6 bgp (ipv6_address/masklen)
```

Parameters

ipv6_address/masklen	Optionally specify an IPv6 address along with a mask length.

Mode

Privileged Execution

Usage

The **show ipv6 bgp** command displays information about IPv6 BGP routes installed in the BGP RIB. By optionally specifying an IPv6 prefix with a mask or netmask, the output will only display detailed information for this route.

Example

The following example returns BGP information for all BGP routes installed in the BGP RIB.

```
S Chassis(rw)->show ipv6 bgp


S Chassis(rw)->
```

Table 72-4 table describes the fields that appear in the **show ipv6 bgp** query.

Table 72-4 show ipv6 bgp peer Output Details

Output...	What it displays...
Stat	Specifies the status of the route as follows: • **adv** - advertised • **sup** - suppressed • **pw** - route pending withdrawal • **wd** - route withdrawn
Aggr	Specifies a route aggregation code as follows: • **1** - This route is neither aggregating nor aggregated • **2** - This route is aggregating • **3** - This route is an unsuppressed aggregate • **4** - This route is a suppressed aggregate
Network	Specifies the network this route is on.
Next Hop	Specifies the IP address of the nearest gateway used to reach the EBGP peer
Rib	Specifies whether the route is installed in the unicast or multicast RIB
MED	Specifies the MED value for the route.
Local-Pref	Specifies the Local Preference value for the route.
Origin	Specifies whether the origin of the route is an internal or external protocol.
AS Path	Specifies the route's AS Path.

show ipv6 bgp neighbors

This command displays information about the state of BGP's IPv6 peering sessions.

Syntax

show ipv6 bgp neighbors [*ipv6-address/length*]

Parameters

ipv6_address/length	(Optional) Specifies an IPv6 address along with a mask length.

Mode

Privileged Execution

Usage

The **show ipv6 bgp neighbors** command displays detailed information about the state of BGP's peering sessions. You can optionally specify an IPv6 address. When you do so, the output of the query will display information for the specified address.

Example

The following example shows detailed information about all BGP peering sessions.

```
S Chassis(rw)->show ipv6 bgp neighbors
BGP neighbor is ::10.11.31.32, remote AS 65534
BGP version is 4, remote router ID 10.133.10.32
Negotiated version is 4
TTL is 0
holdtime is 180
restart-time is 0
Restarting: no
Current state is "Established"
Last state was "OpenConfirm"
Last event was "RecvKeepAlive"
Last error code was 0
Last error subcode was 0
Local address is ::10.11.31.31
Local AS is 65535
Local router ID is 192.168.11.31
Capabilities:
Multicprotocol IPv4 Unicast: no
Graceful Restart IPv4 Unicast: no
Multiprotocol IPv4 Multicast: no
Graceful Restart IPv4 Multicast: no
Route Refresh: no
Send End-of-RIB messages: no
Dynamic Capabilities: no
BGP neighbor is ::10.11.31.33, remote AS 65533
BGP version is 4, remote router ID 192.168.11.33
Negotiated version is 4
TTL is 0
holdtime is 180
restart-time is 0
Restarting: no
Current state is "Established"
Last state was "OpenConfirm"
Last event was "RecvKeepAlive"
Last error code was 0
Last error subcode was 0
Local address is 10.11.31.31
Local AS is 65535
```

```
Local router ID is 192.168.11.31
Capabilities:
Multiprotocol IPv4 Unicast: no
Graceful Restart IPv4 Unicast: no
Multiprotocol IPv4 Multicast: no
Graceful Restart IPv4 Multicast: no
Route Refresh: no
Send End-of-RIB messages: no
Dynamic Capabilities: no
```

show ipv6 bgp summary

This command shows IPv6 summarized BGP information.

Syntax

show ipv6 bgp summary

Parameters

None.

Defaults

None.

Mode

All command modes

Example

The following example shows a request for summarized BGP information.

```
S ChassisS Chassisshow ipv6 bgp summary
BGP router identifier 1.2.3.4, local AS number 10
Neighbor IPv6                           Version      Remote-AS    State
In updates  Out updates   Activated?
S Chassis(rw)->
```

73

OSPFv2 Commands

This chapter describes the Open Shortest Path First (OSPF) set of commands and how to use them. For information about configuring OSPF, refer to the "Open Shortest Path First (OSPF) Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
router ospf	73-3
address-family ipv4	73-3
network	73-4
router-id	73-5
neighbor	73-5
passive-interface	73-6
redistribute	73-7
distribute-list route-map in	73-8
rfc1583compatible	73-9
log-adjacency	73-9
spf lsa-thresholds	73-10
spf pause-frequency	73-11
timers spf	73-12
bfd all-intfs-on	73-12
distance ospf	73-13
enable-pe-ce	73-14
domain-tag	73-15
domain-id	73-16
area range	73-17
area stub	73-18
area default cost	73-18
area nssa	73-19
area nssa-range	73-20
area sham-link	73-20
area sham-link authentication-key	73-21

For information about...	Refer to page...
area sham-link dead-interval	73-22
area sham-link hello-interval	73-23
area sham-link keychain	73-24
area sham-link message-digest-key	73-25
area sham-link retransmit-interval	73-26
area sham-link transmit-delay	73-27
area sham-link cost	73-28
area virtual-link	73-29
auto-cost reference-bandwidth	73-30
graceful-restart enable	73-31
graceful-restart restart-interval	73-32
ip ospf cost	73-32
ip ospf cost track	73-33
ip ospf network	73-42
ip ospf priority	73-35
ip ospf poll-interval	73-35
ip ospf retransmit-interval	73-36
ip ospf transmit-delay	73-37
ip ospf ignore-mtu	73-37
ip ospf hello-interval	73-38
ip ospf dead-interval	73-39
ip ospf authentication-key	73-40
ip ospf message-digest-key md5	73-40
ip ospf helper-disable	73-41
ip ospf network	73-42
show ip ospf	73-42
show ip ospf database	73-44
show ip ospf border-routers	73-46
show ip ospf interface	73-47
show ip ospf neighbor	73-48
show ip ospf sham-link	73-49
show ip ospf virtual-links	73-50
show ip protocols	73-51
clear ip ospf process	73-52
debug ip ospf	73-52

router ospf

Use this command to enable or disable Open Shortest Path First (OSPF) configuration mode.

Syntax

router ospf *process-id*

no router ospf *process-id*

Parameters

process-id	Specifies the process ID, an internally used identification number for an OSPF routing process run on a router. Multiple OSPF processes are configurable per router. Valid values are **1** to **65535**.

Defaults

None.

Mode

Configuration command**.**

Usage

You must execute the **router ospf** command to enable the protocol before completing many OSPF-specific configuration tasks.

Multiple OSPF processes (*process-id*) are allowed per router. The S-Series router supports 4 OSPF processes per VRF and 16 OSPF processes per router.

The "no" form of this command disables OSPF configuration mode.

Example

This example shows how to enable routing for OSPF process 1:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router ospf 1
S Chassis(rw-config-ospf-1)->
```

address-family ipv4

This command enters IPv4 address family mode and configures unicast or multicast modes for this OSPF process.

Syntax

address-family ipv4 [**unicast** | **multicast**]

no address-family ipv4 {**unicast** | **multicast**}

Parameters

unicast | **multicast**	(Optional) Specifies that IPv4 is configured for either unicast or multicast. The default value is unicast.

Defaults

IPv4 unicast is the default address-family mode.

Mode

OSPF Router Configuration.

Usage

The **no address-family ipv4** command removes all topology configuration from this router configuration.

Example

The following example enters the IPv4 multicast address family configuration mode:

```
S Chassis(su-config-ospf-1)->address-family ipv4 multicast
S Chassis(su-config-ospf-1-af)->
```

The following example removes all topology configuration from this router configuration:

```
S Chassis(su-config-ospf-1)->no address-family ipv4
S Chassis(su-config-ospf-1)->
```

network

Use this command to configure area IDs for OSPF interfaces.

Syntax

network *ip-address wildcard-mask* **area** *area-id*

no network *ip-address wildcard-mask* **area** *area-id*

Parameters

ip-address	Specifies the IP address of an interface or a group of interfaces within the network address range.
wildcard-*mask*	Specifies the IP-address-type mask that includes “don't care” bits.
area *area-id*	Specifies the *area-id* to be associated with the OSPF address range. Valid values are decimal values between **0** - **4294967295** or an IP address. A subnet address can be specified as the *area-id* to associate areas with IP subnets.

Defaults

None.

Mode

OSPF router configuration.

Usage

OSPF network wildcard masks are reverse networks. This means that wherever there is a 1 in a regular netmask, use a 0 in a wildcard mask. For example, if the network mask is 255.255.255.0 (/24), specify a wildcard mask of 000.000.000.255.

The “no” form of this command removes OSPF routing for interfaces identified by the IP address and mask parameters.

Example

This example shows how to configure IP address 182.127.62.1 255.255.255.224 as OSPF area 0:

```
S Chassis(rw-config)->router ospf 1
S Chassis(rw-config-ospf-1)->network 182.127.62.1 0.0.0.31 area 0
```

router-id

Use this command to set the OSPF router ID for the device.

Syntax

router-id *ip-address*

Parameters

ip-address	Specifies the IP address that OSPF will use as the router ID.

Defaults

None.

Mode

OSPF router configuration.

Usage

The OSPF protocol uses the router ID as a tie-breaker for path selection. If not specified, this will be set to the highest IP address of the interfaces configured for IP routing. If no router ID is configured, then the OSPF router ID is set to the highest loopback address configured. If no loopback address is configured, then the highest IP address configured will be used. If no IP addresses are configured, then OSPF will not enable.

Example

This example shows how to set the OSPF router ID to IP address 182.127.62.1:

```
S Chassis(rw-config-ospf-1)->router-id 182.127.62.1
```

neighbor

Use this command to configure an OSPF neighbor of this router.

Syntax

neighbor *ip-address* [**priority** *priority*]

no neighbor *ip-address* [**priority** *priority*]

Parameters

priority *priority*	Specifies the OSPF priority of a non-broadcast neighbor. Valid values: **0**-**255**.

Defaults

None.

Mode

OSPF Configuration command.

Usage

OSPF dynamically discovers each neighbor for a given OSPF router. OSPF cannot dynamically discover its neighbors on non-broadcast and point-to-multipoint networks. For these networks neighbors must be configured. The router uses the information in the neighbor entry to send unicast hellos to the neighbor to start an adjacency. Use this command to specify the neighbor this OSPF router will form an adjacency with.

Example

This example shows how to configure neighbor 20.20.20.1 for this router:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router ospf 1
S Chassis(rw-config-ospf-1)->neighbor 20.20.20.1
S Chassis(rw-config-ospf-1)->
```

passive-interface

Use this command to enable passive OSPF on an interface.

Syntax

passive-interface {*vlan-id* | *interface-name* | **default**}

no passive-interface {*vlan-id* | *interface-name* | **default**}

Parameters

vlan-id	Specifies the VLAN number on which to enable passive OSPF mode.
interface-name	Specifies a VLAN in the interface-name format: vlan.*x*.*y*
default	Sets all enabled OSPF interfaces to passive.

Defaults

None.

Mode

OSPF router configuration.

Usage

This allows an interface to be included in the OSPF route table, but turns off sending and receiving hellos for the specified interface. It also prevents OSPF adjacencies from being formed on the specified interface.

The "no" form of this command disables passive OSPF mode.

Example

This example shows how to enable passive OSPF mode on VLAN 102 (can be specified as **102** or **vlan.0.102**):

```
S Chassis(rw-config)router ospf 1
S Chassis(rw-config-ospf-1)->passive-interface 102
```

redistribute

Use this command to allow routing information discovered through non-OSPF protocols to be distributed in OSPF update messages.

Syntax

redistribute {**rip** | **static** | **connected** | **bgp** [**global**]} [**route-map** *name*] [**metric** *metric-value*] [**metric-type** *type-value*] [**tag** *tag*]

no redistribute {**connected** | **rip** | **static** | **bgp** [**global**]}

Parameters

rip	Specifies that RIP routing information will be redistributed in OSPF.
static	Specifies that non-OSPF information discovered via static routes will be redistributed. Static routes are those created using the **ip route** command detailed in "ip route" on page 56-5.
connected	Specifies that non-OSPF information discovered via directly connected interfaces will be redistributed. These are routes not specified in the OSPF network command as described in "network" on page 73-4.
bgp	Specifies that BGP routing information will be redistributed in OSPF.
global	(Optional) Specifies that BGP prefixes from the global router are redistributed. VPN4-address prefixes are translated appropriately.
route-map *name*	(Optional) Redistributes routes using the rules established by the designated route-map.
metric *metric-value*	(Optional) Specifies a metric for the connected, RIP or static redistribution route. This value should be consistent with the designation protocol.
metric-type *type-value*	(Optional) Specifies the external link type associated with the default connected, RIP or static route advertised into the OSPF routing domain. Valid values are **1** for type 1 external route, and **2** for type 2 external route.
tag *tag*	(Optional) Specifies that tagged routes will be redistributed in OSPF.

Defaults

- If global is not specified, routes associated with the VRF BGP instance are redistributed.

- If *metric-value* is not specified, **20** will be applied.
- If *type-value* is not specified, type 2 (external route) will be applied.
- If **route-map** is not specified, none will be applied.
- If **tag** is not specified, none will be applied.

Mode

OSPF router configuration.

Usage

Specifying the global BGP option requires that the PE-CE feature is enabled using "enable-pe-ce" on page 73-14. The global option turns on the RFC 4577 DN bit.

The "no" form of thiscommand clears redistribution parameters.

Example

This example shows how to distribute external type 2 RIP routing information from routes in OSPF updates:

```
S Chassis(rw-config)->router ospf 1
S Chassis(rw-config-ospf-1)->redistribute rip
```

distribute-list route-map in

Use this command to assign an OSPF route filter route-map with the distribute-list for the purpose of filtering routes being installed into the route table.

Syntax

distribute-list route-map *name* **in**

no distribute-list route-map *name* **in**

Parameters

name	Specifies the OSPF route filter route-map to associate with this distribute-list.

Defaults

None.

Mode

OSPF router configuration.

Usage

See "Filter-Based Route-Map Commands" on page 85-24 for a detailed discussion of OSPF filter-based route-map commands.

The "no" form of this command clears the specified route-map from the distribute-list.

Example

This example shows how to assign the ospf1 filter route-map to the distribute-list for this OSPF router:

```
S Chassis(rw-config)->router ospf 1
S Chassis(rw-config-ospf-1)->distribute-list route-map ospf1 in
```

rfc1583compatible

Use this command to enable the OSPF router for RFC 1583 compatibility.

Syntax

rfc1583compatible

no rfc1583compatible

Parameters

None.

Defaults

None.

Mode

OSPF router configuration.

Usage

This implementation of OSPF is compatible with RFC 2328. This command enables compatibility with RFC 1583.

The “no” form of this command removes OSPF RFC 1583 compatibility.

Example

This example shows how to configure RFC 1583 compatibility:

```
S Chassis(rw-config)->router ospf 1
S Chassis(rw-config-ospf-1)->rfc1583compatible
```

log-adjacency

Use this command to enable or disable adjacency logging on this OSPF router.

Syntax

log-adjacency

no log-adjacency

Parameters

None.

Defaults

None.

Mode

OSPF router configuration command mode.

Usage

The “no” form of this command disables adjacency logging for this OSPF router.

Example

This example shows how to enable adjacency logging on the OSPF process 1:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router ospf 1
S Chassis(rw-config-ospf-1)->log-adjacency
```

spf lsa-thresholds

Use this command to specify the number of Shortest Path First (SPF) LSA thresholds to optimize the performance of the routing calculation.

Syntax

spf lsa-thresholds *num-start num-restart num-intra-full num-ia-ext-full*

no lsa-thresholds

Parameters

num-start	Specifies the number of LSA updates that force a full routing calculation. Valid values: **0** - **4294967295**; Default: **4294967295**.
num-restart	Specifies the number of LSA updates that interrupt and restart a full routing calculation. Valid values: **0** - **4294967295**; Default: **4294967295**.
num-ia-ext-full	Specifies the number of LSA inter-area/external updates that force a full routing calculation. Valid values: **0** - **4294967295**; Default: **50**.
num-intra-full	Specifies the number of intra updates that force a full routing calculation. Valid values: **0** - **4294967295**; Default: **0**.

Defaults

None.

Mode

OSPF router configuration.

Usage

The “no” form of this command restores the default values.

A value of **0** for either the number of LSA inter-area/external updates or intra updates means a full routing calculation would always be done for any inter-area/external update received.

Example

This example shows how to change the number of LSA inter-area/external updates that force a full routing calculation to 75 leaving the remaining defaults unchanged:

```
S Chassis(rw-config)->router ospf 1
S Chassis(rw-config-ospf-1)->spf lsa-thresholds 4294967295 4294967295 75 0
S Chassis(rw-config-ospf-1)->
```

spf pause-frequency

Use this command to specify the number of units of CPU credits SPF calculation runs before pausing.

Syntax

spf pause-frequency *units*

no pause-frequency

Parameters

units	Specifies the number of units of CPU credit an SPF calculation runs before pausing. Valid values: **0** - **4294967295**; Default: **10000**.

Defaults

None.

Mode

OSPF router configuration.

Usage

The SPF algorithm is a method of calculating the best path to all known destinations based on the information in its link state database. A CPU credit is a unit of processing controlled by the operating system. After the SPF calculation has run the configured number of CPU credits, the SPF process will pause allowing other active processes a share of CPU time. The SPF calculation will start up again after all other active processes have used up their allotted credits. Increasing this value will allow a faster completion of an SPF calculation at the expense of all other active processes.

Entering 0 specifies the SPF calculation does not pause until it is completed.

The “no” form of this command restores the default values.

Example

This example shows how to set the SPF pause frequency setting to 12000 units:

```
S Chassis(rw-config)->router ospf 1
S Chassis(rw-config-ospf-1)->spf pause-frequency 12000
```

timers spf

Use this command to change OSPF timer values.

Syntax

timers spf *spf-delay*

no timers spf

Parameters

spf-delay	Specifies the delay, in milli-seconds, between the receipt of an update and the SPF execution. Valid values are **0** to **4294967295**. The default value is **5** seconds. The value is entered in milli-seconds.

Defaults

None.

Mode

OSPF router configuration.

Usage

The “no” form of this command restores the default timer values.

Example

This example shows how to set spf delay time to 7 seconds:

```
S Chassis(rw-config)->router ospf 1
S Chassis(rw-config-ospf-1)->timers spf 7000
```

bfd all-intfs-on

Use this command to enable the Bidirectional Forwarding Detection (BFD) protocol on all OSPF interfaces.

Syntax

bfd all-intfs-on

no bfd all-intfs-on

Parameters

None.

Defaults

The BFD protocol is enabled on all OSPF interfaces by default.

Mode

OSPF router configuration.

Usage

BFD is used to detect a communications failure with an OSPF forwarding plane next-hop. BFD detects failures in under one second. BFD augments the OSPF Hello mechanism. The OSPF Hello interval defaults to 10 seconds. With high speed data rates, a failure requiring multiple seconds to detect can result in significant data loss. The OSPF implementation of the BFD protocol uses the following non-configurable parameters:

Transmit Interval – The period of time between the transmission of BFD control packets, set for 100ms.

Receive Interval – The period of time between received BFD control packets, set for 100ms.

Detection Multiplier – The Number of consecutive control packets that can be missed before the BFD session transitions to down, set to 3.

The "no" form of this command disables the BFD protocol on all OSPF interfaces.

Example

This example shows how to disable the BFD protocol on all OSPF interfaces for OSPF instance 1:

```
S Chassis(rw-config)->router ospf 1
S Chassis(rw-config-ospf-1)->no bfd all-intfs-on
```

distance ospf

Use this command to configure the administrative distance for OSPF routes.

Syntax

distance [**ospf** {**external** | **intra-area**}] *weight*

no distance ospf {**external** | **intra-area**}

Parameters

external | **intra-area**	Applies the distance value to external (type 5 and type 7) or to intra-area routes. **Note:** The value for intra-area distance must be less than the value for external distance.
weight	Specifies an administrative distance for OSPF routes. Valid values are **1**-**255**. Default: **110**.

Defaults

If route type is not specified, the distance value will be applied to all OSPF routes (110).

Mode

OSPF router configuration.

Usage

If several routes (coming from different protocols) are presented to the Extreme Networks S-Series Route Table Manager (RTM), the protocol with the lowest administrative distance will be chosen for route installation. By default, OSPF administrative distance is set to 110. The **distance** command can be used to change this value, resetting OSPF's route preference in relation to other routes as shown in the table below.

Route Source	Default Distance
Connected	0
Static	1
BGP	20 - Routes external to the AS 200 - Routes internal to the AS
OSPF	110
RIP	120

The **distance ospf** command applies the value to the specified route type.

The "no" form of this command resets OSPF administrative distance to the default value of 110.

Example

This example shows how to change the default administrative distance for external OSPF routes to 100:

```
S Chassis(rw-config)->router ospf 1
S Chassis(rw-config-ospf-1)->distance ospf external 100
```

enable-pe-ce

Use this command to enable the Customer Edge (CE) routers as Provider Edge (PE) router peers.

Syntax

enable-pe-ce

no enable-pe-ce

Parameters

None.

Defaults

CE routers are disabled as PE router peers by default.

Mode

VRF configuration, OSPF router configuration.

Usage

Enabling CE routers as PE router peers is defined in RFC 4577.

The "no" form of this command disables CE routers as PE router peers for this device.

Example

This example enables CE routers as PE router routing peers for this device:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->
```

domain-tag

Use this command to specify an OSPF VPN routing and forwarding (VRF) domain tag.

Syntax

domain-tag *tag*

no domain-tag

Parameters

tag	Specifies an OSPF VRF domain tag value. Valid values are **0** - **4294967295**. Default value is **0**.

Defaults

The OSPF VRF domain tag default value is **0**.

Mode

VRF configuration, OSPF router configuration.

Usage

The configuration and inclusion of the OSPF VRF domain tag is required for PE-CE protocol enabled systems to be backward compatible with systems that do not set the PE-CE protocol DN bit in type 5 LSAs. When a prefix is received from a BGP speaker and redistributed into the PE-CE protocol enabled OSPF instance, the OSPF process for the VRF is given a domain tag. In the event that the customer site attempts to re-advertise the prefix to another PE using the same domain tag, the domain tag will be matched and the prefix will not be accepted by the second PE for redistribution into BGP. Setting the same domain tag for all backbone PE routers on the same VPN prevents routing loops.

Setting the OSPF VRF domain tag is optional when the PE-CE protocol is enabled for all PE backbone routers for a given VRF. If legacy PE routers that do not support the PE-CE protocol are present in the VRF backbone, set the domain tag for this router to agree with the domain tag of the legacy router.

The PE-CE protocol (RFC 4577) must be enabled using “enable-pe-ce” on page 73-14 to set the OSPF VRF domain tag.

The “no” form of this command restores the default domain tag value of **0**.

Example

This example shows how to set the OSPF VRF domain tag value to 100 for VRF **doc**:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->domain-tag 100
```

domain-id

Use this command to specify an OSPF VPN routing and forwarding (VRF) domain ID.

Syntax

domain-id type *type* **value** *value* [**secondary**]

no domain-id type *type* **value** *value* [**secondary**]

Parameters

type *type*	Specifies an OSPF VRF domain ID type. Valid values are **0005** | **0105** | **0205** | **8005**.
value *value*	Specifies an OSPF VRF domain ID value. Valid values are six octets in hex format (up to 12 hex characters). Default value is **0**.
secondary	(Optional) Specifies an OSPF secondary domain ID

Defaults

- The OSPF VRF domain ID type defaults to **0005**
- The OSPF VRF domain ID default value is **0**.

Mode

VRF configuration, OSPF router configuration.

Usage

If the OSPF instances of an OSPF domain are given one or more domain IDs, OSPF can determine whether an OSPF-originated VPN-IPv4 route belongs to the same domain as a given OSPF instance and whether the route should be redistributed to that OSPF instance as an inter-area route or as an OSPF AS-external route.

If two OSPF instances with a domain ID configured are in the same OSPF domain, the PE-CE protocol requires that the primary domain ID of each instance must be one its own domain IDs (either primary or secondary). If two OSPF instances with a domain ID configured are not in the same OSPF domain, the primary domain ID of each instance must not be configured as a domain ID of the other OSPF instance.

The PE-CE protocol (RFC 4577) must be enabled using “enable-pe-ce” on page 73-14 to set the OSPF VRF domain ID.

The “no” form of this command restores the default domain ID type to **0005** and value to **0**.

Example

This example shows how to set the OSPF VRF primary domain ID type to **0105** and value to **100** for VRF **doc**:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->domain-id type 0105 100
```

area range

Use this command to define the range of addresses to be used by Area Border Routers (ABRs) when they communicate routes to other areas.

Syntax

area *area-id* **range** *ip-address ip-mask* [**not-advertise**]

no area *area-id* **range** *ip-address ip-mask* [**not-advertise**]

Parameters

area-id	Specifies the area at the boundary of which routes are to be summarized.
ip-address	Specifies the common prefix of the summarized networks.
ip-mask	Specifies the length of the common prefix.
not-advertise	(Optional) Prevents advertisement of the specified IP address range

Defaults

If **not-advertise** is not specified, the specified IP address range is advertised.

Mode

OSPF router configuration.

Usage

The “no” form of this command stops the routes from being summarized.

Example

This example shows how to define the address range as 172.16.0.0/16 for summarized routes communicated at the boundary of area 0.0.0.0:

```
S Chassis(rw-config)->router ospf 1
S Chassis(rw-config-ospf-1)->area 0.0.0.0 range 172.16.0.0 255.255.0.0
```

area stub

Use this command to define an OSPF area as a stub area.

Syntax

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub** [**no-summary**]

Parameters

area-id	Specifies the stub area. Valid values are decimal values or ip addresses.
no-summary	(Optional) Prevents an Area Border Router (ABR) from sending type 3 summary Link State Advertisements (LSAs) into the stub area. When this parameter is used, it means that all destinations outside of the stub area are represented by means of a default route.

Defaults

If **no-summary** is not specified, the stub area will be able to receive LSAs.

Mode

OSPF router configuration.

Usage

This is an area that carries no external routes.

The "no" form of this command changes the stub back to a plain area.

Example

The following example shows how to define OSPF area 10 as a stub area:

```
S Chassis(rw-config)->router ospf 1
S Chassis(rw-config-ospf-1)->area 10 stub
```

area default cost

Use this command to set the cost value for the default route that is sent into a stub area by an Area Border Router (ABR).

Syntax

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

Parameters

area-id	Specifies the stub area. Valid values are decimal values or IP addresses.
cost	Specifies a cost value for the summary route that is sent into a stub area by default. Valid values: **0** to **65535**.

Defaults

None.

Mode

OSPF router configuration.

Usage

The use of this command is restricted to ABRs attached to stub areas.

The “no” form of this command removes the cost value from the summary route that is sent into the stub area.

Example

This example shows how to set the cost value for stub area 10 to 99:

```
S Chassis(rw-config)->router ospf 1
S Chassis(rw-config-ospf-1)->area 10 default-cost 99
```

area nssa

Use this command to configure an area as a Not-So-Stubby-Area (NSSA).

Syntax

area {*area-id* | *ip-address*} **nssa** [**no-summary**] [**transstabilityint** *seconds*] [**transrole always**]

no area *area-id* **nssa** [**no-summary**] [**transstabilityint**][**transrole always**]

Parameters

area-id | *ip-address*	Specifies the NSSA area. Valid values are decimal values or IP addresses.
no-summary	(Optional) Prevents an Area Border Router (ABR) from sending type 3 summary Link State Advertisements (LSAs) into the NSSA area. When this parameter is used, it means that all destinations outside of the NSSA area are represented by means of a default route.
transstabilityint *seconds*	(Optional) Specifies the translator stability interval in seconds. Valid values: **0** - **65535**
transrole always	(Optional) Specifies that an NSSA router will unconditionally translate Type-7 LSAs to Type-5 LSAs when acting as an NSSA border router. Configuring the identity of the translator can be used to bias the routing to aggregated destinations. When translator role is set to Always, Type-7 LSAs are always translated regardless of the translator state of other NSSA border routers.

Defaults

If **no-summary**, **transstabilityint** and **transrole always** are not specified, a default NSSA area is configured.

Mode

OSPF router configuration.

Usage

An NSSA area allows some external routes represented by external Link State Advertisements (LSAs) to be imported into it. This is in contrast to a stub area that does not allow any external routes.

The "no" form of this command changes the NSSA back to a default area.

Example

This example shows how to configure area 10 as an NSSA area:

```
S Chassis(rw-config)->router ospf 1
S Chassis(rw-config-ospf-1)->area 10 nssa
```

area nssa-range

Use this command to Summarize Type 7 to Type 5 routes matching the specified address and mask on an Autonomous System Border Router (ASBR) at an NSSA border.

Syntax

area {*area-id | ip-address*} **nssa-range** *ip-address mask*

no area {*area-id | ip-address*} **nssa-range** *ip-address* [*mask*]

Parameters

area-id | *ip-address*	Specifies the NSSA area. Valid values are decimal values or IP addresses.
ip-address mask	Specifies the IP address and mask to match for this Type 7–>5 ASBR summarization.

Defaults

None.

Mode

OSPF router configuration.

Example

This example shows how to summarize area 10 Type 7 to Type 5 routes from IP address and mask for this ASBR:

```
S Chassis(rw-config)->router ospf 1
S Chassis(rw-config-ospf-1)->area 10 nssa-range 50.0.0.0 255.0.0.0
```

area sham-link

Use this command to configure an OSPF sham link between two PE routers.

Syntax

area *area-id* **sham-link** *source-ip-address destination-ip-address*

no area *area-id* **sham-link** *source-ip-address destination-ip-address*

Parameters

area-id	Specifies the OSPF area the two PE routers belong to.
source-ip-address	Specifies the source IPv4 address for this sham link.
destination-ip-address	Specifies the destination IPv4 address for this sham link.

Defaults

None.

Mode

VRF configuration, OSPF router configuration.

Usage

If a VRF contains both an OSPF-distributed route and a VPN-IPv4 route for the same IPv4 prefix, then the backdoor OSPF-distributed route is preferred over the VPN backbone route, unless the next hop interface for an installed (OSPF distributed) route is the sham link, in which case, the VPN backbone VPN-IPv4 route is used.

If it is desired to have OSPF prefer the routes through the VPN backbone over the routes through the OSPF backdoor link, then the routes through the backbone must appear to be intra-area routes. The sham link provides this appearance of an intra-area link connecting the two PE routers.

The "no" form of this command deletes the configured sham link.

Example

This example shows how to configure a sham link between two PE routers with a source address of **172.16.1.10** and a destination address of **172.16.2.20** on OSPF router instance **10**, VRF **doc**:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->area 10 sham-link 172.16.1.10 172.16.2.20
```

area sham-link authentication-key

Use this command to configure the authentication key on an OSPF sham link.

Syntax

area *area-id* **sham-link** *source-ip-address destination-ip-address* **authentication-key** *password*

no area *area-id* **sham-link** *source-ip-address destination-ip-address* **authentication-key**

Parameters

area-id	Specifies the OSPF area the two PE routers belong to.
source-ip-address	Specifies the source IP address for this sham link.
destination-ip-address	Specifies the destination IP address for this sham link.
password	Specifies an OSPF authentication password. Valid values are alphanumeric strings up to 8 bytes in length.

Defaults

None.

Mode

VRF configuration, OSPF router configuration.

Usage

All neighboring routers on the same network must have the same password configured to be able to exchange OSPF information.

This password is used as a "key" that is inserted directly into the OSPF header in routing protocol packets. A separate password can be assigned to each sham link.

The "no" form of this command deletes the configured sham link authentication key.

Example

This example shows how to configure a sham link between two PE routers with a source address of **172.16.1.10** and a destination address of **172.16.2.20** on OSPF router instance **10**, VRF **doc** and assign an authentication key of **yourpass**::

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->area 10 sham-link 172.16.1.10 172.16.2.20
authentication-key yourpass
```

area sham-link dead-interval

Use this command to configure the dead interval for an OSPF sham link.

Syntax

area *area-id* **sham-link** *source-ip-address destination-ip-address* **dead-interval** *seconds*

no area *area-id* **sham-link** *source-ip-address destination-ip-address* **dead-interval**

Parameters

area-id	Specifies the OSPF area the two PE routers belong to.
source-ip-address	Specifies the source IP address for this sham link.
destination-ip-address	Specifies the destination IP address for this sham link.

seconds	(Optional) Specifies the number of seconds that the hello packets of a router are not communicated to neighbor routers before the neighbor routers determine that the router sending the hello packet is out of service. This value must be the same for all nodes attached to a certain subnet, and it is a value ranging from **1** to **2147843647**. The default value is **60** seconds.

Defaults

The dead interval defaults to 60 seconds.

Mode

VRF configuration, OSPF router configuration.

Usage

Dead interval must be the same on neighboring routers (on a specific subnet), but can vary between subnets.

The "no" form of this command resets the sham link dead interval to 10 seconds.

Example

This example shows how to configure a sham link dead interval to 80 seconds between two PE routers with a source address of **172.16.1.10** and a destination address of **172.16.2.20** on OSPF router instance **10**, VRF **doc**:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->area 10 sham-link 172.16.1.10 172.16.2.20
dead-interval 80
```

area sham-link hello-interval

Use this command to configure the hello interval for an OSPF sham link.

Syntax

area *area-id* **sham-link** *source-ip-address destination-ip-address* **hello-interval** *seconds*

no area *area-id* **sham-link** *source-ip-address destination-ip-address* **hello-interval**

Parameters

area-id	Specifies the OSPF area the two PE routers belong to.
source-ip-address	Specifies the source IP address for this sham link.
destination-ip-address	Specifies the destination IP address for this sham link.
seconds	(Optional) Specifies the number of seconds between hello packets on an interface. Valid values range from **1** to **65535**. The default value is **10** seconds.

Defaults

The hello interval defaults to 10 seconds.

Mode

VRF configuration, OSPF router configuration.

Usage

This value must be the same for all nodes attached to a network. By default, hello packets are sent out every 10 seconds. If after 40 seconds, there is no response on the interface, the interface will be shutdown.

The "no" form of this command resets the hello interval to the default value for this sham link.

Example

This example shows how to configure the hello interval to **15** seconds for a sham link between two PE routers with a source address of **172.16.1.10** and a destination address of **172.16.2.20** on OSPF router instance **10**, VRF **doc**:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->area 10 sham-link 172.16.1.10 172.16.2.20
hello-interval 15
```

area sham-link keychain

Use this command to configure an MD5 keychain for this sham link.

Syntax

area *area-id* **sham-link** *source-ip-address destination-ip-address* **keychain** *name*

no area *area-id* **sham-link** *source-ip-address destination-ip-address* **keychain**

Parameters

area-id	Specifies the OSPF area the two PE routers belong to.
source-ip-address	Specifies the source IP address for this sham link.
destination-ip-address	Specifies the destination IP address for this sham link.
name	Specifies the name of the OSPF keychain that holds MD5 keys.

Defaults

None.

Mode

VRF configuration, OSPF router configuration.

Usage

The "no" form of this command removes the current keychain from the sham link.

Example

This example shows how to configure keychain **keychain1** to a sham link between two PE routers with a source address of **172.16.1.10** and a destination address of **172.16.2.20** on OSPF router instance **10**, VRF **doc**:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->area 10 sham-link 172.16.1.10 172.16.2.20
keychain keychain1
```

area sham-link message-digest-key

Use this command to configure a message digest key for an OSPF sham link.

Syntax

area *area-id* **sham-link** *source-ip-address destination-ip-address* **message-digest-key** *digest-key* **md5** *auth-key*

no area *area-id* **sham-link** *source-ip-address destination-ip-address* **message-digest-key** *digest-key*

Parameters

area-id	Specifies the OSPF area the two PE routers belong to.
source-ip-address	Specifies the source IP address for this sham link.
destination-ip-address	Specifies the destination IP address for this sham link.
message-digest-key *digest-key* **md5** *auth-key*	(Optional) Specifies the message digest key settings: • *digest-key* - Specifies the key identifier on the interface where MD5 authentication is enabled in a value range from **1** - **255**. • *auth-key* - Specifies a password for MD5 authentication to be used with the *digest-key*. Valid values are alphanumeric strings of up to 16 bytes.

Defaults

None.

Mode

VRF configuration, OSPF router configuration.

Usage

This command validates OSPF MD5 routing updates between neighboring routers.

The “no” form of this command removes the message digest key configuration from the sham link.

Example

This example shows how to enable OSPF MD5 authentication on a sham link between two PE routers with a source address of **172.16.1.10** and a destination address of **172.16.2.20** on OSPF router instance **10**, VRF **doc**, set the key identifier to **20**, and set the password to **passone**:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->area 10 sham-link 172.16.1.10 172.16.2.20
message-digest-key 20 md5 passone
```

area sham-link retransmit-interval

Use this command to configure the retransmit interval for an OSPF sham link.

Syntax

area *area-id* **sham-link** *source-ip-address destination-ip-address* **retransmit-interval** *seconds*

no area *area-id* **sham-link** *source-ip-address destination-ip-address* **retransmit-interval**

Parameters

area-id	Specifies the OSPF area the two PE routers belong to.
source-ip-address	Specifies the source IP address for this sham link.
destination-ip-address	Specifies the destination IP address for this sham link.
seconds	(Optional) Specifies the number of seconds between successive retransmissions of the same LSAs. Valid values are greater than the expected amount of time required for the update packet to reach and return from the interface, and range from **1** to **3600**. The default value is **5** seconds.

Defaults

Retransmit interval defaults to **5** seconds.

Mode

VRF configuration, OSPF router configuration.

Usage

The “no” form of this command resets the sham link retransmit interval value to the default value.

Example

This example shows how to configure the retransmit interval to **10** for a sham link between two PE routers with a source address of **172.16.1.10** and a destination address of **172.16.2.20** on OSPF router instance **10**, VRF **doc**:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
```

```
S Chassis(su-doc-config)->router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->area 10 sham-link 172.16.1.10 172.16.2.20
```

area sham-link transmit-delay

Use this command to configure a transmit delay period for an OSPF sham link.

Syntax

area *area-id* **sham-link** *source-ip-address destination-ip-address* **transmit-delay** *seconds*

no area *area-id* **sham-link** *source-ip-address destination-ip-address* **transmit-delay**

Parameters

area-id	Specifies the OSPF area the two PE routers belong to.
source-ip-address	Specifies the source IP address for this sham link.
destination-ip-address	Specifies the destination IP address for this sham link.
seconds	(Optional) Specifies the estimated number of seconds for a link state update packet on the interface to be transmitted. Valid values range from **1** to **3600**. The default value is **1** second.

Defaults

The sham link transmit delay period defaults to **1** second.

Mode

VRF configuration, OSPF router configuration.

Usage

The “no” form of this command resets the sham link transmit delay value to the default.

Example

This example shows how to configure a transmit delay period of **5** seconds for the sham link between two PE routers with a source address of **172.16.1.10** and a destination address of **172.16.2.20** on OSPF router instance **10**, VRF **doc**:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->area 10 sham-link 172.16.1.10 172.16.2.20
transmit-delay 5
```

area sham-link cost

Use this command to configure the cost of an OSPF sham link.

Syntax

area *area-id* **sham-link** *source-ip-address destination-ip-address* **cost** *cost*

no area *area-id* **sham-link** *source-ip-address destination-ip-address* **cost**

Parameters

area-id	Specifies the OSPF area the two PE routers belong to.
source-ip-address	Specifies the source IP address for this sham link.
destination-ip-address	Specifies the destination IP address for this sham link.
cost	Specifies the cost of the sham link. Valid values are **1** - **65535**. The default value is the reference bandwidth divided by the interface bandwidth.

Defaults

The default cost of the sham link is the reference bandwidth divided by the interface bandwidth.

Mode

VRF configuration, OSPF router configuration.

Usage

Each router interface that participates in OSPF routing is assigned a default cost. This command overwrites the default OSPF interface cost.

The reference bandwidth defaults to 100Mbps and can be modified using “auto-cost reference-bandwidth” on page 73-30.

The “no” form of this command resets the OSPF cost for the sham link to the default of 10.

Example

This example shows how to configure a cost of 20 for the sham link between two PE routers with a source address of **172.16.1.10** and a destination address of **172.16.2.20** on OSPF router instance **10**, VRF **doc**:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->area 10 sham-link 172.16.1.10 172.16.2.20 cost
20
```

area virtual-link

Use this command to define an OSPF virtual link, which represents a logical connection between the backbone and a non-backbone OSPF area.

Syntax

area *area-id* **virtual-link** *ip-address*

The options for using this syntax are:

area *area-id* **virtual-link** *ip-address* **authentication-key** *key*

area *area-id* **virtual-link** *ip-address* **dead-interval** *seconds*

area *area-id* **virtual-link** *ip-address* **hello-interval** *seconds*

area *area-id* **virtual-link** *ip-address* **message-digest-key** *digest-key* **md5** *auth-key*

area *area-id* **virtual-link** *ip-address* **retransmit-interval** *seconds*

area *area-id* **virtual-link** *ip-address* **transmit-delay** *seconds*

no area *area-id* **virtual-link** *ip-address* **authentication-key** *key*

no area *area-id* **virtual-link** *ip-address* **dead-interval** *seconds*

no area *area-id* **virtual-link** *ip-address* **hello-interval** *seconds*

no area *area-id* **virtual-link** *ip-address* **retransmit-interval** *seconds*

no area *area-id* **virtual-link** *ip-address* **transmit-delay** *seconds*

Parameters

area-id	Specifies the transit area for the virtual link. Valid values are decimal values or IP addresses. A transit area is an area through which a virtual link is established.
ip-address	Specifies the router id of the virtual link neighbor. A virtual link is established through the transit area to the virtual link neighbor.
authentication- key *key*	(Optional) Specifies a password to be used by neighbor routers. Valid values are alphanumeric strings of up to 8 bytes. Neighbor routers on a network must have the same password.
dead-interval *seconds*	(Optional) Specifies the number of seconds that the hello packets of a router are not communicated to neighbor routers before the neighbor routers determine that the router sending the hello packet is out of service. This value must be the same for all nodes attached to a certain subnet, and it is a value ranging from **1** to **2147843647**. The default value is **60** seconds.
hello-interval *seconds*	(Optional) Specifies the number of seconds between hello packets on an interface. This value must be the same for all nodes attached to a network and it is a value ranging from **1** to **65535**. The default value is **10** seconds.
message-digest-key *digest-key* **md5** *auth-key*	(Optional) Specifies the message digest key settings: • *digest-key* - Specifies the key identifier on the interface where MD5 authentication is enabled in a value range from **1** - **255**. • *auth-key* - Specifies a password for MD5 authentication to be used with the *digest-key*. Valid values are alphanumeric strings of up to 16 bytes.

retransmit-interval *seconds*	(Optional) Specifies the number of seconds between successive retransmissions of the same LSAs. Valid values are greater than the expected amount of time required for the update packet to reach and return from the interface, and range from **1** to **3600**. The default value is **5** seconds.
transmit-delay *seconds*	(Optional) Specifies the estimated number of seconds for a link state update packet on the interface to be transmitted. Valid values range from **1** to **3600**. The default value is **1** second.

Defaults

None.

Mode

OSPF router configuration.

Usage

The "no" form of this command removes the virtual link if only the area ID and IP-address are specified. If an optional parameter is specified, that option is reset to its default value.

Example

This example shows how to configure a virtual link between a router in OSPF area 0.0.0.2 and the ABR 134.141.7.2:

```
S Chassis(rw-config)->router ospf 1
S Chassis(rw-config-ospf-1)->area 0.0.0.2 virtual-link 134.141.7.2
```

auto-cost reference-bandwidth

Use this command to configure an OSPF auto cost reference bandwidth for this OSPFv2 instance.

Syntax

auto-cost reference-bandwidth *bandwidth-multiplier*

no auto-cost reference-bandwidth *bandwidth-multiplier*

Parameters

bandwidth-multiplier	Specifies the auto cost bandwidth multiplier in megabits per second for this OSPFv2 instance. Valid values are **1** - **4294967**. The default value is **100**.

Defaults

None.

Mode

OSPF router configuration.

Usage

The formula for calculating the OSPF interface cost metric is the reference bandwidth divided by the interface bandwidth. By default the reference bandwidth is set to 100 Mbps. For 10 Mbps links,

the resulting cost is 10. For 100, 1000, or 10000 Mbps links, the resulting cost is 1. The ability to re-center the reference bandwidth to a higher value, allows for OSPF interface costs to default to a value greater than 1 for 100, 1000, or 10000 Mbps links and greater than 10 for 10 Mbps links.

It is recommended that the auto cost reference bandwidth be the same value for all OSPF routers in the domain.

The OSPF interface cost can be statically set or determined using the interface summoning method with tracked objects using "ip ospf cost" on page 73-32.

The "no" form of this command resets the auto cost reference bandwidth to 100 Mbps for this OSPFv2 instance.

Example

This example shows how to configure the auto cost reference bandwidth to 1Gbps for OSPF instance 10:

```
S Chassis(su)->configure
S Chassis(su-config)->router ospf 10
S Chassis(su-config-ospf-10)->auto-cost reference-bandwidth 1000
S Chassis(su-config-ospf-10)->
```

graceful-restart enable

Use this command to enable the graceful-restart ability on this router.

Syntax

graceful-restart enable

no graceful-restart enable

Parameters

None.

Defaults

None.

Mode

OSPF router configuration.

Usage

Graceful restart allows this router to stay on the forwarding path during a failover. For more information about graceful restart, see the *Extreme Networks S-Series Configuration Guide*.

The "no" form of this command disables graceful-restart for this router.

Example

This example shows how to enable the graceful restart ability on this router:

```
S Chassis(rw-config)->router ospf 1
S Chassis(rw-config-ospf-1)->graceful-restart enable
S Chassis(rw-config-ospf-1)->
```

graceful-restart restart-interval

Use this command to set the graceful-restart restart interval.

Syntax

graceful-restart restart-interval *interval*

no graceful-restart restart-interval *interval*

Parameters

interval	Specifies the maximum amount of time in seconds that this router will remain in graceful-restart mode starting at the time it enters graceful-restart. Valid values are **1** - **1800** seconds. Default value is **120** seconds.

Defaults

None.

Mode

OSPF router configuration.

Usage

The restart interval sets the maximum amount of time that this router will remain in graceful restart once an OSPF restart is initiated.

The “no” form of this command resets the graceful-restart restart-interval to its default value.

Example

This example sets the graceful restart restart-interval to 300 seconds:

```
S Chassis(rw-config)->router ospf 1
S Chassis(rw-config-ospf-1)->graceful-restart enable
S Chassis(rw-config-ospf-1)->graceful-restart restart-interval 300
```

ip ospf cost

Use this command to statically set the cost of sending an OSPF packet on an interface.

Syntax

ip ospf cost *cost*

no ip ospf cost *cost*

Parameters

cost	Specifies the cost of sending a packet. Valid values range from **1** to **65535**. The default value is the reference bandwidth divided by the interface bandwidth.

Defaults

None.

Mode

Configuration command, Interface configuration.

Usage

Each router interface that participates in OSPF routing is assigned a default cost. This command overwrites the default OSPF interface cost.

The reference bandwidth defaults to 100Mbps and can be modified using "auto-cost reference-bandwidth" on page 73-30.

The "no" form of this command resets the OSPF cost to the default of 10.

Example

This example shows how to set the OSPF cost to 20 for VLAN 1:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip ospf cost 20
```

ip ospf cost track

Use this command to sum the interface speeds contained in the specified tracked object when setting the OSPF interface cost.

Syntax

ip ospf cost track *trackobject-name*

no ip ospf cost track *trackobject-name*

Parameters

trackobject-name	Specifies the name of the tracked object containing the port names of interfaces to be summed to set the aggregate interface speed when calculating OSPF interface cost.

Defaults

None.

Mode

Configuration command, Interface configuration.

Usage

The formula for calculating the OSPF interface cost metric is the reference bandwidth divided by the interface bandwidth. By default the reference bandwidth is set to 100 Mbps. For logical interfaces containing multiple physical interfaces, such as a LAG, the aggregate interface speed is not readily available. A tracked object configured with the ports belonging to the logical interface can return the physical interface speed of each physical port specified in the tracked object. OSPF will sum the returned interface speeds and use that aggregate value when calculating OSPF interface cost.

Note: The speed used in the cost calculation is sum of all ports capabilities in the tracked object. Setting the speed manually will not change the tracked interface speed. A 1GB capable port has a 1 GB speed regardless of the manual speed setting. The same holds true for ports that auto-negotiate to a lower speed. The expectation is that both sides of the link are using the same ports and SFP connectors and should result in the same speed.

Because the tracked object will report when a physical interface is up or down, OSPF will dynamically adjust the aggregate speed when an interface becomes active or goes down and adjust the OSPF interface cost accordingly.

When adding an additional physical port to a logical interface that uses the interface summation method to determine OSPF interface cost, you must also add the physical port to the associated tracked object.

See "Tracked Object Commands" on page 22-24" for tracked object command details.

The "no" form of this command resets the OSPF cost to the value based upon the auto cost setting as set using "auto-cost reference-bandwidth" on page 73-30.

Example

This example shows how to set the OSPF interface cost for VLAN **1** using the summation method based upon ports configured in track object **ospfIntf1**:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip ospf cost track ospfIntf1
```

ip ospf network

Use this command to configure the IPv4 OSPF network link type.

Syntax

ip ospf network *type*

no ip ospf network *type*

Parameters

non-broadcast	Specifies this interface is a non-broadcast network link type.
broadcast	Specifies this interface is a broadcast network link type.
point-to-point	Specifies this interface is a point-to-point network link type.
point-to-multipoint	Specifies this interface is a point-to-point network link type.

Defaults

None.

Mode

Interface configuration.

Usage

The "no" form of this command removes .

Example

This example shows how to set the IPv4 OSPF interface link type to point-to-point:

```
S Chassis(su)->configure terminal
S Chassis(su-config)->interface vlan 15
S Chassis(su-config-intf-vlan.0.15)->ip ospf network point-to-point
```

ip ospf priority

Use this command to set the OSPF priority value for router interfaces.

Syntax

ip ospf priority *number*

no ip ospf priority

Parameters

number	Specifies the router's OSPF priority in a range from **0** to **255**.

Defaults

None.

Mode

OSPF router configuration.

Usage

The priority value is communicated between routers by means of hello messages and influences the election of a designated router.

The "no" form of this command resets the value to the default of 1.

Example

This example shows how to set the OSPF priority to 20 for VLAN 1:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip ospf priority 20
```

ip ospf poll-interval

Use this command to set a non-broadcast neighbor polling interval.

Syntax

ip ospf poll-interval *seconds*

no ip ospf poll-interval

Parameters

seconds	Specifies the number of seconds between polls for this non-broadcast neighbor. Valid Values: **0** - **4294967295**. Default: 120 seconds.

Defaults

None.

Mode

Interface configuration mode.

Usage

The polling interval sets the time between hello messages sent to this interface's neighbor.

The "no" form of this command resets the value to the default of 1.

Example

This example shows how to set the OSPF polling interval to 150 seconds for VLAN 1:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip ospf poll-interval 150
```

ip ospf retransmit-interval

Use this command to set the amount of time between retransmissions of link state advertisements (LSAs) for adjacencies that belong to an interface.

Syntax

ip ospf retransmit-interval *seconds*

no ip ospf retransmit-interval

Parameters

seconds	Specifies the retransmit time in seconds. Valid values are **1** to **3600**. Default: 5 Seconds.

Defaults

None.

Mode

OSPF router configuration.

Usage

The "no" form of this command resets the retransmit interval value to the default.

Example

This example shows how to set the OSPF retransmit interval for VLAN 1 to 20:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip ospf retransmit-interval 20
```

ip ospf transmit-delay

Use this command to set the amount of time required to transmit a link state update packet on an interface.

Syntax

ip ospf transmit-delay *seconds*

no ip ospf transmit-delay

Parameters

seconds	Specifies the transmit delay in seconds. Valid values are from **1** to **65535**. Default: **1** Second.

Defaults

None.

Mode

OSPF router configuration.

Usage

The “no” form of this command resets the transmit delay value to the default.

Example

This example shows how to set the time required to transmit a link state update packet on VLAN 1 at 20 seconds:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip ospf transmit-delay 20
```

ip ospf ignore-mtu

Use this command to ignore the MTU advertised by the neighbor.

Syntax

ip ospf ignore-mtu

no ip ospf ignore-mtu

Parameters

None.

Defaults

None.

Mode

Configuration command, Interface configuration.

Usage

If the interface MTU field in the Database Description (DBD) packet indicates an ip datagram size that is greater than the router can accept on the receiving side without fragmentation, the DBD packet is rejected. If the ignore MTU feature is enabled with this command, the DBD packet will not be rejected and will be processed instead.

The "no" form of this command disables the ignore MTU feature.

Example

This example shows how to enable the ignore MTU feature on this interface:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip ospf ignore-mtu
```

ip ospf hello-interval

Use this command to set the number of seconds a router must wait before sending a hello packet to neighbor routers on an interface.

Syntax

ip ospf hello-interval *seconds*

no ip ospf hello-interval

Parameters

seconds	Specifies the hello interval in seconds. Hello interval must be the same on neighboring routers (on a specific subnet), but can vary between subnets. This parameter is an unsigned integer with valid values between **1** and **65535**. Defaults: **10** seconds.

Defaults

None.

Mode

OSPF router configuration.

Usage

Each Extreme Networks S-Series routing module or Standalone device can support communications between up to 60 neighboring routers.

The "no" form of this command sets the hello interval value to the default.

Example

This example shows how to set the hello interval to 5 for VLAN 1:

```
S Chassis(rw-router-config)->interface vlan 1
S Chassis(rw-router-intf-Vlan-1)->ip ospf hello-interval 5
```

ip ospf dead-interval

Use this command to set the number of seconds a router must wait to receive a hello packet from its neighbor before determining that the neighbor is out of service.

Syntax

ip ospf dead-interval {*seconds* | **minimal** [**hello-multiplier** *number*]}

no ip ospf dead-interval

Parameters

seconds	Specifies the number of seconds that a router must wait to receive a hello packet. This parameter is an unsigned integer ranging from **1** to **65535**. Default: **40** Seconds.
minimal	Sets the dead-interval to 1 second for fast hello.
hello-multiplier *number*	(Optional) Specifies the number of hello-packets that will be sent in 1 second.

Defaults

If no parameter is specified, default values are assigned.

Mode

Configuration command, Interface configuration.

Usage

Dead interval must be the same on neighboring routers (on a specific subnet), but can vary between subnets.

The “no” form of this command sets the dead interval value to the default.

Example

This example shows how to set the dead interval to 20 for VLAN 1:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip ospf dead-interval 20
```

ip ospf authentication-key

Use this command to assign a password to be used by neighboring routers using OSPF's simple password authentication.

Syntax

ip ospf authentication-key *password*

no ip ospf authentication-key

Parameters

password	Specifies an OSPF authentication password. Valid values are alphanumeric strings up to 8 bytes in length.

Defaults

None.

Mode

Configuration command, Interface configuration.

Usage

All neighboring routers on the same network must have the same password configured to be able to exchange OSPF information.

This password is used as a "key" that is inserted directly into the OSPF header in routing protocol packets. A separate password can be assigned to each OSPF network on a per-interface basis.

The "no" form of this command removes an OSPF authentication password on an interface.

Example

This example shows how to enable an OSPF authentication key on VLAN 1 with the password "yourpass":

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip ospf authentication-key yourpass
```

ip ospf message-digest-key md5

Use this command to enable or disable OSPF MD5 authentication on an interface.

Syntax

ip ospf message-digest-key *keyid* **md5** *key*

no ip ospf message-digest-key *keyid*

Parameters

keyid	Specifies the key identifier on the interface where MD5 authentication is enabled. Valid values are integers from **1** to **255**.
key	Specifies a password for MD5 authentication to be used with the *keyid*. Valid values are alphanumeric strings of up to 16 bytes.

Defaults

None.

Mode

Configuration command, Interface configuration**.** Read-Write

Usage

This command validates OSPF MD5 routing updates between neighboring routers.

The “no” form of this command disables MD5 authentication on an interface.

Example

This example shows how to enable OSPF MD5 authentication on VLAN 1, set the key identifier to 20, and set the password to “passone”:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip ospf message-digest-key 20 md5 passone
```

ip ospf helper-disable

Use this command to disable the graceful restart helper function on this router interface.

Syntax

ip ospf helper-disable

no ip ospf helper-disable

Parameters

None.

Defaults

Helper mode enabled.

Mode

Configuration command, Interface configuration.

Usage

Each restarting router network segment functions as a helper by monitoring the network for topology changes. So long as the helper does not see an LSA change, it continues to advertise its LSAs as though the restarting router remained in continuous operation. This command disables this capability. For more information on the graceful restart helper function, see the *Extreme Networks S-Series Configuration Guide*.

The “no” form of this command enables graceful-restart helper mode for this router.

Example

This example shows how to disable the helper function on this router:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip ospf helper-disable
S Chassis(rw-config-intf-vlan.0.1)->
```

ip ospf network

Use this command to specify the network type for this interface.

Syntax

ip ospf network {**non-broadcast** | **broadcast** | **point-to-point** | **point-to-multipoint**}

no ip ospf network

Parameters

non-broadcast	Specifies this interface is connected to a non-broadcast network.
broadcast	Specifies this interface is connected to a broadcast network.
point-to-point	Specifies this interface is connected to a point-to-point network.
point-to-multipoint	Specifies this interface is connected to a point-to-multipoint network.

Defaults

None.

Mode

Configuration command, Interface configuration.

Usage

Broadcast is the default interface network type.

The “no” form of this command resets the network type for this interface to the default.

Example

This example shows how to specify that VLAN 1 is connected to a point-to-point network:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip ospf network point-to-point
S Chassis(rw-config-intf-vlan.0.1)->
```

show ip ospf

Use this command to display OSPF information.

Syntax

show ip ospf

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display OSPF information:

```
S Chassis(rw)->show ip ospf
Routing Process "ospf 20" with ID 134.141.7.2
Supports only single TOS(TOS0) route
It is an area border and autonomous system boundary router
Summary Link update interval is 0 seconds.
External Link update interval is 0 seconds.
Redistributing External Routes from,
Number of areas in this router is 3
Area BACKBONE (0)
    Number of interfaces in this area is 0
    Area has no authentication
    SPF algorithm executed 65 times
    Area ranges are

    Link State Update Interval is 00:30:00 and due in 00:03:12.
    Link State Age Interval is 00:00:00 and due in 00:00:00.

Area 0.0.0.3
    Number of interfaces in this area is 1
    Area has no authentication
    SPF algorithm executed 59 times
    Area ranges are

    Link State Update Interval is 00:30:00 and due in 00:02:28.
    Link State Age Interval is 00:00:00 and due in 00:00:00.

Area 0.0.0.2
    Number of interfaces in this area is 3
    Area has no authentication
    SPF algorithm executed 61 times
    Area ranges are
         140.20.0.0/255.255.0.0
```

```
Link State Update Interval is 00:30:00 and due in 00:03:07.
Link State Age Interval is 00:00:00 and due in 00:00:00.
```

show ip ospf database

Use this command to display the OSPF link state database.

Syntax

show ip ospf database *type* [*link-state-id*]

The options for using this syntax are:

show ip ospf database asbr-summary [*link-state-id*]

show ip ospf database database-summary

show ip ospf database external [*link-state-id*]

show ip ospf database network [*link-state-id*]

show ip ospf database nssa-external [*link-state-id*]

show ip ospf database router [*link-state-id*]

show ip ospf database summary [*link-state-id*]

Parameters

link-state-id	(Optional) Specifies the link state identifier. Valid values are IP addresses.
router	Displays router (Type 1) link state advertisements in their detailed format. Router advertisements are originated by all routers.
network	Displays network (Type 2) link state advertisements in their detailed format. Network advertisements are originated by designated routers.
summary	Displays summary (Type 3) link state advertisements in their original format. Summary advertisements are originated by ABRs.
asbr-summary	Displays Autonomous System Border Router (ASBR) summary (Type 4) link status advertisements in their detail format. ASBR-summary advertisements are originated by ABRs.
external	Displays external (Type 5) link state advertisements. Type 5 link state advertisements in their detailed format.
nssa-external	Displays nssa-external (Type 7) link state advertisements in their detailed format. Type 7 advertisements are originated by ASBRs.
database-summary	Displays a numerical summary of the contents of the link state database.

Defaults

If *link-state-id* is not specified, the specified type of database records will be displayed for all link state IDs.

Mode

All command modes.

Example

This example show how to display external OSPF database information for link-state ID 10.1.128.0:

```
S Chassis(rw)->show ip ospf database external 10.1.128.0
Displaying External Advertisements
LS age: 1461
Options: No TOS-capability
LS Type: AS External Links
Link State ID: 10.1.128.0
Advertising Router: 5.5.5.5
LS Seq Number: 80000004
Checksum: 0xb9a1
Length: 24
Network Mask: 255.255.128.0
Metric type 2 external (larger than any link state path)
TOS: 0 Metric: 20
Forwarding Address: 0.0.0.0
External Route Tag: 0
Number of TOS metrics: 0
S Chassis(rw)->
```

Table 73-1 provides an explanation of the command output.

Table 73-1 show ip ospf database Output Details

Output...	What it displays...
Advertising Router	Router ID of the router originating the link state record.
LS Age	Age (in seconds) of the link state record.
Options	Options associated with this link state record.
LS Type	Specifies the link state type for this link state record.
Link State ID	Link ID, which varies as a function of the link state record type, as follows: • Net Link States - Shows the interface IP address of the designated router to the broadcast network. • Router Link States - Shows the ID of the router originating the record. • Summary Link States - Shows the summary network prefix.
Advertising Router	Specifies the IP address of the router advertising this link state.
LS Seq Number	OSPF sequence number assigned to each link state record.
Checksum	Field in the link state record used to verify the contents upon receipt by another router.
Length	Link count of router link state records. This number is equal to, or greater than, the number of active OSPF interfaces on the originating router.
Network Mask	Specifies the network mask for this link state record.

Table 73-1 show ip ospf database Output Details (continued)

Output...	What it displays...
TOS	Specifies the Type of Service (ToS) configured for this link state record.
Metric	Specifies the ToS metric value.
Forwarding Address	Specifies the forwarding IP address associated with this link state record.
External Route Tag	Specifies the external route tag assigned to this link state record.
Number of TOS metrics	Specifies the number of ToS metrics associated with this link state record.

show ip ospf border-routers

Use this command to display information about Area Border Routers (ABRs) and Autonomous System Boundary Routers (ASBRs).

Syntax

```
show ip ospf border-routers
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display information about OSPF border routers:

```
S Chassis(rw)->show ip ospf border-routers
Area Border Routers:
  Area 0.0.0.0         Number of reachable:  1
                        192.168.200.1
  Area 0.0.0.1         Number of reachable:  2
                        192.168.200.1
                        192.168.201.10

Autonomous System Boundary Routers:
  Area 0.0.0.0         Number of reachable:  1
                        192.168.200.1
  Area 0.0.0.1         Number of reachable:  2
                        192.168.200.1
                        192.168.201.10
```

show ip ospf interface

Use this command to display OSPF interface related information, including network type, priority, cost, hello interval, and dead interval.

Syntax

show ip ospf [*process-id***] interface** [*ifName*]

Parameters

process-id	(Optional) Specifies a configured OSPF process by its process ID. If *process-id* is included, information for the specified routing process only is displayed.
ifName	(Optional) Displays OSPF information for an interface, such as a specific VLAN. The interface must be configured for IP routing as described in the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *ifName* is not specified, OSPF statistics are displayed for all interfaces (including all VLANs).

Mode

All command modes.

Example

This example shows how to display all OSPF related information for VLAN 1:

```
S Chassis(rw)->show ip ospf interface vlan1
Vlan  1 is UP
 Internet Address  182.127.63.2  Mask  255.255.255.0,Area 0.0.0.0
 Router ID 182.127.64.1,Network Type BROADCAST,Cost: 10
 Transmit Delay is 1 sec,State BACKUPDR,Priority 1
 Designated Router id 182.127.62.1, Interface addr 182.127.63.1
 Backup Designated Router id 182.127.63.2,
 Timer intervals configured, Hello 10,Dead 40,Wait 40,Retransmit 5
    Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 182.127.63.1 (Designated Router)
```

Table 73-2 provides an explanation of the command output.

Table 73-2 show ip ospf interface Output Details

Output...	What it displays...
Vlan	Interface (VLAN) administrative status as up or down.
Internet Address	IP address and mask assigned to this interface.
Router ID	Router ID, which OSPF selects from IP addresses configured on this router.
Network Type	OSPF network type, for instance, broadcast.
Cost	OSPF interface cost, which is either default, or assigned with the **ip ospf cost** command. For details, refer to “ip ospf cost” on page 73-32.
Transmit Delay	The number (in seconds) added to the LSA (Link State Advertisement) age field.

Table 73-2 show ip ospf interface Output Details (continued)

Output...	What it displays...
State	The interface state (versus the state between neighbors). Valid values include BACKUPDR (Backup Designated Router), and DR (Designated Router) and Drother.
Priority	The interface priority value, which is either default, or assigned with the **ip ospf priority** command. For details, refer to "ip ospf priority" on page 73-35.
Designated Router IP	The router IP of the designated router on this subnet, if one exists.
Backup Designated Router IP	IP address of the backup designated router on this interface, if one exists.
Timer intervals configured	OSPF timer intervals. These are either default, or configured with the **ip ospf retransmit-interval** ("ip ospf retransmit-interval" on page 73-36), the **ip ospf hello-interval** ("ip ospf hello-interval" on page 73-38), and the **ip ospf dead interval** ("ip ospf dead-interval" on page 73-39) commands. The wait timer represents the amount of time a router waits before initiating a designated router/backup designated router election. The wait timer changes when the dead interval changes. The retransmit timer represents the amount of time between successive transmissions of LSAs (Link State Advertisements) until acknowledgement is received.
Neighbor Count	Number of neighbors over this interface.
Adjacent neighbor count	Number of adjacent (FULL state) neighbors over this interface.
Adjacent with neighbor	IP address of the adjacent neighbor.

show ip ospf neighbor

Use this command to display the state of communication between an OSPF router and its neighbor routers.

Syntax

show ip ospf neighbor [**detail**] [*ip-address*] [**vlan** *vlan-id*]

Parameters

detail	(Optional) Displays detailed information about the neighbors, including the area in which they are neighbors, who the designated router/backup designated router is on the subnet, if applicable, and the decimal equivalent of the E-bit value from the hello packet options field.
ip-address	(Optional) Displays OSPF neighbors for a specific IP address.
vlan *vlan*-id	(Optional) Displays OSPF neighbors for a specific VLAN. This VLAN must be configured for IP routing as described in the *Extreme Networks S-Series Configuration Guide*.

Defaults

- If **detail** is not specified, summary information will be displayed.
- If *ip-address* is not specified, OSPF neighbors will be displayed for all IP addresses configured for routing.

- If *vlan-id* is not specified, OSPF neighbors will be displayed for all VLANs configured for routing.

Mode

All command modes.

Example

This example shows how to use the **show ip ospf neighbor** command:

```
S Chassis(rw)->show ip ospf neighbor
ID              Pri    State     Dead-Int  Address       Interface
182.127.62.1      1    FULL      40        182.127.63.1  vlan1
```

Table 73-3 provides an explanation of the command output.

Table 73-3 show ip ospf neighbor Output Details

Output...	What it displays...
ID	Neighbor's router ID of the OSPF neighbor.
Pri	Neighbor's priority over this interface.
State	Neighbor's OSPF communication state.
Dead-Int	Interval (in seconds) this router will wait without receiving a Hello packet from a neighbor before declaring the neighbor is down.
Address	Neighbor's IP address.
Interface	Neighbor's interface (VLAN).

show ip ospf sham-link

Use this command to display OSPF sham link configuration.

Syntax

show ip ospf sham-link

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to use the **show ip ospf sham-link** command:

```
S Chassis(rw)->show ip ospf sham-link
```

Table 73-4 provides an explanation of the command output.

Table 73-4 show ip ospf sham-link Details

Output...	What it displays...

show ip ospf virtual-links

Use this command to display information about the virtual links configured on a router.

Syntax

show ip ospf virtual-links

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

A virtual link represents a logical connection between the backbone and a non-backbone OSPF area.

Example

This example shows how to display OSPF virtual links information:

```
S Chassis(rw)->show ip ospf virtual-links
Virtual Link to router 5.5.5.1, is UP
Transmit Delay is 1 sec(s), State POINT-TO-POINT
 Timer intervals configured:
                Hello 10, Dead 40, Wait 40, Retransmit 5
 Adjacency State FULL
```

Table 73-5 provides an explanation of the command output.

Table 73-5 show ip ospf virtual links Output Details

Output...	What it displays...
Virtual Link	ID of the virtual link neighbor, and the virtual link status, which is up or down.
Cost of using	OSPF cost of routing through the virtual link.
Transmit Delay	Time (in seconds) added to the LSA (Link State Advertisement) age field when the LSA is transmitted through the virtual link.
State	Interface state assigned to a virtual link, which is point-to-point.
Timer intervals configured	Timer intervals configured for the virtual link, including Hello, Dead, Wait, and Retransmit intervals.
Adjacency State	State of adjacency between this router and the virtual link neighbor of this router.

show ip protocols

Use this command to display information about RIP and OSPF IP protocols running on the device.

Syntax

```
show ip protocols
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display IP protocol information:

```
S Chassis(rw)->show ip protocols

Routing Protocol is RIP
  Triggered Updates always
  Sending Updates every 30 seconds
  Invalid after 180 seconds
  Flush after 120 seconds
  Redistributing:
  Send and Receive version 2 only
                       Offset Offset
  Flag      Interface  In     Out    Key-chain
  -----     ---------- ---    ---    ----------
```

```
  Routing For Networks:
  Routing Information Sources:
  Distance: (default is 120)

Routing Protocol is OSPF
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing:  ospf 1
  Routing Information Sources:
199.113.113.0     0.0.0.255
```

clear ip ospf process

Use this command to reset the OSPF process.

Syntax

clear ip ospf process [*process-id*]

Parameters

process-id	(Optional) Specifies the process ID, an internally used identification number for each instance of the OSPF routing process run on a router. Valid values are **1** to **65535**.

Defaults

If the *process-id* is not specified, the OSPF process is reset.

Mode

All command modes.

Usage

This command will require adjacencies to be reestablished and routes to be reconverged.

Example

This example shows how to reset OSPF process 1:

```
S Chassis(rw)->clear ip ospf process 1
```

debug ip ospf

Use this command to enable OSPF protocol debugging output.

Syntax

debug ip ospf {*subsystem*}

no debug ip ospf {*subsystem*}

Parameters

subsystem	Specifies the OSPF subsystem for which protocol debugging will be enabled. Valid entries and their associated outputs are: • **adj** - OSPF adjacency events • **lsa-generation** - OSPF Link State Advertisement generation • **packet** - OSPF packets • **retransmission** - OSPF retransmission events

Defaults

None.

Mode

Configuration command.

Usage

The “no” form of this command disables OSPF protocol debugging output.

Example

This example shows how to enable OSPF protocol debugging output to display information about Link State Advertisement generation:

```
S Chassis(rw-config)->debug ip ospf lsa-generation
```

74

OSPFv3 Commands

This chapter describes the Open Shortest Path First Version 3 (OSPFv3) set of commands and how to use them. For information about configuring OSPF, refer to the "Open Shortest Path First Version 3 (OSPFv3) Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

Router OSPFv3 Configuration Commands

This section details commands for enabling and configuring router OSPFv3 configuration mode commands.

For information about...	Refer to page...
ipv6 router ospf	74-2
address-family ipv6	74-3
area default-cost	74-3
area nssa	74-4
area nssa-range	74-5
area range	74-6
area sham-link	74-6
area sham-link authentication-key	74-8
area sham-link dead-interval	74-9
area sham-link hello-interval	74-10
area sham-link keychain	74-11
area sham-link message-digest-key	74-11
area sham-link retransmit-interval	74-12
area sham-link transmit-delay	74-13
area sham-link cost	74-14
show ip ospf sham-link	74-15
area stub	74-16
area virtual-link	74-16
auto-cost reference-bandwidth	74-18
bfd all-intfs-on	74-19
distance (OSPF)	74-19

For information about...	Refer to page...
distribute-list route-map in	74-21
domain-id	74-21
enable-pe-ce	74-22
graceful-restart enable	74-23
graceful-restart restart-interval	74-24
log-adjacency	74-24
passive-interface	74-25
redistribute	74-26
router-id	74-27
spf lsa-thresholds	74-27
spf pause-frequency	74-28
timers spf	74-29

ipv6 router ospf

Use this command to enable or disable Open Shortest Path First Version 3 (OSPFv3) configuration mode.

Syntax

ipv6 router ospf *process-id*

no ipv6 router ospf *process-id*

Parameters

process-id	Specifies the process ID, an internally used identification number for an OSPF routing process run on a router. A single OSPFv3 process is configurable per router. Valid values are **1** to **65535**.

Defaults

None.

Mode

Configuration command.

Usage

You must execute the **ipv6 router ospf** command to enable the protocol before completing many OSPFv3-specific configuration tasks.

A single OSPFv3 process (*process-id*) is allowed per router.

The "no" form of this command disables OSPFv3 for the specified process.

Example

This example shows how to enable routing for OSPFv3 process 60:

```
S Chassis(rw)->configure
S Chassis(rw-config)->ipv6 router ospf 60
S Chassis(rw-config-ospfv3)->
```

address-family ipv6

This command enters IPv6 address family mode and configures unicast or multicast modes for this OSPFv3 process.

Syntax

address-family ipv6 [**unicast** | **multicast**]

no address-family ipv6 {**unicast** | **multicast**}

Parameters

unicast | **multicast**	(Optional) Specifies that IPv6 is configured for either unicast or multicast. The default value is unicast.

Defaults

IPv6 unicast is the default address-family mode for OSPFv3 IPv6.

Mode

OSPFv3 Router Configuration.

Usage

The **no address-family ipv6** command removes all topology configuration from this router configuration.

Example

The following example enters the IPv6 multicast address family configuration mode:

```
S Chassis(su-config-ospfv3)->address-family ipv6 multicast
S Chassis(su-config-ospfv3-af)->
```

The following example removes all topology configuration from this router configuration:

```
S Chassis(su-config-ospfv3)->no address-family ipv6
S Chassis(su-config-ospfv3)->
```

area default-cost

Use this command to set the summary cost value for the default route that is sent into a stub area by an Area Border Router (ABR).

Syntax

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

Parameters

area-id	Specifies the stub area. Valid values are decimal values **0** - **4294967295** or dotted-quad notation.
cost	Specifies a cost value for the summary route that is sent into a stub area by default. Valid values: **0** to **16777215**. Default value is **10**.

Defaults

None.

Mode

OSPFv3 router configuration.

Usage

The use of this command is restricted to ABRs attached to stub areas.

Use the **show ipv6 ospf interface** command to display the current area default cost.

The "no" form of this command removes the cost value from the summary route that is sent into the stub area.

Example

This example shows how to set the cost value for stub area **10** to **99**:

```
S Chassis(rw-config)->ipv6 router ospf 1
S Chassis(rw-config-ospfv3)->area 10 default-cost 99
```

area nssa

Use this command to configure an area as a Not-So-Stubby-Area (NSSA).

Syntax

area {*area-id | A.B.C.D*} **nssa** [**no-summary**] [**transstabilityint** *seconds*] [**transrole always**]

no area *area-id* **nssa** [**no-summary**] [**transstabilityint**][**transrole always**]

Parameters

*area-id	A.B.C.D*	Specifies the NSSA area. Valid values are decimal values **0** - **4294967295** or dotted-quad notation.
no-summary	(Optional) Prevents an Area Border Router (ABR) from sending type 3 summary Link State Advertisements (LSAs) into the NSSA area. When this parameter is used, it means that all destinations outside of the NSSA area are represented by means of a default route.
transstabilityint *seconds*	(Optional) Specifies the translator stability interval in seconds. Valid values: **0** - **65535**

transrole always	(Optional) Specifies that an NSSA router will unconditionally translate Type-7 LSAs to Type-5 LSAs when acting as an NSSA border router. Configuring the identity of the translator can be used to bias the routing to aggregated destinations. When translator role is set to **always**, Type-7 LSAs are always translated regardless of the translator state of other NSSA border routers.

Defaults

If **no-summary**, **transstabilityint** and **transrole always** are not specified, a default NSSA area is configured.

Mode

OSPFv3 router configuration.

Usage

An NSSA area allows some external routes represented by external Link State Advertisements (LSAs) to be imported into it. This is in contrast to a stub area that does not allow any external routes.

The "no" form of this command changes the NSSA back to a default area.

Example

This example shows how to configure area 10 as an NSSA area:

```
S Chassis(rw-config)->ipv6 router ospf 1
S Chassis(rw-config-ospfv3)->area 10 nssa
```

area nssa-range

Use this command to summarize Type 7 to Type 5 routes matching the specified address and mask length on an Autonomous System Border Router (ASBR) at an NSSA border.

Syntax

area {*area-id | A.B.C.D*} **nssa-range** *ipv6-address* [**not-advertise**]

no area {*area-id | ip-address*} **nssa-range** *ipv6-address* [**not-advertise**]

Parameters

*area-id	A.B.C.D*	Specifies the NSSA area. Valid values are decimal values **0** - **4294967295** or dotted-quad notation.
ipv6-address	Specifies the IPv6 address and mask length to match for this Type 7–>5 ASBR summarization.
not-advertised	(Optional) Specifies that the NSSA range is not advertised.

Defaults

If **not-advertised** is not specified, the specified NSSA range is advertised.

Mode

OSPFv3 router configuration.

Example

This example shows how to summarize area 10 Type 7 to Type 5 routes from IPv6 address **2001:FA04:0050::1/64**:

```
S Chassis(rw-config)->ipv6 router ospf 1
S Chassis(rw-config-ospfv3)->area 10 nssa-range 2001:FA04:0050::1/64
```

area range

Use this command to define the range of IPv6 addresses to be used by Area Border Routers (ABRs) when they communicate routes to other areas.

Syntax

area *area-id* **range** *ipv6-address* [**not-advertise**]

no area *area-id* **range** *ipv6-address* [**not-advertise**]

Parameters

area-id	Specifies the area at the boundary of which routes are to be summarized. Valid values are decimal values **0** - **4294967295** or dotted-quad notation.
ipv6-address	Specifies IPv6 address and mask of routes to be summarized at the boundary of the specified area. Used only by ABRs.
not-advertise	(Optional) Prevents advertisement of the specified IPv6 address range

Defaults

If **not-advertise** is not specified, the specified IPv6 address range is advertised.

Mode

OSPFv3 router configuration.

Usage

The “no” form of this command stops the routes from being summarized.

Example

This example shows how to define the address range as 2001:FA04:0005:0050::0/64 for summarized routes communicated at the boundary of area 0.0.0.0:

```
S Chassis(rw-config)->ipv6 router ospf 1
S Chassis(rw-config-ospfv3)->area 0.0.0.0 range 2001:FA04:0005:0050::0/64
```

area sham-link

Use this command to configure an OSPF sham link between two PE routers.

Syntax

area *area-id* **sham-link** *source-ipv6-address destination-ipv6-address*

no area *area-id* **sham-link** *source-ipv6-address destination-ipv6-address*

Parameters

area-id	Specifies the OSPF area the two PE routers belong to.
source-ipv6-address	Specifies the source IPv6 address for this sham link.
destination-ipv6-address	Specifies the destination IPv6 address for this sham link.

Defaults

If no sham link option is specified, the following defaults are used:

- authentication key - none
- dead-interval - 60 seconds
- hello-interval - 10 seconds
- keychain - none
- message-digest-key - none
- retransmit-delay - 5 seconds
- cost - reference bandwidth divided by the interface bandwidth

Mode

VRF configuration, OSPF router configuration.

Usage

If a VRF contains both an OSPF-distributed route and a VPN-IPv4 route for the same IPv4 prefix, then the backdoor OSPF-distributed route is preferred over the VPN backbone route, unless the next hop interface for an installed (OSPF distributed) route is the sham link, in which case, the VPN backbone VPN-IPv4 route is used.

If it is desired to have OSPF prefer the routes through the VPN backbone over the routes through the OSPF backdoor link, then the routes through the backbone must appear to be intra-area routes. The sham link provides this appearance of an intra-area link connecting the two PE routers.

The “no” form of this command deletes the configured sham link.

Example

This example shows how to configure a sham link between two PE routers with a source address of 2001:FA04:0005:0001::0 and a destination address of 2002:FA04:0005:0002::0 on OSPF router instance **10**, VRF **doc**:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->ipv6 router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->area 10 sham-link 2001:FA04:0005:0001::0
2002:FA04:0005:0002::0
```

area sham-link authentication-key

Use this command to configure the authentication key on an OSPF sham link.

Syntax

area *area-id* **sham-link** *source-ipv6-address destination-ipv6-address* **authentication-key** *password*

no area *area-id* **sham-link** *source-ipv6-address destination-ipv6-address* **authentication-key**

Parameters

area-id	Specifies the OSPF area the two PE routers belong to.
source-ipv6-address	Specifies the source IPv6 address for this sham link.
destination-ipv6-address	Specifies the destination IPv6 address for this sham link.
password	Specifies an OSPF authentication password. Valid values are alphanumeric strings up to 8 bytes in length.

Defaults

None.

Mode

VRF configuration, OSPF router configuration.

Usage

All neighboring routers on the same network must have the same password configured to be able to exchange OSPF information.

This password is used as a “key” that is inserted directly into the OSPF header in routing protocol packets. A separate password can be assigned to each sham link.

The “no” form of this command deletes the configured sham link authentication key.

Example

This example shows how to configure a sham link between two PE routers with a source address of 2001:FA04:0005:0001::0 and a destination address of 2002:FA04:0005:0002::0 on OSPF router instance **10**, VRF **doc** and assign an authentication key of **yourpass**:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->ipv6 router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->area 10 sham-link 2001:FA04:0005:0001::0
2002:FA04:0005:0002::0 authentication-key yourpass
```

area sham-link dead-interval

Use this command to configure the dead interval for an OSPF sham link.

Syntax

area *area-id* **sham-link** *source-ipv6-address destination-ipv6-address* **dead-interval** *seconds*

no area *area-id* **sham-link** *source-ipv6-address destination-ipv6-address* **dead-interval**

Parameters

area-id	Specifies the OSPF area the two PE routers belong to.
source-ipv6-address	Specifies the source IPv6 address for this sham link.
destination-ipv6-address	Specifies the destination IPv6 address for this sham link.
seconds	(Optional) Specifies the number of seconds that the hello packets of a router are not communicated to neighbor routers before the neighbor routers determine that the router sending the hello packet is out of service. This value must be the same for all nodes attached to a certain subnet, and it is a value ranging from **1** to **2147843647**. The default value is **60** seconds.

Defaults

The dead interval defaults to 60 seconds.

Mode

VRF configuration, OSPF router configuration.

Usage

Dead interval must be the same on neighboring routers (on a specific subnet), but can vary between subnets.

The “no” form of this command resets the sham link dead interval to 10 seconds.

Example

This example shows how to configure a sham link dead interval to **80** seconds between two PE routers with a source address of 2001:FA04:0005:0001::0 and a destination address of 2002:FA04:0005:0002::0 on OSPF router instance **10**, VRF **doc**:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->ipv6 router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->area 10 sham-link 2001:FA04:0005:0001::0
2002:FA04:0005:0002::0 dead-interval 80
```

area sham-link hello-interval

Use this command to configure the hello interval for an OSPF sham link.

Syntax

area *area-id* **sham-link** *source-ipv6-address destination-ipv6-address* **hello-interval** *seconds*

no area *area-id* **sham-link** *source-ipv6-address destination-ipv6-address* **hello-interval**

Parameters

area-id	Specifies the OSPF area the two PE routers belong to.
source-ipv6-address	Specifies the source IPv6 address for this sham link.
destination-ipv6-address	Specifies the destination IPv6 address for this sham link.
seconds	(Optional) Specifies the number of seconds between hello packets on an interface. Valid values range from **1** to **65535**. The default value is **10** seconds.

Defaults

The hello interval defaults to 10 seconds.

Mode

VRF configuration, OSPF router configuration.

Usage

This value must be the same for all nodes attached to a network. By default, hello packets are sent out every 10 seconds. If after 40 seconds, there is no response on the interface, the interface will be shutdown.

The “no” form of this command resets the hello interval to the default value for this sham link.

Example

This example shows how to configure the hello interval to **15** seconds for a sham link between two PE routers with a source address of 2001:FA04:0005:0001::0 and a destination address of 2002:FA04:0005:0002::0 on OSPF router instance **10**, VRF **doc**:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->ipv6 router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->area 10 sham-link 2001:FA04:0005:0001::0
2002:FA04:0005:0002::0 hello-interval 15
```

area sham-link keychain

Use this command to configure an MD5 keychain for this sham link.

Syntax

area *area-id* **sham-link** *source-ipv6-address destination-ipv6-address* **keychain** *name*

no area *area-id* **sham-link** *source-ipv6-address destination-ipv6-address* **keychain**

Parameters

area-id	Specifies the OSPF area the two PE routers belong to.
source-ipv6-address	Specifies the source IPv6 address for this sham link.
destination-ipv6-address	Specifies the destination IPv6 address for this sham link.
name	Specifies the name of the OSPF keychain that holds MD5 keys.

Defaults

None.

Mode

VRF configuration, OSPF router configuration.

Usage

The “no” form of this command removes the current keychain from the sham link.

Example

This example shows how to configure keychain **keychain1** to a sham link between two PE routers with a source address of 2001:FA04:0005:0001::0 and a destination address of 2002:FA04:0005:0002::0 on OSPF router instance **10**, VRF **doc**:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->ipv6 router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->area 10 sham-link 2001:FA04:0005:0001::0
2002:FA04:0005:0002::0 keychain keychain1
```

area sham-link message-digest-key

Use this command to configure a message digest key for an OSPF sham link.

Syntax

area *area-id* **sham-link** *source-ipv6-address destination-ipv6-address*
message-digest-key *digest-key* **md5** *auth-key*

no area *area-id* **sham-link** *source-ipv6-address destination-ipv6-address*
message-digest-key *digest-key*

Parameters

area-id	Specifies the OSPF area the two PE routers belong to.
source-ipv6-address	Specifies the source IPv6 address for this sham link.
destination-ipv6-address	Specifies the destination IPv6 address for this sham link.
message-digest-key *digest-key* **md5** *auth-key*	(Optional) Specifies the message digest key settings: • *digest-key* - Specifies the key identifier on the interface where MD5 authentication is enabled in a value range from **1** - **255**. • *auth-key* - Specifies a password for MD5 authentication to be used with the *digest-key*. Valid values are alphanumeric strings of up to 16 bytes.

Defaults

None.

Mode

VRF configuration, OSPF router configuration.

Usage

This command validates OSPF MD5 routing updates between neighboring routers.

The “no” form of this command removes the message digest key configuration from the sham link.

Example

This example shows how to enable OSPF MD5 authentication on a sham link between two PE routers with a source address of 2001:FA04:0005:0001::0 and a destination address of 2002:FA04:0005:0002::0 on OSPF router instance **10**, VRF **doc**, set the key identifier to **20**, and set the password to **passone**:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->ipv6 router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->area 10 sham-link 2001:FA04:0005:0001::0
2002:FA04:0005:0002::0 message-digest-key 20 md5 passone
```

area sham-link retransmit-interval

Use this command to configure the retransmit interval for an OSPF sham link.

Syntax

area *area-id* **sham-link** *source-ipv6-address destination-ipv6-address* **retransmit-interval** *seconds*

no area *area-id* **sham-link** *source-ipv6-address destination-ipv6-address* **retransmit-interval**

Parameters

area-id	Specifies the OSPF area the two PE routers belong to.
source-ipv6-address	Specifies the source IPv6 address for this sham link.
destination-ipv6-address	Specifies the destination IPv6 address for this sham link.
seconds	(Optional) Specifies the number of seconds between successive retransmissions of the same LSAs. Valid values are greater than the expected amount of time required for the update packet to reach and return from the interface, and range from **1** to **3600**. The default value is **5** seconds.

Defaults

The sham link retransmit interval defaults to **5** seconds.

Mode

VRF configuration, OSPF router configuration.

Usage

The "no" form of this command resets the sham link retransmit interval value to the default value.

Example

This example shows how to configure retransmit interval to 10 for a sham link between two PE routers with a source address of 2001:FA04:0005:0001::0 and a destination address of 2002:FA04:0005:0002::0 on OSPF router instance **10**, VRF **doc**:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->ipv6 router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->area 10 sham-link 2001:FA04:0005:0001::0
2002:FA04:0005:0002::0 retransmit-interval 10
```

area sham-link transmit-delay

Use this command to configure a transmit delay period for an OSPF sham link.

Syntax

area *area-id* **sham-link** *source-ipv6-address destination-ipv6-address* **transmit-delay** *seconds*

no area *area-id* **sham-link** *source-ipv6-address destination-ipv6-address* **transmit-delay**

Parameters

area-id	Specifies the OSPF area the two PE routers belong to.
source-ipv6-address	Specifies the source IPv6 address for this sham link.
destination-ipv6-address	Specifies the destination IPv6 address for this sham link.

seconds	(Optional) Specifies the estimated number of seconds for a link state update packet on the interface to be transmitted. Valid values range from **1** to **3600**. The default value is **1** second.

Defaults

The sham link transmit delay period defaults to **1** second.

Mode

VRF configuration, OSPF router configuration.

Usage

The "no" form of this command resets the sham link transmit delay value to the default.

Example

This example shows how to configure a transmit delay period of 5 seconds for the sham link between two PE routers with a source address of 2001:FA04:0005:0001::0 and a destination address of 2002:FA04:0005:0002::0 on OSPF router instance **10**, VRF **doc**:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->ipv6 router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->area 10 sham-link 2001:FA04:0005:0001::0
2002:FA04:0005:0002::0 transmit-delay 5
```

area sham-link cost

Use this command to configure the cost of an OSPF sham link.

Syntax

area *area-id* **sham-link** *source-ipv6-address destination-ipv6-address* **cost** *cost*

no area *area-id* **sham-link** *source-ipv6-address destination-ipv6-address* **cost**

Parameters

area-id	Specifies the OSPF area the two PE routers belong to.
source-ipv6-address	Specifies the source IPv6 address for this sham link.
destination-ipv6-address	Specifies the destination IPv6 address for this sham link.
cost	Specifies the cost of the sham link. Valid values are **1** - **65535**. The default value is the reference bandwidth divided by the interface bandwidth.

Defaults

The cost of the sham link defaults to the reference bandwidth divided by the interface bandwidth.

Mode

VRF configuration, OSPF router configuration.

Usage

Each router interface that participates in OSPF routing is assigned a default cost. This command overwrites the default OSPF interface cost.

The reference bandwidth defaults to 100Mbps and can be modified using "auto-cost reference-bandwidth" on page 74-18.

The "no" form of this command resets the OSPF cost for the sham link to the default of 10.

Example

This example shows how to configure a cost of 20 for the sham link between two PE routers with a source address of 2001:FA04:0005:0001::0 and a destination address of 2002:FA04:0005:0002::0 on OSPF router instance **10**, VRF **doc**:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->ipv6 router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->area 10 sham-link 2001:FA04:0005:0001::0
2002:FA04:0005:0002::0 cost 20
```

show ip ospf sham-link

Use this command to display OSPF sham link configuration.

Syntax

show ip ospf sham-link

Parameters

None.

Defaults

None.

Mode

All command modes**.**

Example

This example shows how to use the **show ip ospf sham-link** command:

```
S Chassis(rw)->show ip ospf sham-link
```

Table 74-1 provides an explanation of the command output.

Table 74-1 show ip ospf sham-link Details

Output...	What it displays...

Table 74-1 show ip ospf sham-link Details

Output...	What it displays...

area stub

Use this command to define an OSPF area as a stub area.

Syntax

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub** [**no-summary**]

Parameters

area-id	Specifies the stub area. Valid values are decimal values **0** - **4294967295** or dotted-quad notation.
no-summary	(Optional) Prevents an Area Border Router (ABR) from sending type 3 summary Link State Advertisements (LSAs) into the stub area. When this parameter is used, it means that all destinations outside of the stub area are represented by means of a default route.

Defaults

If **no-summary** is not specified, the stub area will be able to receive LSAs.

Mode

OSPFv3 router configuration.

Usage

This is an area that carries no external routes.

The "no" form of this command changes the stub back to a plain area.

Example

The following example shows how to define OSPF area 10 as a stub area:

```
S Chassis(rw-config)->ipv6 router ospf 1
S Chassis(rw-config-ospfv3)->area 10 stub
```

area virtual-link

Use this command to define an OSPF virtual link, which represents a logical connection between the backbone and a non-backbone OSPF area.

Syntax

area *area-id* **virtual-link** *router-id* {**dead-interval** *seconds* | **hello-interval** *seconds* | **retransmit-interval** *seconds* | **transmit-delay** *seconds* | **dead-interval**

seconds | **hello-interval** *seconds* | **retransmit-interval** *seconds* | **transmit-delay** *seconds*}

Parameters

area-id	Specifies the transit area for the virtual link. A transit area is an area through which a virtual link is established. Valid values are decimal values **0** - **4294967295** or dotted-quad notation.
router-id	Specifies the router ID of the virtual link neighbor in dotted-quad notation. A virtual link is established through the transit area to the virtual link neighbor.
dead-interval *seconds*	(Optional) Specifies the number of seconds that the hello packets of a router are not communicated to neighbor routers before the neighbor routers determine that the router sending the hello packet is out of service. This value must be the same for all nodes attached to a certain subnet, and it is a value ranging from **1** to **65535**. The default value is **40** seconds.
hello-interval *seconds*	(Optional) Specifies the number of seconds between hello packets on an interface. This value must be the same for all nodes attached to a network and it is a value ranging from **1** to **65535**. The default value is **10** seconds (broadcast) and **30** seconds (non-broadcast and point-to-multipoint).
retransmit-interval *seconds*	(Optional) Specifies the number of seconds between successive retransmissions of the same LSAs. Valid values are greater than the expected amount of time required for the update packet to reach and return from the interface, and range from **1** to **3600**. The default value is **5** seconds.
transmit-delay *seconds*	(Optional) Specifies the estimated number of seconds for a link state update packet on the interface to be transmitted. Valid values range from **1** to **3600**. The default value is **1** second.

Defaults

If no optional values are specified, optional values remain unchanged from current values.

Mode

OSPFv3 router configuration.

Usage

The “no” form of this command removes the virtual link if only the area ID and router ID are specified. If an optional parameter is specified, that option is reset to its default value.

Example

This example shows how to configure a virtual link between a router in OSPF area 0.0.0.2 and the ABR 1.1.1.1:

```
S Chassis(rw-config)->ipv6 router ospf 1
S Chassis(rw-config-ospfv3)->area 0.0.0.2 virtual-link 1.1.1.1
```

auto-cost reference-bandwidth

Use this command to configure an OSPF auto cost reference bandwidth for this OSPFv3 instance.

Syntax

auto-cost reference-bandwidth *bandwidth-multiplier*

no auto-cost reference-bandwidth *bandwidth-multiplier*

Parameters

bandwidth-multiplier	Specifies the auto cost bandwidth multiplier in megabits per second for this OSPFv3 instance. Valid values are **1** - **4294967**. The default value is **100**.

Defaults

None.

Mode

OSPFv3 router configuration.

Usage

The formula for calculating the OSPF interface cost metric is the reference bandwidth divided by the interface bandwidth. By default the reference bandwidth is set to 100 Mbps. For 10 Mbps links, the resulting cost is 10. For 100, 1000, or 10000 Mbps links, the resulting cost is 1. The ability to re-center the reference bandwidth to a higher value, allows for OSPF interface costs to default to a value greater than 1 for 100, 1000, or 10000 Mbps links and greater than 10 for 10 Mbps links.

It is recommended that the auto cost reference bandwidth be the same value for all OSPF routers in the domain.

The OSPF interface cost can be statically set or determined using the interface speed summoning method with tracked objects using “ipv6 ospf cost” on page 74-34.

The “no” form of this command resets the auto cost reference bandwidth to 100 Mbps for this OSPFv3 instance.

Example

This example shows how to configure the auto cost reference bandwidth to 1Gbps for OSPFv3 instance 10:

```
S Chassis(su)->configure
S Chassis(su-config)->ipv6 router ospf 10
S Chassis(su-config-ospfv3)->auto-cost reference-bandwidth 1000
S Chassis(su-config-ospfv3)->
```

bfd all-intfs-on

Use this command to enable the Bidirectional Forwarding Detection (BFD) protocol on all OSPF interfaces.

Syntax

bfd all-intfs-on

no bfd all-intfs-on

Parameters

None.

Defaults

The BFD protocol is enabled on all OSPF interfaces by default.

Mode

OSPF router configuration.

Usage

BFD is used to detect a communications failure with an OSPF forwarding plane next-hop. BFD detects failures in under one second. BFD augments the OSPF Hello mechanism. The OSPF Hello interval defaults to 10 seconds. With high speed data rates, a failure requiring multiple seconds to detect can result in significant data loss. The OSPF implementation of the BFD protocol uses the following non-configurable parameters:

Transmit Interval – The period of time between the transmission of BFD control packets, set for 100ms.

Receive Interval – The period of time between received BFD control packets, set for 100ms.

Detection Multiplier – The Number of consecutive control packets that can be missed before the BFD session transitions to down, set to 3.

The “no” form of this command disables the BFD protocol on all OSPF interfaces.

Example

This example shows how to disable the BFD protocol on all OSPF interfaces for OSPF instance 1:

```
S Chassis(rw-config)->router ospf 1
S Chassis(rw-config-ospf-1)->no bfd all-intfs-on
```

distance (OSPF)

Use this command to configure the administrative distance for OSPFv3 routes.

Syntax

distance [**ospf** {**external** | **intra-area**}] *weight*

no distance [**ospf** {**external** | **intra-area**}]

Parameters

ospf external | intra-area	(Optional) Applies the specified distance value to external (type 5 and type 7) or to intra-area routes. **Note:** The value for intra-area distance must be less than or equal to the value for external distance.
weight	Specifies an administrative distance for OSPF routes. Valid values are **1**-**255**. Default: **110**.

Defaults

If route type is not specified using the **ospf** option, the distance value specified will be applied to all OSPF routes.

Mode

OSPFv3 router configuration.

Usage

If several routes (coming from different protocols) are presented to the Extreme Networks S-Series Route Table Manager (RTM), the protocol with the lowest administrative distance will be chosen for route installation. The distance for inter-area routes is fixed at **110**. By default, OSPF administrative distance is set to **110** for all OSPF routes. The **distance** command can be used to change this value, resetting OSPF's route preference in relation to other routes as shown in the table below.

Route Source	Default Distance
Connected	0
Static	1
BGP	20 - Routes external to the AS 200 - Routes internal to the AS
OSPF	110
RIP	120
Unknown (The router will not use the route)	255

The **distance** command applies the value to the specified route type.

The "no" form of this command resets OSPF administrative distance to the default value of 110.

Example

This example shows how to change the default administrative distance for external OSPF routes to 100:

```
S Chassis(rw-config)->ipv6 router ospf 1
S Chassis(rw-config-ospfv3)->distance ospf external 100
```

distribute-list route-map in

Use this command to assign an OSPFv3 route filter route-map assigned to the distribute-list for the purpose of filtering routes being installed into the route table.

Syntax

distribute-list route-map *name* **in**

no distribute-list route-map *name* **in**

Parameters

name	Specifies the OSPFv3 route filter route-map to associate with this distribute-list.

Defaults

None.

Mode

OSPFv3 router configuration.

Usage

See "Filter-Based Route-Map Commands" on page 85-24 for a detailed discussion of OSPFv3 filter-based route-map commands.

The "no" form of this command clears the specified route-map from the distribute-list.

Example

This example shows how to configure the OSPFv3 redistribution route map for ACLs 3, 6, 11, 14, and 15 and assign the ospf1 filter route-map to the distribute-list for this OSPFv3 router:

```
S Chassis(rw-config)->route-map redistribution ospf1
S Chassis(rw-config-route-map)->match ipv6 address 3 6 11 14 15
S Chassis(rw-config-route-map)->exit
S Chassis(rw-config)->ipv6 router ospf 1
S Chassis(rw-config-ospfv3)->distribute-list route-map ospf1 in
```

domain-id

Use this command to specify an OSPF VPN routing and forwarding (VRF) domain ID.

Syntax

domain-id type *type* **value** *value* [**secondary**]

no domain-id type *type* **value** *value* [**secondary**]

Parameters

type *type*	Specifies an OSPF VRF domain ID type. Valid values are **0005** | **0105** | **0205** | **8005**.
value *value*	Specifies an OSPF VRF domain ID value. Valid values are six octets in hex format (up to 12 hex characters). Default value is **0**.

secondary	(Optional) Specifies an OSPF secondary domain ID

Defaults

- The OSPF VRF domain ID type defaults to **0005**
- The OSPF VRF domain ID default value is **0**.

Mode

VRF configuration, OSPFv3 router configuration.

Usage

If the OSPF instances of an OSPF domain are given one or more domain IDs, OSPF can determine whether an OSPF-originated VPN-IPv6 route belongs to the same domain as a given OSPF instance and whether the route should be redistributed to that OSPF instance as an inter-area route or as an OSPF AS-external route.

If two OSPF instances with a domain ID configured are in the same OSPF domain, the PE-CE protocol requires that the primary domain ID of each instance must be one its own domain IDs (either primary or secondary). If two OSPF instances with a domain ID configured are not in the same OSPF domain, the primary domain ID of each instance must not be configured as a domain ID of the other OSPF instance.

The PE-CE protocol (RFC 6565) must be enabled using "enable-pe-ce" on page 74-22 to set the OSPF VRF domain ID.

The "no" form of this command restores the default domain ID type to **0005** and value to **0**.

Example

This example shows how to set the OSPF VRF primary domain ID type to **0105** and value to **100** for VRF **doc**:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->domain-id type 0105 100
```

enable-pe-ce

Use this command to enable the Customer Edge (CE) routers as Provider Edge (PE) router peers.

Syntax

enable-pe-ce

no enable-pe-ce

Parameters

None.

Defaults

CE routers are disabled as PE router peers by default.

Mode

VRF configuration, OSPFv3 router configuration.

Usage

Enabling CE routers as PE router peers is defined in RFC 6565.

The “no” form of this command disables CE routers as PE router peers for this device.

Example

This example enables CE routers as PE router routing peers for this device:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->router ospf 10
S Chassis(su-doc-config-ospf-10)->enable-pe-ce
S Chassis(su-doc-config-ospf-10)->
```

graceful-restart enable

Use this command to enable the graceful restart ability on this router.

Syntax

graceful-restart enable

no graceful-restart enable

Parameters

None.

Defaults

None.

Mode

OSPFv3 router configuration.

Usage

Graceful restart allows this router to stay on the forwarding path during a failover. For more information about graceful restart, see the *Extreme Networks S-Series Configuration Guide*.

The Version 2 and 3 graceful restart stacks are completely separate. If you wish to enable graceful restart for both OSPFv2 and OSPFv3, you must enable both in the correct OSPF version configuration mode.

The “no” form of this command disables graceful restart for this router.

Example

This example shows how to enable the graceful restart ability on this router for OSPFv3:

```
S Chassis(rw-config)->ipv6 router ospf 1
S Chassis(rw-config-ospfv3)->graceful-restart enable
S Chassis(rw-config-ospfv3)->
```

graceful-restart restart-interval

Use this command to set the graceful restart restart interval.

Syntax

graceful-restart restart-interval *interval*

no graceful-restart restart-interval *interval*

Parameters

interval	Specifies the maximum amount of time in seconds that this router will remain in graceful restart mode starting at the time it enters graceful restart. Valid values are **1** - **1800** seconds. Default value is **120** seconds.

Defaults

None.

Mode

OSPFv3 router configuration.

Usage

The restart interval sets the maximum amount of time that this router will remain in graceful restart once an OSPF restart is initiated.

The “no” form of this command resets the graceful restart restart-interval to its default value.

Example

This example sets the graceful restart restart-interval to 300 seconds:

```
S Chassis(rw-config)->ipv6 router ospf 1
S Chassis(rw-config-ospfv3)->graceful-restart enable
S Chassis(rw-config-ospfv3)->graceful-restart restart-interval 300
```

log-adjacency

Use this command to enable or disable adjacency logging on this OSPFv3 router.

Syntax

log-adjacency

no log-adjacency

Parameters

None.

Defaults

None.

Mode

OSPFv3 router configuration.

Usage

The “no” form of this command disables adjacency logging for this OSPFv3 router.

Example

This example shows how to enable adjacency logging on the OSPFv3 process 1:

```
S Chassis(rw)->configure
S Chassis(rw-config)->ipv6 router ospf 1
S Chassis(rw-config-ospfv3)->log-adjacency
```

passive-interface

Use this command to enable passive OSPFv3 on an interface.

Syntax

passive-interface {*vlan-id* | *interface-name* | **default**}

no passive-interface {*vlan-id* | *interface-name* | **default**}

Parameters

vlan-id	Specifies the VLAN number on which to enable passive OSPF mode.
interface-name	Specifies a VLAN in the interface-name format: vlan.*x*.*y*
default	Sets all enabled OSPF interfaces to passive.

Defaults

None.

Mode

OSPFv3 router configuration.

Usage

The passive interface feature allows an interface to be included in the OSPFv3 route table, but turns off sending and receiving hellos for the specified interface. It also prevents OSPFv3 adjacencies from being formed on the specified interface.

The “no” form of this command disables passive OSPFv3 interface mode.

Example

This example shows how to enable passive OSPFv3 mode on VLAN 102 (can be specified as **vlan 102** or **vlan.0.102**):

```
S Chassis(rw-config)ipv6 router ospf 1
S Chassis(rw-config-ospfv3)->passive-interface vlan 102
```

redistribute

Use this command to allow routing information discovered through non-OSPFv3 protocols to be distributed in OSPFv3 update messages.

Syntax

redistribute {**bgp** [global]| **connected** | **rip** | **static** | **blackhole**} [**route-map** *name*] [**metric** *metric-value*] [**metric-type** *type-value*] [**tag** *tag*]

no redistribute {**bgp** | **connected** | **rip** | **static** | **blackhole**} [**route-map** *name*] [**metric** *metric-value*] [**metric-type** *type-value*] [**tag** *tag*]

Parameters

bgp	Specifies that BGP routing information will be redistributed in OSPFv3.
global	(Optional) Specifies that BGP prefixes from the global router are redistributed. VPN4-address prefixes are translated appropriately.
connected	Specifies that non-OSPFv3 information discovered via directly connected interfaces will be redistributed.
rip	Specifies that RIP routing information will be redistributed in OSPFv3.
static	Specifies that non-OSPFv3 information discovered via static routes will be redistributed. Static routes are those created using the **ipv6 route** command detailed in "ipv6 route" on page 56-7.
blackhole	Specifies that blackhole routes will be redistributed in OSPFv3.
metric *metric-value*	(Optional) Specifies a metric for the redistribution route. This value should be consistent with the designation protocol.
metric-type *type-value*	(Optional) Specifies the external link type associated with the route advertised into the OSPFv3 routing domain. Valid values are **1** for type 1 external route, and **2** for type 2 external route.
route-map *name*	(Optional) Redistributes routes using the rules established by the designated route-map.
tag *tag*	(Optional) Specifies the tag for routes redistributed in OSPFv3.

Defaults

- If global is not specified, routes associated with the VRF BGP instance are redistributed.
- If *metric-value* is not specified, **20** will be applied.
- If *type-value* is not specified, type 2 (external route) will be applied.
- If **route-map** is not specified, none will be applied.
- If **tag** is not specified, none will be applied.

Mode

OSPFv3 router configuration.

Usage

The "no" form of this command clears redistribution parameters.

Example

This example shows how to distribute external type 2 RIP routing information from routes in OSPFv3 updates:

```
S Chassis(rw-config)->ipv6 router ospf 1
S Chassis(rw-config-ospfv3)->redistribute rip
```

router-id

Use this command to set the OSPFv3 router ID for the device.

Syntax

router-id *router-id*

Parameters

router-id	Specifies the OSPFv3 router ID expressed as a 32-bit integer in dotted-quad notation.

Defaults

None.

Mode

OSPFv3 router configuration.

Usage

The OSPFv3 protocol uses the router ID as a tie-breaker for path selection and as the OSPFv3 neighbor ID. If no router ID is configured, then the OSPFv3 router ID is set to the highest loopback address configured. If no loopback address is configured, then the highest IP address configured will be used. If no IP addresses are configured, then OSPFv3 will not enable.

Example

This example shows how to set the OSPFv3 router ID to 182.127.62.1:

```
S Chassis(rw-config-ospfv3)->router-id 182.127.62.1
```

spf lsa-thresholds

Use this command to specify thresholds for the the number of Shortest Path First (SPF) LSA updates that force or restart a full routing calculation.

Syntax

spf lsa-thresholds *num-start num-restart num-intra-full num-ia-ext-full*

no lsa-thresholds

Parameters

num-start	Specifies the number of LSA updates that force a full routing calculation. Valid values: **0** - **4294967295**; Default: **4294967295**.

num-restart	Specifies the number of LSA updates that interrupt and restart a full routing calculation. Valid values: **0** - **4294967295**; Default: **4294967295**.
num-ia-ext-full	Specifies the number of LSA inter-area/external updates that force a full routing calculation. Valid values: **0** - **4294967295**; Default: **50**.
num-intra-full	Specifies the number of intra updates that force a full routing calculation. Valid values: **0** - **4294967295**; Default: **0**.

Defaults

None.

Mode

OSPFv3 router configuration.

Usage

The "no" form of this command restores the default values.

A value of **0** for either the number of LSA inter-area, external updates, or intra-area updates means a full routing calculation would always be done for any inter-area, external, or intra-area update received.

Example

This example shows how to change the number of LSA inter-area/external updates that force a full routing calculation to 75 leaving the remaining defaults unchanged:

```
S Chassis(rw-config)->ipv6 router ospf 1
S Chassis(rw-config-ospfv3)->spf lsa-thresholds 4294967295 4294967295 75 0
S Chassis(rw-config-ospfv3)->
```

spf pause-frequency

Use this command to specify the number of units of CPU credits an SPF calculation runs before pausing.

Syntax

spf pause-frequency *units*

no pause-frequency

Parameters

units	Specifies the number of units of CPU credit an SPF calculation runs before pausing. Entering **0** specifies the SPF calculation does not pause until it is completed. Valid values: **0** - **4294967295**; Default: **10000**.

Defaults

None.

Mode

OSPFv3 router configuration.

Usage

The SPF algorithm is a method of calculating the best path to all known destinations based on the information in its link state database. A CPU credit is a unit of processing controlled by the operating system. After the SPF calculation has run the configured number of CPU credits, the SPF process will pause allowing other active processes a share of CPU time. The SPF calculation will start up again after all other active processes have used up their allotted credits. Increasing this value will allow a faster completion of an SPF calculation at the expense of all other active processes.

Entering **0** specifies the SPF calculation does not pause until it is completed.

The "no" form of this command restores the default values.

Example

This example shows how to set the SPF pause frequency setting to 12000 units:

```
S Chassis(rw-config)->ipv6 router ospf 1
S Chassis(rw-config-ospfv3)->spf pause-frequency 12000
```

timers spf

Use this command to change delay between the receipt of an update and the SPF execution.

Syntax

timers spf *spf-delay*

no timers spf

Parameters

spf-delay	Specifies the delay, in milli-seconds, between the receipt of an update and the SPF execution. Valid values are **0** to **4294967295** milli-seconds. The default value is **5** seconds (**5000** milli-seconds). The value is entered in milli-seconds.

Defaults

None.

Mode

OSPFv3 router configuration.

Usage

The "no" form of this command restores the default timer values.

Example

This example shows how to set spf delay time to 7 seconds:

```
S Chassis(rw-config)->ipv6 router ospf 1
S Chassis(rw-config-ospfv3)->timers spf 7000
```

OSPFv3 Interface Commands

This section details OSPFv3 commands entered in interface configuration mode.

For information about...	Refer to page...
ipv6 ospf	74-30
ipv6 ospf authentication	74-31
ipv6 ospf encryption	74-32
crypto ipsec	74-34
ipv6 ospf cost	74-34
ipv6 ospf dead-interval	74-36
ipv6 ospf hello-interval	74-37
ipv6 ospf helper-disable	74-38
ipv6 ospf ignore-mtu	74-38
ipv6 ospf neighbor	74-39
ipv6 ospf poll-interval	74-40
ipv6 ospf neighbor priority	74-40
ipv6 ospf neighbor cost	74-41
ipv6 ospf neighbor database-filter-all-out	74-42
ipv6 ospf network	74-42
ipv6 ospf priority	74-43
ipv6 ospf retransmit-interval	74-44
ipv6 ospf transmit-delay	74-44

ipv6 ospf

Use this command to configure the IPv6 OSPFv3 process ID, area, and optional instance on an interface.

Syntax

ipv6 ospf *process* **area** *area* [**instance** *instance-id*]

no ipv6 ospf *process* **area** *area* [**instance** *instance-id*]

Parameters

process	Specifies an OSPFv3 process ID for this IPv6 interface.
area *area*	Specifies the OSPFv3 area for this process. The area can be specified as either a decimal value from **0** - **4294967295** or in the dotted-quad notation **A.B.C.D**.
instance	(Optional) Specifies an OSPFv3 instance for this interface. Configurable values are **1** - **255**. The default value is **0**. Instance **0** can not be removed.

Defaults

If an instance is not specified, the instance defaults to **0**.

Mode

Interface configuration.

Usage

Enable OSPFv3 on the interface by specifying an OSPFv3 process and area at the interface level. You must first configure the process in OSPFv3 router configuration mode using "ipv6 router ospf" on page 74-2. The area is specified using a decimal value or dotted-quad notation.

OSPFv3 supports multiple OSPFv3 instances on an interface. An OSPFv3 interface instance allows several providers running separate OSPFv3 domains to share one or more physical network segments they may have in common. You can also use OSPFv3 interface instances to assign multiple OSPFv3 areas to a single interface. The OSPFv3 instance on an interface solely affects the reception of OSPFv3 packets.

The "no" form of this command removes .

Example

This example shows how to configure VLAN 15 for OSPFv3 process 60, area 77.0.0.0 instance 1:

```
S Chassis(su)->configure
S Chassis(su-config)->interface vlan 15
S Chassis(su-config-intf-vlan.0.15)->ipv6 ospf 60 area 77.0.0.0 instance 1
```

ipv6 ospf authentication

Use this command to configure IPsec authentication on an interface.

Syntax

ipv6 ospf authentication ipsec spi *spi* {**md5** *key* | **sha1** *key* | **aescbc** *key*} [**hex**]

no ipv6 ospf authentication

Parameters

ipsec	Sets the authentication type to IPsec for OSPFv3.
spi *spi*	Specifies the Security Parameters Index (SPI) for this IPv6 OSPF IPsec authentication configuration. Valid values are **256** - **4294967295**
md5 *key*	Specifies the MD5 authentication algorithm and configures a 16 byte MD5 key for this SPI entry.
sha1 *key*	Specifies the 20-byte sha1 key for this SPI entry.
aescbc *key*	Specifies the 16-byte aescbc key for this SPI entry.
hex	(Optional) Specifies that the SPI entry key is a hex string.

Defaults

If the hex option is not specified, the key is an ASCII passphrase value.

Mode

Interface configuration.

Usage

IPsec is an end-to-end security scheme that provides for the securing of IP communications using authentication and optional encryption. An IPsec authentication only entry consists of an SPI value to identify the entry, the specifying of the authentication algorithm for the entry, and the entry key. IPsec authentication entries are configured on a per interface basis.

IPsec authentication supports algorithms:

- **MD5** – Message-Digest algorithm 5
- **SHA1** – Secure Hash Algorithm 1
- **AESCBC** – Advanced Encryption Standard (AES) Cipher Algorithm in Cipher Block Chaining (CBC)

IPsec must be enabled in global VRF router configuration mode using the **crypto ipsec enable** command before using IPsec for OSPFv3 authentication.

If FIPS security mode is enabled using "set security fips mode" on page 3-9, only the SHA1 authentication algorithm is supported on the interface.

The "no" form of this command removes the IPsec authentication configuration on the interface.

Example

This example shows how to configure VLAN 1 for IPsec SPI entry 256 for MD5 authentication with a hex key of **1234567890abcdef**:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ipv6 ospf authentication spi 256 md5
1234567890abcdef hex
```

ipv6 ospf encryption

Use this command to configure IPsec encrypted authentication on an interface.

Syntax

ipv6 ospf encryption ipsec spi *spi* **esp** {**none** | **3des** *key* | **aescbc** {**128** | **192** | **256**} *key*} [**hex**] **auth** {**md5** *key* | **sha1** *key* | **aescbc** *key* | **no-auth**}

no ipv6 ospf encryption

Parameters

ipsec	Sets the encrypted authentication type to IPsec for OSPFv3.
spi *spi*	Specifies the Security Parameters Index (SPI) for this IPv6 OSPF IPsec authentication configuration. Valid values are **256** - **4294967295**
esp	An Encapsulation Security Payload or none will be specified.
none	Specifies that no cipher algorithm is configured for this IPsec entry.
3des *key*	Configures the Cipher algorithm 3-DES (Triple Data Encryption Standard) specifying a 24-byte key

aescbc {**128** | **192** | **256**} *key*	Configures the AES (Cipher Block Chaining) cipher algorithm specifying: 128 – Configures a 128-bit (16-byte) key 192 – Configures a 192-bit (24-byte) key 256 – Configures a 256-bit (32-byte) key
auth	The authentication keyword followed by the authentication algorithm to be configured.
md5 *key*	Specifies the MD5 authentication algorithm and configures a 16-byte MD5 key for this SPI entry.
sha1 *key*	Specifies the 20-byte sha1 key for this SPI entry.
aescbc *key*	Specifies the 16-byte aescbc key for this SPI entry.
hex	(Optional) Specifies that the SPI entry key is a hex string.

Defaults

If the hex option is not specified, the key is an ASCII passphrase value.

Mode

Interface configuration.

Usage

IPsec is an end-to-end security scheme that provides for the securing of IP communications using an authentication algorithm and optional encryption. An encrypted IPsec authentication entry consists of an SPI value to identify the entry, the specifying of a cipher encryption algorithm or no algorithm, the specifying of the authentication algorithm for the entry or no authentication, and the entry key. Encrypted IPsec authentication entries are configured on a per interface basis.

IPsec encryption supports ciphers:

- **3DES** – Triple Data Encryption Standard cipher algorithm
- **AESCBC** – AES (Cipher Block Chaining) cipher algorithm

IPsec authentication supports algorithms:

- **MD5** – Message-Digest algorithm 5
- **SHA1** – Secure Hash Algorithm 1
- **AESCBC** – Advanced Encryption Standard (AES) Cipher Algorithm in Cipher Block Chaining (CBC)

IPsec must be enabled in global VRF router configuration mode using the **crypto ipsec enable** command before using IPsec for OSPFv3 encrypted authentication.

If FIPS security mode is enabled using “set security fips mode” on page 3-9, only the SHA1 authentication algorithm is supported on the interface.

The “no” form of this command removes the IPsec encrypted authentication configuration on the interface.

Example

This example shows how to configure VLAN 1 for IPsec SPI entry 256 for the 128-bit aescbc encryption with a key of **1234567890abcdef**, and for MD5 authentication with a hex key of **1234567890abcdef**:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ipv6 ospf encryption ipsec spi 256 esp aescbc
128 1234567890abcedf hex auth md5 1234567890abcdef hex
```

crypto ipsec

Use this command to enable IPsec on the router.

Syntax

crypto ipsec enable

no crypto ipsec enable

Parameters

enable	Enables IPsec for this router

Defaults

None.

Mode

Global VRF router configuration.

Usage

IPsec must be enabled on the Global VRF router in order to configure IPsec for OSPFv3 authentication and encrypted authentication. Enable IPsec on the global VRF router using the **crypto ipsec enable** command.

Example

This example shows how to enable IPsec on the global VRF router:

```
S Chassis(rw-config)->crypto ipsec enable
```

ipv6 ospf cost

Use this command to set the cost of sending an OSPFv3 packet on an interface.

Syntax

ipv6 ospf cost *cost*

no ipv6 ospf cost *cost*

Parameters

cost	Specifies the cost of sending an OSPFv3 packet on this interface. Valid values range from **1** to **65535**. The default value is the reference bandwidth divided by the interface bandwidth.

Defaults

The default OSPFv3 interface cost is the reference bandwidth divided by the interface bandwidth.

Mode

Interface configuration.

Usage

Each router interface that participates in OSPFv3 routing is assigned a default cost. This command overwrites the default OSPF interface cost.

The reference bandwidth defaults to 100Mbps and can be modified using "auto-cost reference-bandwidth" on page 74-18.

The "no" form of this command resets the OSPFv3 cost to the default of 10.

Example

This example shows how to set the OSPFv3 cost to 20 for VLAN 1:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ipv6 ospf cost 20
```

ip ospf cost track

Use this command to sum the interface speeds contained in the specified tracked object when setting the OSPF interface cost.

Syntax

ip ospf cost track *trackobject-name*

no ip ospf cost track *trackobject-name*

Parameters

trackobject-name	Specifies the name of the tracked object containing the port names of interfaces to be summed to set the aggregate interface speed when calculating OSPF interface cost.

Defaults

None.

Mode

Configuration command, Interface configuration.

Usage

The formula for calculating the OSPF interface cost metric is the reference bandwidth divided by the interface bandwidth. By default the reference bandwidth is set to 100 Mbps. For logical interfaces containing multiple physical interfaces, such as a LAG, the aggregate interface speed is not readily available. A tracked object configured with the ports belonging to the logical interface can return the physical interface speed of each physical port specified in the tracked object. OSPF will sum the returned interface speeds and use that aggregate value when calculating OSPF interface cost.

Note: The speed used in the cost calculation is sum of all ports capabilities in the tracked object. Setting the speed manually will not change the tracked interface speed. A 1GB capable port has a 1 GB speed regardless of the manual speed setting. The same holds true for ports that auto-negotiate to a lower speed. The expectation is that both sides of the link are using the same ports and SFP connectors and should result in the same speed.

Because the tracked object will report when a physical interface is up or down, OSPF will dynamically adjust the aggregate speed when an interface becomes active or goes down and adjust the OSPF interface cost accordingly.

When adding an additional physical port to a logical interface that uses the interface summation method to determine OSPF interface cost, you must also add the physical port to the associated tracked object.

See "Tracked Object Commands" on page 22-24" for tracked object command details.

The "no" form of this command resets the OSPF cost to the value based upon the auto cost setting as set using "auto-cost reference-bandwidth" on page 74-18.

Example

This example shows how to set the OSPF interface cost for VLAN **1** using the summation method based upon ports configured in track object **ospfIntf1**:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip ospf cost track ospfIntf1
```

ipv6 ospf dead-interval

Use this command to set the number of seconds a router must wait to receive a hello packet from its neighbor before determining that the neighbor is out of service.

Syntax

ipv6 ospf dead-interval {*seconds* | **minimal hello-multiplier** *number*}

no ipv6 ospf dead-interval

Parameters

seconds	Specifies the number of seconds that a router must wait to receive a hello packet. Dead interval must be the same on neighboring routers (on a specific subnet), but can vary between subnets. This parameter is an unsigned integer ranging from **1** to **65535**. Default: **40** Seconds.
minimal	Sets the dead-interval to 1 second for fast hello.
hello-multiplier *number*	Specifies the number of hello-packets that will be sent in 1 second. Valid values are **3** - **20**.

Defaults

None.

Mode

Interface configuration.

Usage

By default, hello packets are sent out every 10 seconds. If after 40 seconds, there is no response on the interface, the interface will be shutdown. If for any reason you want a short (minimal) dead interval, entering the **minimal** keyword sets the dead interval to to a fixed value 1 second and requires you to specify the number of hello packets that will be sent in that 1 second interval. Keep in mind that setting the **minimal** option can result in a significant increase in OSPF overhead traffic on the network.

The "no" form of this command sets the dead interval value to the default.

Examples

This example shows how to set the dead interval to 20 for VLAN 1:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ipv6 ospf dead-interval 20
```

This example shows how to configure fast hello for VLAN 1, hard setting the dead interval to 1 second and specifying that 3 hello packets will be sent in that fixed 1 second interval:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ipv6 ospf dead-interval minimal
hello-multiplier 3
```

ipv6 ospf hello-interval

Use this command to set the number of seconds a router must wait before sending a hello packet to neighbor routers on an interface.

Syntax

ipv6 ospf hello-interval *seconds*

no ipv6 ospf hello-interval

Parameters

seconds	Specifies the hello interval in seconds. Hello interval must be the same on neighboring routers (on a specific subnet), but can vary between subnets. This parameter is an unsigned integer with valid values between **1** and **65535**. Defaults: **10** seconds.

Defaults

None.

Mode

Interface configuration.

Usage

Each Extreme Networks S-Series routing module or Standalone device can support communications between up to 60 neighboring routers.

The "no" form of this command sets the hello interval value to the default.

Example

This example shows how to set the hello interval to 5 for VLAN 1:

```
S Chassis(rw-router-config)->interface vlan 1
S Chassis(rw-router-intf-Vlan-1)->ipv6 ospf hello-interval 5
```

ipv6 ospf helper-disable

Use this command to disable the graceful restart helper function on this router interface.

Syntax

ipv6 ospf helper-disable

no ipv6 ospf helper-disable

Parameters

None.

Defaults

None.

Mode

Interface configuration.

Usage

Each restarting router network segment functions as a helper by monitoring the network for topology changes. So long as the helper does not see an LSA change, it continues to advertise its LSAs as though the restarting router remained in continuous operation. This command disables this capability. For more information on the graceful restart helper function, see the *Extreme Networks S-Series Configuration Guide*.

The “no” form of this command enables graceful restart helper mode for this router.

Example

This example shows how to disable the helper function on this interface:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ipv6 ospf helper-disable
S Chassis(rw-config-intf-vlan.0.1)->
```

ipv6 ospf ignore-mtu

Use this command to ignore the MTU advertised by the neighbor.

Syntax

ipv6 ospf ignore-mtu

no ipv6 ospf ignore-mtu

Parameters

None.

Defaults

None.

Mode

Interface configuration.

Usage

If the interface MTU field in the Database Description (DBD) packet indicates an IP datagram size that is greater than the router can accept on the receiving side without fragmentation, the DBD packet is rejected. If the ignore MTU feature is enabled with this command, the DBD packet will not be rejected and will be processed instead.

The "no" form of this command disables the ignore MTU feature.

Example

This example shows how to enable the ignore MTU feature on this interface:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ipv6 ospf ignore-mtu
```

ipv6 ospf neighbor

Use this command to configure an OSPFv3 neighbor of this interface on a non-broadcast network.

Syntax

ipv6 ospf neighbor *ipv6-address*

no ipv6 ospf neighbor *ipv6-address*

Parameters

ipv6-address	Specifies the IPv6 address of the neighbor on this interface.

Defaults

None.

Mode

Interface configuration.

Usage

OSPFv3 dynamically discovers each neighbor for a given OSPFv3 router. OSPFv3 cannot dynamically discover its neighbors on non-broadcast and point-to-multipoint networks. For these networks neighbors must be configured. The router uses the information in the neighbor entry to send unicast hellos to the neighbor to start an adjacency. Use this command to specify the neighbor on this interface this OSPFv3 router will form an adjacency with.

Example

This example shows how to configure neighbor 2000:eff0::10 for this router:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ipv6 ospf neighbor 2000:2001:eff0::10
```

ipv6 ospf poll-interval

Use this command to set a non-broadcast neighbor polling interval.

Syntax

ipv6 ospf poll-interval *seconds*

no ipv6 ospf poll-interval

Parameters

seconds	Specifies the number of seconds between polls for this non-broadcast neighbor. Valid values: **0** - **4294967295**. Default: 120 seconds.

Defaults

None.

Mode

Interface configuration.

Usage

The polling interval sets the time between hello messages sent to this interface's neighbor.

The "no" form of this command resets the value to the default of **120**.

Example

This example shows how to set the OSPFv3 neighbor polling interval on VLAN 1:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ipv6 ospf poll-interval 150
```

ipv6 ospf neighbor priority

Use this command to set the OSPFv3 priority value for the specified neighbor on the interface.

Syntax

ipv6 ospf neighbor *ipv6-address* **priority** *number*

no ipv6 ospf neighbor *ipv6-address* **priority**

Parameters

ipv6-address	Specifies the neighbor IPv6 address.
number	Specifies the router's OSPFv3 priority in a range from **0** to **255**. The default value is **1**.

Defaults

None.

Mode

Interface configuration.

Usage

The priority value is communicated between routers by means of hello messages and influences the election of a designated router.

The “no” form of this command resets the value to the default of 1.

Example

This example shows how to set the OSPFv3 priority to 20 for VLAN 1 neighbor 2000:2001:eff0::10:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ipv6 ospf neighbor 2000:2001:eff0::10
priority 20
```

ipv6 ospf neighbor cost

Use this command to assign a cost for the specified neighbor on the interface.

Syntax

ipv6 ospf neighbor *ipv6-address* **cost** *number*

no ipv6 ospf neighbor *ipv6-address* **cost**

Parameters

ipv6-address	Specifies the neighbor IPv6 address.
number	Specifies the cost assigned to the specified neighbor on the interface. Valid values are **1** - **65535**. The default value is **10**.

Defaults

None.

Mode

Interface configuration.

Usage

Assigns a cost to the interface neighbor. If a neighbor cost is not assigned, the cost specified by the **ipv6 ospf cost** command is used. This command does not apply to NBMA networks.

The “no” form of this command resets the neighbor cost to the default of 10.

Example

This example shows how to set the to 5 for VLAN 1 neighbor 2010:2001:eff0::10:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ipv6 ospf neighbor 2010:2001:eff0::10 cost 5
```

ipv6 ospf neighbor database-filter-all-out

Use this command to filter outgoing link-state advertisements to an OSPFv3 neighbor on this interface.

Syntax

ipv6 ospf neighbor *ipv6-address* **database-filter-all-out**

no ipv6 ospf neighbor *ipv6-address* **database-filter-all-out**

Parameters

None.

Defaults

None.

Mode

Interface configuration.

Usage

The "no" form of this command disables the database filter all feature.

Example

This example shows how to set the to 5 for VLAN 1 neighbor 2010:2001:eff0::10:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ipv6 ospf neighbor 2010:2001:eff0::10
database-filter-all-out
```

ipv6 ospf network

Use this command to configure the OSPFv3 network link type.

Syntax

ipv6 ospf network {**non-broadcast** | **broadcast** | **point-to-point** | **point-to-multipoint**}

no ipv6 ospf network

Parameters

non-broadcast	Specifies this interface is a non-broadcast or Non-Broadcast-Multi-Access (NBMA) network link type.
broadcast	Specifies this interface is a broadcast network link type. Default.
point-to-point	Specifies this interface is a point-to-point network link type.
point-to-multipoint	Specifies this interface is a point-to-point network link type.

Defaults

None.

Mode

Interface configuration.

Usage

The “no” form of this command resets the network type to broadcast.

When routers in your network do not support multicast addressing, you can configure them as NBMA networks. NBMA networks can be configured as broadcast networks to avoid the need to configure neighbors. But configuring NBMA networks as either broadcast or nonbroadcast assumes a fully meshed virtual circuit network configuration. For partially meshed networks, configure network type to point-to-multipoint.

Example

This example shows how to set the OSPFv3 interface link type to point-to-point:

```
S Chassis(su)->configure
S Chassis(su-config)->interface vlan 15
S Chassis(su-config-intf-vlan.0.15)->ipv6 ospf network point-to-point
```

ipv6 ospf priority

Use this command to set the OSPFv3 priority value for the interface.

Syntax

ipv6 ospf priority *number*

no ipv6 ospf priority

Parameters

number	Specifies the router’s OSPFv3 priority in a range from **0** to **255**. The default value is **1**.

Defaults

None.

Mode

Interface configuration.

Usage

The priority value is communicated between routers by means of hello messages and influences the election of a designated router.

The “no” form of this command resets the value to the default of 1.

Example

This example shows how to set the OSPFv3 priority to 20 for VLAN 1:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ipv6 ospf priority 20
```

ipv6 ospf retransmit-interval

Use this command to set the amount of time between retransmissions of link state advertisements (LSAs) for adjacencies that belong to the interface.

Syntax

ipv6 ospf retransmit-interval *seconds*

no ipv6 ospf retransmit-interval

Parameters

seconds	Specifies the retransmit time in seconds. Valid values are **1** to **3600**. Default: **5** Seconds.

Defaults

None.

Mode

Interface configuration.

Usage

The "no" form of this command resets the retransmit interval value to the default value of 5 seconds.

Example

This example shows how to set the OSPFv3 retransmit interval for VLAN 1 to 20:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ipv6 ospf retransmit-interval 20
```

ipv6 ospf transmit-delay

Use this command to set the amount of delay before transmitting a link state update packet on an interface.

Syntax

ipv6 ospf transmit-delay *seconds*

no ipv6 ospf transmit-delay

Parameters

seconds	Specifies the transmit delay in seconds. Valid values are from **1** to **65535**. Default: **1** second.

Defaults

None.

Mode

Interface configuration.

Usage

The “no” form of this command resets the transmit delay value to the default of 1 second.

Example

This example shows how to set the delay before transmitting a link state update packet on VLAN 1 at 20 seconds:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ipv6 ospf transmit-delay 20
```

OSPFv3 Show Commands

This section details OSPFv3 show command that display OSPFv3 configuration information and statistics.

For information about...	Refer to page...
show ipv6 ospf	74-45
show ipv6 ospf database	74-46
show ipv6 ospf border-routers	74-48
show ipv6 ospf interface	74-48
show ipv6 ospf neighbor	74-50
show ipv6 ospf virtual-links	74-51

show ipv6 ospf

Use this command to display OSPFv3 information.

Syntax

show ipv6 ospf [*process-id***] interface** [*ifName*]

Parameters

process-id	(Optional) Specifies a configured OSPF process by its process ID. If *process-id* is included, information for the specified routing process only is displayed.
ifName	(Optional) Displays OSPF information for an interface, such as a specific VLAN. The interface must be configured for IP routing as described in the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display OSPFv3 information:

```
S Chassis(rw)->show ipv6 ospf
Routing Process ospf 41 with ID 21.10.1.3
Supports only single TOS(TOS0) route
It is an area border and autonomous system boundary router
Summary Link update interval is 1800 seconds.
External Link update interval is 1800 seconds.
Redistributing External Routes from:
Area BACKBONE (0)
    Number of interfaces in this area is 8
    SPF algorithm executed 7 times
Area 0.0.0.1
    Number of interfaces in this area is 1
    SPF algorithm executed 7 times
```

show ipv6 ospf database

Use this command to display the OSPFv3 link state database.

Syntax

show ipv6 ospf database *type* [*link-state-id*]

The options for using this syntax are:

show ipv6 ospf database database-summary
show ipv6 ospf database external [*link-state-id*]
show ipv6 ospf database inter-area-prefix [*link-state-id*]
show ipv6 ospf database inter-area-router [*link-state-id*]
show ipv6 ospf database intra-area-prefix [*link-state-id*]
show ipv6 ospf database network [*link-state-id*]
show ipv6 ospf database nssa-external [*link-state-id*]
show ipv6 ospf database router [*link-state-id*]

Parameters

link-state-id	(Optional) Specifies the link state identifier. Valid values are IP addresses.
database-summary	Displays a numerical summary of the contents of the link state database.
external	Displays external (Type 5) link state advertisements.
inter-area-prefix	Displays inter-area prefix (Type 3) link state advertisements. Type 3 link state advertisements describe a prefix outside an area but within the OSPFv3 domain.
inter-area-router	Displays inter-area router (Type 4) link state advertisements. Type 4 link state advertisements describe the route to the ASBR.

intra-area-prefix	Displays intra-area prefix (Type 9) link state advertisements. Type 9 link state advertisements advertise IPv6 prefixes that are associated with the router itself, an attached stub network segment, or an attached transit network segment.
network	Displays network (Type 2) link state advertisements in their detailed format. Network advertisements are originated by designated routers.
nssa-external	Displays nssa-external (Type 7) link state advertisements in their detailed format. Type 7 advertisements are originated by ASBRs.
router	Displays router (Type 1) link state advertisements in their detailed format. Router advertisements are originated by all routers.

Defaults

If *link-state-id* is not specified, the specified type of database records will be displayed for all link state IDs.

Mode

All command modes.

Example

This example show how to display a summary of the OSPFv3 database:

```
S Chassis(rw)->show ipv6 ospf database database-summary

show ipv6 ospf database database-summary

    Area ID            Router  Network IntrPfx IntrRtr NSSA IntraPx SubTotal
    0.0.0.0                 2        1       1       0    0       3        7
    0.0.0.1                 1        0       2       1    0       2        6
    0.0.0.9                 1        0       3       1    0       1        6
S Chassis(rw)->
```

Table 74-3 provides an explanation of the command output.

Table 74-2 show ipv6 ospf database database-summary Output Details

Output...	What it displays...
Area ID	Specifies the area ID for this database summary line.
Router	Specifies the number of routers belonging to this area in the database.
Network	Specifies the number of networks in this area in the database.
Intrpfx	Specifies the number of inter-area prefixes in the database for this area.
IntrRtr	Specifies the number of inter-area routers in the database for this area.
NSSA	Specifies the number of Not-So-Stubby-Areas in the database for this area.
IntraPx	Specifies the number of intra-area prefixes in the database for this area.
Subtotal	Specifies the subtotal of all listed database elements for this area summary line.

show ipv6 ospf border-routers

Use this command to display information about Area Border Routers (ABRs) and Autonomous System Boundary Routers (ASBRs).

Syntax

show ipv6 ospf border-routers

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display information about OSPF border routers:

```
S Chassis(rw)->show ipv6 ospf border-routers
Area Border Routers:
```

show ipv6 ospf interface

Use this command to display OSPFv3 interface related information, including network type, priority, cost, hello interval, and dead interval.

Syntax

show ipv6 ospf [*process-id***] interface** [*ifName*]

Parameters

process-id	(Optional) Specifies a configured OSPFv3 process by its process ID. If *process-id* is included, information for the specified routing process only is displayed.
ifName	(Optional) Displays OSPFv3 information for an interface, such as a specific VLAN. The interface must be configured for IP routing as described in the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *ifName* is not specified, OSPFv3 statistics are displayed for all interfaces (including VLANs).

Mode

All command modes.

Example

This example shows how to display all OSPFv3 related information for VLAN 23:

```
S Chassis(rw)->show ipv6 ospf interface vlan.0.23
vlan.0.23 is UP
  Process Id 60 Router Id 41.0.0.0, Network Type BROADCAST, Cost: 10
 Area Id is 0.0.0.0, Transmit Delay is 1 sec, State DESIGNATED-ROUTER, Priority 1
  Designated Router IfIndex 23
  No backup designated router on this network
  Timer intervals configured: Hello 10, Dead 40, Wait 40, Retransmit 5
  Neighbor Count is 0, Adjacent neighbor count is 0
```

Table 74-3 provides an explanation of the command output.

Table 74-3 show ipv6 ospf interface Output Details

Output...	What it displays...
Vlan.*x*.*y* is	Interface (VLAN) administrative status as up or down.
Process Id	OSPFv3 Process ID.
Router Id	Router ID for this router.
Network Type	OSPFv3 network type: non-broadcast, broadcast, point-to-point, or point-to-multipoint
Cost	OSPFv3 interface cost, which is either default, or assigned with the **ipv6 ospf cost** command. For details, refer to “ipv6 ospf cost” on page 74-34.
Area Id	The Area ID that this interface is a member of in dotted-quad notation.
Transmit Delay	The number (in seconds) added to the LSA (Link State Advertisement) age field.
State	The interface state (versus the state between neighbors). Valid values include BACKUP-DESIGNATED-ROUTER and DESIGNATED-ROUTER.
Priority	The interface priority value, which is either default, or assigned with the **ipv6 ospf priority** command. For details, refer to “ipv6 ospf priority” on page 74-43.
Designated Router IfIndex	Interface index of the designated router on this subnet, if one exists.
Backup Designated Router IfIndex	Interface index of the backup designated router on this interface, if one exists.
Timer intervals configured	OSPFv3 timer intervals. These are either default, or configured with the **ipv6 ospf retransmit-interval** (“ipv6 ospf retransmit-interval” on page 74-44), the **ipv6 ospf hello-interval** (“ipv6 ospf hello-interval” on page 74-37), and the **ipv6 ospf dead interval** (“ipv6 ospf dead-interval” on page 74-36) commands. The wait timer represents the amount of time a router waits before initiating a designated router/backup designated router election. The wait timer value is the same as the dead interval timer value. The retransmit timer represents the amount of time between successive transmissions of LSAs (Link State Advertisements) until acknowledgement is received.
Neighbor Count	Number of neighbors on this interface.
Adjacent neighbor count	Number of adjacent (FULL state) neighbors over this interface.

show ipv6 ospf neighbor

Use this command to display the state of communication between an OSPFv3 router and its neighbor routers.

Syntax

show ipv6 ospf neighbor [*router-id*] [**detail**] [**vlan** *vlan-id*]

Parameters

router-id	(Optional) Displays OSPFv3 neighbors for a specific router ID.
detail	(Optional) Displays detailed information about the neighbors, including the area in which they are neighbors, who the designated router/backup designated router is on the subnet, if applicable, and the decimal equivalent of the E-bit value from the hello packet options field.
vlan *vlan*-id	(Optional) Displays OSPFv3 neighbors for a specific VLAN. This VLAN must be configured for IP routing as described in the *Extreme Networks S-Series Configuration Guide*.

Defaults

- If *router-id* is not specified, OSPFv3 neighbors will be displayed for all routers configured for routing.
- If **detail** is not specified, a standard level of information will be displayed.
- If *vlan-id* is not specified, OSPFv3 neighbors will be displayed for all VLANs configured for routing.

Mode

All command modes.

Example

This example shows how to use the **show ospf neighbor** command:

```
S Chassis(rw)->show ipv6 ospf neighbor detail

Neighbor 23.10.3.2 Interface index is 000000000000023
  In the area 0.0.0.0 via vlan.0.23
  Neighbor priority is 1, state is  FULL
  Options 0x13
  Dead interval countdown 38 sec(s)
  Link state retransmission queue length is 0
  Neighbor has changed state 6 times
```

Table 74-4 provides an explanation of the command output.

Table 74-4 show ipv6 ospf neighbor Output Details

Output...	What it displays...
Neighbor	Neighbor's router ID of the OSPFv3 neighbor.
Interface index is	Interface index for this neighbor link.
Neighbor priority is	Neighbor's priority over this interface.
State	Neighbor's OSPFv3 communication state.
Options	OSPFv3 options as defined in RFC 2740.
Dead interval countdown	Interval (in seconds) this router will wait without receiving a Hello packet from a neighbor before declaring the neighbor is down.
Link state retransmission queue length	Length of the link state retransmission queue.
Neighbor has changed state *x* times	Number of times the neighbor has changed state.

show ipv6 ospf virtual-links

Use this command to display information about the virtual links configured on a router.

Syntax

```
show ipv6 ospf virtual-links
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

A virtual link represents a logical connection between the backbone and a non-backbone OSPFv3 area.

Example

This example shows how to display OSPFv3 virtual links information:

```
S Chassis(rw)->show ipv6 ospf virtual-links
Virtual Link to router 77.0.0.3, is UP
 Transit area  0.0.0.1,
 Transmit Delay is 1 sec(s), State DOWN
 Timer intervals configured:
                Hello 10, Dead 60, Wait 60, Retransmit 5
```

Table 74-5 provides an explanation of the command output.

Table 74-5 show ipv6 ospf virtual links Output Details

Output...	What it displays...
Virtual Link	Router ID of the virtual link neighbor, and the virtual link status, which is up or down.
Transit area	Area for this virtual link neighbor
Transmit Delay	Time (in seconds) added to the LSA (Link State Advertisement) age field when the LSA is transmitted through the virtual link.
State	Interface state assigned to a virtual link, which is point-to-point.
Timer intervals configured	Timer intervals configured for the virtual link, including Hello, Dead, Wait, and Retransmit intervals.

75

Intermediate System To Intermediate System (IS-IS) Commands

This chapter describes the Intermediate System to Intermediate System (IS-IS) set of commands and how to use them.

For information about...	Refer to page...
IS-IS Configuration Overview	75-1
Configuration Commands	75-1
Interface Commands	75-22
Show Commands	75-37

IS-IS Configuration Overview

For IS-IS to operate on an interface:

- IS-IS must be enabled on the device using "router isis" on page 75-2
- The network entity title (NET) must be configured using "net" on page 75-18
- An IPv4 address must be configured on the interface using "ip address" on page 54-6 or an IPv6 address must be configured on the interface using "ipv6 address" on page 55-3

By default, IS-IS configuration applies to both IPv4 and IPv6 routes. With the above items configured, use "address-family" on page 75-3 to configure IPv6 specific configuration on the device. IPv6 unicast specific IS-IS configuration currently supports:

- Administrative distance using "distance (IS-IS)" on page 75-7
- Redistribution of routes from other protocols into IS-IS using "redistribute" on page 75-19
- Address summarization using "summary-address" on page 75-22

For IPv6 routing, IPv6 IS-IS must be enabled on the interface using "ipv6 router isis" on page 75-24.

Configuration Commands

For information about...	Refer to page...
router isis	75-2
address-family	75-3

For information about...	Refer to page...
area-password	75-4
authentication key-chain	75-4
authentication mode	75-5
authentication send-only	75-6
distance (IS-IS)	75-7
domain-password	75-8
graceful-restart enable	75-9
graceful-restart enable-help-peer	75-9
graceful-restart restart-adj-interval	75-10
graceful-restart restart-interval	75-11
graceful-restart restart-sync-interval	75-11
hostname dynamic	75-12
ignore-lsp-errors	75-13
is-type	75-13
lsp-buf-size	75-14
lsp-gen-interval	75-15
max-lsp-lifetime	75-16
maximum-paths	75-16
metric-style	75-17
net	75-18
redistribute	75-19
set-overload-bit	75-20
spf-interval	75-21
summary-address	75-22

router isis

Use this command to enable or disable Intermediate System to Intermediate System (IS-IS) and gain access to IS-IS configuration mode.

Syntax

```
router isis
no router isis
```

Parameters

None.

Defaults

None.

Mode

Global router configuration**.**

Usage

You must execute the **router isis** command to enable the IS-IS protocol before completing many IS-IS-specific configuration tasks.

The "no" form of this command disables the IS-IS on this device.

Example

This example shows how to enable IS-IS routing on the device:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->
```

address-family

Use this command to enter the IPv6 unicast IS-IS address family configuration mode.

Syntax

address-family ipv6 unicast

no address-family ipv6 unicast

Parameters

ipv6	Specifies the IPv6 address family.
unicast	Specifies the unicast address family.

Defaults

None.

Mode

IS-IS router configuration.

Usage

By default, IS-IS configuration applies to both IPv4 and IPv6 routes. Use this command to configure IPv6 specific configuration on the device. IPv6 unicast specific address family configuration currently supports:

- Administrative distance using "distance (IS-IS)" on page 75-7
- Redistribution of routes from other protocols into IS-IS using "redistribute" on page 75-19
- Address summarization using "summary-address" on page 75-22

The "no" form of this command removes any IPv6 unicast address family configuration.

Example

This example shows how to enter IPv6 unicast IS-IS address family configuration mode:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->address-family ipv6 unicast
S Chassis(rw-config-isis-af)->
```

area-password

Use this command to set the area password for this IS-IS area.

Syntax

area-password *password*

Parameters

password	Specifies the area password.

Defaults

None.

Mode

IS-IS router configuration.

Usage

Configuring an area password enables authentication on the device.

A key chain or area password can be configured for the device, but not both a key chain and password. If a key chain is configured for the device, it must be removed before attempting to configure an area password. The area password can be overridden by configuring either a key chain or a password on the interface. A device level area password can coexist with an interface key chain because the interface is checked first, and if either an interface key chain or password exist, the device level configuration is not checked.

The “no” form of this command deletes the specified area password.

Example

This example shows how to set the area password to **docpass**:

```
S Chassis(rw-config-isis)->area-password docpass
S Chassis(rw-config-isis)->
```

authentication key-chain

Use this command to configure IS-IS authentication key chain for this device.

Syntax

authentication key-chain *keychain* [**level-1** | **level-1-2** | **level-2**]

no authentication key-chain *keychain* [**level-1** | **level-1-2** | **level-2**]

Parameters

keychain	Specifies the name of the key chain. Valid values are up to 16 alpha-numeric characters.
level-1	(Optional) Specifies that the key chain configuration should be restricted to level 1.
level-1-2	(Optional) Specifies that the key chain configuration should be applied to both level 1 and level 2.
level-2	(Optional) Specifies that the key chain configuration should be restricted to level 2.

Defaults

If no option is specified, the key chain is applied to both level 1 and level 2.

Mode

IS-IS router configuration.

Usage

Configuring a device key chain enables authentication on the device.

A key chain or area and domain passwords can be configured for the device, but not both a key chain and any password. If either an area or domain password is configured for the device, it must be removed before attempting to configure a device key chain. The device key chain can be overridden by configuring either a key chain or a password on the interface. A device level key chain can coexist with an interface password because the interface is checked first, and if either an interface key chain or password exist, the device level configuration is not checked.

The "no" form of this command removes the authentication key-chain configuration.

Example

This example shows how to configure the IS-IS authentication key chain to keychainlv1 and restricts the key chain configuration to level 1:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->authentication keychain keychainlv1 level-1
S Chassis(rw-config-isis)->
```

authentication mode

Use this command to configure IS-IS authentication mode for this device.

Syntax

authentication mode {**md5** | **text**} [**level-1** | **level-1-2** | **level-2**]

no authentication mode {**md5** | **text**} [**level-1** | **level-1-2** | **level-2**]

Parameters

md5	Specifies MD5 as the IS-IS authentication mode.
text	Specifies text as the IS-IS authentication mode.

level-1	(Optional) Specifies that the authentication mode configuration should be restricted to level 1.
level-1-2	(Optional) Specifies that the authentication mode configuration should be applied to both level 1 and level 2.
level-2	(Optional) Specifies that the authentication mode configuration should be restricted to level 2.

Defaults

If no option is specified, the mode configuration is applied to both level 1 and level 2.

Mode

IS-IS router configuration.

Usage

The IS-IS MD5 mode authentication provides a cryptographic hash MD5 digest to each IS-IS PDU, preventing unauthorized routing messages to enter the IS-IS domain.

IS-IS has five packet types: link state packet (LSP), LAN Hello, Serial Hello, CSNP, and PSNP. The MD5 authentication or the clear text password authentication is applied to each IS-IS PDU type. The IS-IS level that the authentication is applied to can be specified for each level type.

The "no" form of this command removes the IS-IS authentication mode configuration.

Example

This example shows how to configure the IS-IS authentication to MD5 for level 1:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->authentication mode md5 level-1
S Chassis(rw-config-isis)->
```

authentication send-only

Use this command to configure IS-IS authentication only on sent IS-IS frames.

Syntax

```
authentication send-only [level-1 | level-1-2 | level-2]
no authentication send-only [level-1 | level-1-2 | level-2]
```

Parameters

level-1	(Optional) Specifies that the authentication send-only configuration should be restricted to level 1.
level-1-2	(Optional) Specifies that the authentication send-only configuration should be applied to both level 1 and level 2.
level-2	(Optional) Specifies that the authentication send-only configuration should be restricted to level 2.

Defaults

If no level option is specified, IS-IS authentication is configured for sent IS-IS frames for both level 1 and level 2.

Mode

IS-IS router configuration.

Usage

The "no" form of this command removes the IS-IS authentication send only configuration for the specified level or both level 1 and level 2.

Example

This example shows how to configure the IS-IS authentication on sent IS-IS frames only for level 1:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->authentication send-only level-1
S Chassis(rw-config-isis)->
```

distance (IS-IS)

Use this command to configure the administrative distance for IS-IS routes.

Syntax

distance [**isis** {**external** | **internal**}] *weight*

no distance [**isis** {**external** | **internal**}]

Parameters

isis external | **internal**	(Optional) Applies the distance value to either external or internal routes only. **Note:** The value for intra-area distance must be less than the value for external distance.
weight	Specifies an administrative distance for IS-IS routes. Valid values are **1**-**255**. Default: **115**.

Defaults

If route type is not specified, the distance value will be applied to all IS-IS routes.

Mode

IS-IS router configuration or IS-IS IPv6 unicast address family configuration.

Usage

If several routes (coming from different protocols) are presented to the Extreme Networks S-Series Route Table Manager (RTM), the protocol with the lowest administrative distance will be chosen for route installation. By default, IS-IS administrative distance is set to 110. The **distance** command can be used to change this value, resetting IS-IS's route preference in relation to other routes as shown in the table below.

Route Source	Default Distance
Connected	0
Static	1
BGP	20 - Routes external to the AS 200 - Routes internal to the AS
OSPF	110
RIP	120

You must be in IS-IS IPv6 unicast address family configuration mode to configure distance on an IPv6 IS-IS router instance. Use "address-family" on page 75-3 to enter IS-IS IPv6 unicast address family configuration mode.

The **distance isis** command applies the value to the specified external or internal route type only.

The "no" form of this command resets IS-IS administrative distance to the default value of **115**.

Example

This example shows how to change the administrative distance for external IS-IS routes to 100:

```
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->distance isis external 100
```

domain-password

Use this command to configure the IS-IS domain password for this device.

Syntax

domain-password *password*

no domain-password *password*

Parameters

password	Specifies the password for routers that interconnect IS-IS domains.

Defaults

None.

Mode

IS-IS router configuration.

Usage

Configuring a domain password enables authentication on the device.

A key chain or domain password can be configured for the device, but not both a key chain and password. If a key chain is configured for the device, it must be removed before attempting to configure a domain password. The domain password can be overridden by configuring either a key chain or a password on the interface. A device level domain password can coexist with an

interface key chain because the interface is checked first, and if either an interface key chain or password exist, the device level configuration is not checked.

The “no” form of this command removes the IS-IS domain password configuration for this device.

Example

This example shows how to configure the IS-IS domain password to Area1ToArea2:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->domain-password Area1ToArea2
S Chassis(rw-config-isis)->
```

graceful-restart enable

Use this command to enable IS-IS graceful restart.

Syntax

graceful-restart enable

no graceful-restart enable

Parameters

None.

Defaults

Graceful restart is disabled by default.

Mode

IS-IS router configuration.

Usage

The “no” form of this command configure graceful restart for the default state of disabled.

Example

This example shows how to enable IS-IS graceful restart:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->graceful-restart enable
S Chassis(rw-config-isis)->
```

graceful-restart enable-help-peer

Use this command to enable helping a peer to restart.

Syntax

graceful-restart enable-help-peer

no graceful-restart enable-help-peer

Parameters

None.

Defaults

Graceful restart helping a peer to restart is enabled by default.

Mode

IS-IS router configuration.

Usage

The "no" form of this command disables graceful restart helping a peer functionality on this router.

Example

This example shows how to disable IS-IS graceful restart helping a peer:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->no graceful-restart enable-help-peer
S Chassis(rw-config-isis)->
```

graceful-restart restart-adj-interval

Use this command to configure the length of time graceful restart waits for the adjacency to form.

Syntax

graceful-restart restart-adj-interval *interval*

no graceful-restart restart-adj-interval

Parameters

interval	Specifies the restart adjacency interval in seconds. Valid values are 1 – 3600. The default value is 10 seconds.

Defaults

The restart adjacency interval defaults to 10 seconds.

Mode

IS-IS router configuration.

Usage

The "no" form of this command resets the restart adjacency interval to the default value of 10 seconds.

Example

This example shows how to set the restart adjacency interval to 15 seconds:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->graceful-restart restart-adj-interval 15
S Chassis(rw-config-isis)->
```

graceful-restart restart-interval

Use this command to configure the length of time graceful restart will attempt to complete a restart before terminating.

Syntax

graceful-restart restart-interval *interval*

no graceful-restart restart-interval

Parameters

interval	Specifies the length of time in seconds graceful restart will attempt to complete a restart before terminating. Valid values are 1 – 65535. The default value is 65535 seconds.

Defaults

The restart interval defaults to 65535 seconds.

Mode

IS-IS router configuration.

Usage

The “no” form of this command resets the restart interval to the default value of 65535 seconds.

Example

This example shows how to set the restart interval to 35000 seconds:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->graceful-restart restart-interval 35000
S Chassis(rw-config-isis)->
```

graceful-restart restart-sync-interval

Use this command to configure the length of time to allow for database re-synchronization during a graceful restart.

Syntax

graceful-restart restart-sync-interval {**level-1** | **level-1-2** | **level-2**} *interval*

no graceful-restart restart-sync-interval {**level-1** | **level-1-2** | **level-2**}

Parameters

level-1	Specifies this router is an IS-IS level 1 router.
level-1-2	Specifies this router is an IS-IS level 1 and level 2 router.
level-2	Specifies this router is an IS-IS level 2 router.
interval	Specifies the length of time in seconds to allow for database re-synchronization during a graceful restart for the specified router level. Valid values are 1 – 3600. The default value is 60 seconds.

Defaults

The restart sync interval defaults to 60 seconds.

Mode

IS-IS router configuration.

Usage

The "no" form of this command resets the restart sync interval to the default value of 60 seconds.

Example

This example shows how to set the restart sync interval to 70 seconds for this level 1 and level 2 router:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->graceful-restart restart-sync-interval level-1-2 75
S Chassis(rw-config-isis)->
```

hostname dynamic

Use this command to configure a dynamic hostname.

Syntax

hostname dynamic *hostname*

no hostname dynamic *hostname*

Parameters

hostname	Specifies a dynamic hostname. Valid values are up to 255 alpha-numeric characters.

Defaults

None.

Mode

IS-IS router configuration.

Usage

The "no" form of this command deletes the specified hostname.

Example

This example shows how to configure the hostname to **host1**:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->hostname dynamic host1
S Chassis(rw-config-isis)->
```

ignore-lsp-errors

Use this command to enable IS-IS to ignore link state packet checksum errors on the device.

Syntax

ignore-lsp-errors

no ignore-lsp-errors

Parameters

None.

Defaults

None.

Mode

IS-IS router configuration.

Usage

By default, IS-IS link state packets that are received with internal checksum errors are purged by the receiver. This command overrides that default behavior and simply ignores internal checksum errors for received link state packets.

The “no” form of this command restores the default behavior of purging link state packets with internal checksum errors.

Example

This example shows how to configure IS-IS to ignore link-state packet internal checksum errors:

```
S Chassis(rw-config)router isis
S Chassis(rw-config-isis)->ignore-lsp-errors
S Chassis(rw-config-isis)->
```

is-type

Use this command to configure the IS-IS type for this IS-IS instance.

Syntax

is-type {**level-1** | **level-1-2** | **level-2**}

no is-type {**level-1** | **level-1-2** | **level-2**}

Parameters

level-1	Specifies that the IS-IS routing instance type as an area level 1.
level-1-2	Specifies that the IS-IS routing instance type as both area level 1 and domain level 2 (Default).
level-2	Specifies that the IS-IS routing instance type as domain level 2.

Defaults

None.

Mode

IS-IS router configuration.

Usage

The "no" form of this command resets the IS-IS type for the routing instance to the default value of both level 1 and level 2.

Example

This example shows how to configure the IS-IS type for this routing instance to level 1:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->is-type level-1
S Chassis(rw-config-isis)->
```

lsp-buf-size

Use this command to configure the LSP buffer size based upon the specified maximum size of LSPs originated by this IS-IS routing instance.

Syntax

lsp-buf-size *size* [**level-1** | **level-1-2** | **level-2**]

no lsp-buf-size *size*

Parameters

size	Specifies the maximum allowed size of LSPs originated by this IS-IS routing instance. Valid values are 500 - 16000 bytes. The default value is 1492.
level-1	(Optional) Specifies that the configured maximum LSP size is restricted to level 1.
level-1-2	(Optional) Specifies that the configured maximum LSP size is for both level 1 and level 2. (Default).
level-2	(Optional) Specifies that the configured maximum LSP size is restricted to level 2.

Defaults

If no level option is specified, this configuration applies to both level 1 and level 2 routers.

Mode

IS-IS router configuration.

Usage

Using LSP sizes greater than 1492 bytes requires that the size of the IS-IS database be increased. This command increases the size of the IS-IS database to account for larger LSP sizes. The “no” form of this command resets the maximum size of LSPs that originate from this IS-IS instance to the default value of 1492.

Example

This example shows how to configure the maximum size of LSPs that originate from this IS-IS instance to 1600:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->lsp-buf-size 1600
S Chassis(rw-config-isis)->
```

lsp-gen-interval

Use this command to configure the minimum interval between the generation of LSPs.

Syntax

lsp-gen-interval *interval* [**level-1** | **level-1-2** | **level-2**]

no lsp-gen-interval *interval*

Parameters

interval	Specifies the minimum interval in seconds between the generation of LSPs for this routing instance. Valid values are 1 - 120 seconds. The default value is 1 second.
level-1	(Optional) Specifies that the configured minimum interval between the generation of LSPs is restricted to level 1.
level-1-2	(Optional) Specifies that the configured minimum interval between the generation of LSPs is for both level 1 and level 2. (Default).
level-2	(Optional) Specifies that the configured minimum interval between the generation of LSPs is restricted to level 2.

Defaults

If no level option is specified, this configuration applies to both level 1 and level 2 routers.

Mode

IS-IS router configuration.

Usage

The “no” form of this command resets the minimum interval between the generation of LSPs to the default value of 1 second.

Example

This example shows how to configure the minimum interval between the generation of LSPs to 3 seconds:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->lsp-gen-interval 3
S Chassis(rw-config-isis)->
```

max-lsp-lifetime

Use this command to configure the maximum time that LSPs persist without being refreshed.

Syntax

max-lsp-lifetime *lifetime*

no max-lsp-lifetime *lifetime*

Parameters

lifetime	Specifies the maximum LSP lifetime in seconds. Valid values are **1200** - **65535** seconds. The default value is **1200** seconds.

Defaults

None.

Mode

IS-IS router configuration.

Usage

The “no” form of this command resets the maximum time that LSPs persist without being refreshed to the default value of **1200** seconds.

Example

This example shows how to configure the maximum LSP lifetime to 1500 seconds:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->max-lsp-lifetime 1500
S Chassis(rw-config-isis)->
```

maximum-paths

Use this command to configure the maximum number of parallel routes to be installed into the routing table for this device.

Syntax

maximum-paths *num*

no maximum-paths *num*

Parameters

num	Specifies the maximum number of paths to be installed into the routing table for this device. Valid values are 1 - 32 routes. The default value is 8 routes.

Defaults

None.

Mode

IS-IS router configuration.

Usage

The “no” form of this command resets the maximum number of parallel routes to be installed into the routing table to the default value of 8 routes.

Example

This example shows how to configure the maximum number of parallel routes installable in the routing table to 12:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->maximum-paths 12
S Chassis(rw-config-isis)->
```

metric-style

Use this command to configure the TLV metric style for this IS-IS instance.

Syntax

metric-style {**wide** | **both**}

no metric-style

Parameters

wide	Specifies the wide TLV metric style.
both	Specifies both the wide TLV metric style and the narrow metric style (Default).

Defaults

None.

Mode

IS-IS router configuration.

Usage

The “no” form of this command resets the TLV metric style used for this routing instance to the default value of both wide and narrow TLV metric styles.

Example

This example shows how to configure the IS-IS metric style to wide only:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->metric-style wide
S Chassis(rw-config-isis)->
```

net

Use this command to configure the Network Entity Title (NET) that specifies the area address and the system ID for for this IS-IS router.

Syntax

net *net*

no net *net*

Parameters

net	Specifies a NET for this IS-IS routing instance in the format: *xx.xxxx*.(...).*xxxx.xxxx.xxxx*.**00** where (...) indicates a variable number of *xxxx* area address segments.

Defaults

None.

Mode

IS-IS router configuration.

Usage

A NET is a Network Service Access Point (NSAP) address of varying length where the last byte (the NSAP-selector) is always zero. All routers within an IS-IS domain must use the same length NET. The first variable number of bytes identify the area, followed by seven fixed bytes that are divided between six bytes identifying the system ID and a single selector byte. Each router has a unique system identifier. To configure separate areas for the router, enter each area number, followed by the unique system ID for this router, followed by 00 (the NSAP-selector octet). For example: NET address **12.3333.4444.5555.6666.00** has an

- Area of **12.3333**
- System identifier of **4444.5555.6666**
- NSAP-selector of **00**

The “no” form of this command removes the configured NET for this IS-IS router.

Example

This example shows how to configure the NET with an area of **47**, a system identifier of **1000.5000.0001**, and a NSAP-selector of **00** for this router:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
```

```
S Chassis(rw-config-isis)->net 47.1000.5000.0001.00
S Chassis(rw-config-isis)->
```

redistribute

Use this command to allow routing information discovered through non-IS-IS protocols or IS-IS level 2 to be distributed in IS-IS update messages.

Syntax

redistribute {**bgp** | **connected** | **ospf** *process_id*| **rip** | **static** | **blackhole** | **isis level-2 into level-1** [**distribute-list** *access-list*]} [**route-map** *name*] [**metric** *metric-value*]

no redistribute {**bgp** | **connected** | **ospf** *process_id*| **rip** | **static** | **blackhole** | **isis level-2 into level-1** [**distribute-list** *access-list*]}

Parameters

bgp	Specifies that BGP routing information will be redistributed in IS-IS.
connected	Specifies that non-IS-IS information discovered via directly connected interfaces will be redistributed. These are routes not specified in the IS-IS network command as described in "net" on page 75-18.
ospf *process_id*	Specifies that OSPF routing information for the specified process will be redistributed in IS-IS.
rip	Specifies that RIP routing information will be redistributed in IS-IS.
static	Specifies that non-IS-IS information discovered via static routes will be redistributed. Static routes are those created using the **ip route** command detailed in "ip route" on page 56-5.
blackhole	Specifies that blackhole routes are redistributed in IS-IS.
route-map *name*	(Optional) Redistributes routes using the rules established by the designated route-map.
metric *metric-value*	(Optional) Specifies a metric for the BGP, connected, RIP, or static redistribution route. This value should be consistent with the designated protocol.
isis level-2 into level-1	(Optional) Specifies that IS-IS level 2 routes will be redistributed into IS-IS level 1.
distribute-list *access-list*	(Optional) Specifies an ACL for the the filtering of IS-IS level 2 routes into IS-IS level 1.

Defaults

- If **route-map** is not specified, none will be applied.
- If *metric-value* is not specified, a metric value of **20** will be applied.

Mode

IS-IS router configuration for IPv4 addresses.

IPv6 unicast address family configuration for IPv6 addresses.

Usage

You must be in IS-IS IPv6 unicast address family configuration mode to configure redistribution on an IPv6 IS-IS router instance. Use "address-family" on page 75-3 to enter IS-IS IPv6 unicast address family configuration mode.

If you do not specify a distribute list when redistributing IS-IS level 2 routes into IS-IS level 1, all layer 2 addresses are redistributed into layer 1.

The "no" form of this command clears redistribution parameters.

Example

This example shows how to distribute RIP routing information from IPv4 routes in IS-IS updates:

```
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->redistribute rip
```

This example shows how to distribute RIP routing information from IPv6 routes in IS-IS updates:

```
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->address-family ipv6 unicast
S Chassis(rw-config-isis-af)->redistribute rip
S Chassis(rw-config-isis-af)->
```

set-overload-bit

Use this command to configure the router to signal other routers not to use it as an intermediate hop in their SPF calculations.

Syntax

set-overload-bit [**level-1** | **level-1-2** | **level-2**]

no set-overload-bit

Parameters

level-1	(Optional) Specifies that the set overload bit configuration is restricted to level 1.
level-1-2	(Optional) Specifies that the set overload bit configuration is for both level 1 and level 2. (Default).
level-2	(Optional) Specifies that the set overload bit configuration is restricted to level 2.

Defaults

If no level option is specified, this configuration is applied to both level 1 and level 2 routers.

Mode

IS-IS router configuration.

Usage

The overload bit is not set by default. Other routers can use this router as an intermediate hop in their SPF calculations.

The "no" form of this command resets set overload bit setting to the default value of not set.

Example

This example shows how to instruct other routers not to use this router as an intermediate hop in their SPF calculations:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->set-overload-bit
S Chassis(rw-config-isis)->
```

spf-interval

Use this command to configure the minimum amount of time between Shortest Path First (SPF) processing on an IS-IS instance.

Syntax

spf-interval *interval*

no spf-interval *interval*

Parameters

interval	Specifies the time delay (in milli-seconds) between successive SPFs. Valid values are **0** - **5000** milli-seconds. Default value is **33** milli-seconds.

Defaults

None.

Mode

IS-IS router configuration.

Usage

When a topology change occurs the SPF calculation is run. The SPF calculation is not run when external routes change.

The SPF calculation is CPU intensive. For a network with a large area and frequent topology changes you may want to increase the minimum time between SPF calculations. Increasing the SPF interval reduces the processor load, but potentially slows the rate of convergence.

The “no” form of this command resets the minimum interval between consecutive SPFs to the default value of 33 milli-seconds.

Example

This example shows how to set the interval between consecutive SPFs to 75 milli-seconds:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->spf-interval 75
S Chassis(rw-config-isis)->
```

summary-address

Use this command to create an aggregate IS-IS address for summarization of routes.

Syntax

summary-address *ip-address/length*

no summary-address *ip-address/length*

Parameters

ip-address/length	Specifies an IP address in dotted notation followed by the length.

Defaults

None.

Mode

IS-IS router configuration for IPv4 addresses.

IPv6 unicast address family configuration for IPv6 addresses.

Usage

Summarizing addresses reduces the number of LSPs and the size of the link state database. Multiple addresses can be summarized for a given IS-IS instance.

To summarize a unicast IPv6 address, you must be in the IPv6 unicast family address configuration mode. Use "address-family" on page 75-3 to enter IPv6 unicast family address configuration mode.

The "no" form of this command deletes the IS-IS aggregate address configuration.

Example

This example shows how to apply address summarization to prefix **20.10.1.0/24**:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->summary-address 20.10.1.0/24
S Chassis(rw-config-isis)->
```

This example shows how to apply address summarization to prefix **2003:2010::0/64**:

```
S Chassis(rw)->configure
S Chassis(rw-config)->router isis
S Chassis(rw-config-isis)->address-family ipv6 unicast
S Chassis(rw-config-isis-af)->summary-address 2003:2010::0/64
S Chassis(rw-config-isis-af)->
```

Interface Commands

For information about...	Refer to page...
ip router isis	75-23

For information about...	Refer to page...
ipv6 router isis	75-24
isis authentication key-chain	75-24
isis authentication mode	75-25
isis authentication send-only	75-26
isis circuit-type	75-27
isis csnp-interval	75-28
isis hello-interval	75-29
isis hello-multiplier	75-30
isis hello-padding	75-30
isis lsp-mtu	75-31
isis lsp-throttle	75-32
isis metric	75-33
isis network-point-to-point	75-33
isis passive-interface	75-34
isis password	75-35
isis priority	75-35
isis retransmit-interval	75-36

ip router isis

Use this command to enable or disable IPv4 Intermediate System to Intermediate System (IS-IS) routing on the interface.

Syntax

```
ip router isis
no ip router isis
```

Parameters

None.

Defaults

None.

Mode

Interface configuration.

Usage

The “no” form of this command disables the IPv4 IS-IS routing on the interface.

Example

This example shows how to enable IPv4 IS-IS routing on VLAN 100:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 100
S Chassis(rw-config-intf-vlan.0.100)->ip router isis
S Chassis(rw-config-isis)->
```

ipv6 router isis

Use this command to enable or disable IPv6 Intermediate System to Intermediate System (IS-IS) routing on the interface.

Syntax

ipv6 router isis

no ipv6 router isis

Parameters

None.

Defaults

None.

Mode

Interface configuration.

Usage

The “no” form of this command disables the IPv6 IS-IS routing on the interface.

Example

This example shows how to enable IPv6 IS-IS routing on VLAN 100:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 100
S Chassis(rw-config-intf-vlan.0.100)->ipv6 router isis
S Chassis(rw-config-isis)->
```

isis authentication key-chain

Use this command to configure IS-IS authentication key chain on an interface.

Syntax

isis authentication key-chain *keychain* [**level-1** | **level-2**]

no isis authentication key-chain *keychain* [**level-1** | **level-2**]

Parameters

keychain	Specifies the name of the key chain. Valid values are up to 16 alpha-numeric characters.
level-1	(Optional) Specifies that the key chain configuration should be restricted to level 1.
level-2	(Optional) Specifies that the key chain configuration should be restricted to level 2.

Defaults

If no level option is specified, the key chain is applied to both level 1 and level 2.

Mode

Interface configuration.

Usage

Key chain authentication is only performed if a key chain is configured.

Entering a key chain on an interface overrides any device level key chain or password configuration. Both a key chain and password can not coexist on an interface. If a password configuration already exists on the interface, it must be removed before configuring an interface level key chain.

You can specify authentication for an entire instance of IS-IS instead of at the interface level using "authentication key-chain" on page 75-4.

The "no" form of this command removes the authentication key-chain interface configuration.

Example

This example shows how to configure the VLAN 100 IS-IS authentication key chain to **keychainlv1** and restricts the key chain configuration to level 1:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 100
S Chassis(rw-config-intf-vlan.0.100)->isis authentication key-chain keychainlv1
level-1
S Chassis(rw-config-intf-vlan.0.100)->
```

isis authentication mode

Use this command to configure IS-IS authentication mode on an interface.

Syntax

```
isis authentication mode {md5 | text} [level-1 | level-2]
no isis authentication mode {md5 | text} [level-1 | level-2]
```

Parameters

md5	Specifies MD5 as the IS-IS authentication mode for the interface.
text	Specifies text as the IS-IS authentication mode for the interface.

level-1	(Optional) Specifies that the authentication mode configuration should be restricted to level 1.
level-2	(Optional) Specifies that the authentication mode configuration should be restricted to level 2.

Defaults

If no level option is specified, the mode configuration is applied to both level 1 and level 2.

Mode

Interface configuration.

Usage

The IS-IS MD5 mode authentication provides a cryptographic hash MD5 digest to each IS-IS PDU, preventing unauthorized routing messages to enter the IS-IS domain.

IS-IS has five packet types: link state packet (LSP), LAN Hello, Serial Hello, CSNP, and PSNP. The MD5 authentication or the clear text password authentication is applied to each IS-IS PDU type. The IS-IS authentication defaults to level 1 and level 2 and can be restricted to level 1 or level 2.

The authentication mode for the interface can be configured without a preexisting key chain or password configuration, but interface level authentication is not enable until either a key chain or password is configured for the interface.

The “no” form of this command removes the interface IS-IS authentication mode configuration.

Example

This example shows how to configure VLAN 100 IS-IS authentication to MD5 for a level 1 instance:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 100
S Chassis(rw-config-intf-vlan.0.100)->isis authentication mode md5 level-1
S Chassis(rw-config-intf-vlan.0.100)->
```

isis authentication send-only

Use this command to configure IS-IS authentication only on sent IS-IS frames on an interface.

Syntax

```
isis authentication send-only [level-1 | level-2]
no isis authentication send-only [level-1 | level-2]
```

Parameters

level-1	(Optional) Specifies that the authentication send-only configuration should be restricted to level 1.
level-2	(Optional) Specifies that the authentication send-only configuration should be restricted to level 2.

Defaults

If no option is specified, IS-IS authentication is configured for sent IS-IS frames only for both level 1 and level 2.

Mode

Interface configuration.

Usage

The "no" form of this command removes the IS-IS authentication send only configuration.

Example

This example shows how to configure VLAN 100 to authenticate sent IS-IS frames only for level 1:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 100
S Chassis(rw-config-intf-vlan.0.100)->authentication send-only level-1
S Chassis(rw-config-intf-vlan.0.100)->
```

isis circuit-type

Use this command to configure the IS-IS type for an interface.

Syntax

isis circuit-type {**level-1** | **level-1-2** | **level-2**}

no isis circuit-type {**level-1** | **level-1-2** | **level-2**}

Parameters

level-1	Specifies that the IS-IS type is level 1 for the interface.
level-1-2	Specifies that the IS-IS type is both level 1 and level 2 for the interface (Default).
level-2	Specifies that the IS-IS type is level 2 for the interface.

Defaults

None.

Mode

Interface configuration.

Usage

The "no" form of this command resets the IS-IS type to the default value of both level 1 and level 2 for the interface.

Example

This example shows how to configure the IS-IS type to level 1 for VLAN 100:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 100
```

```
S Chassis(rw-config-intf-vlan.0.100)->isis circuit-type level-1
S Chassis(rw-config-intf-vlan.0.100)->
```

isis csnp-interval

Use this command to configure the IS-IS complete sequence number PDU (CSNP) interval for the interface.

Syntax

isis csnp-interval *seconds* [**level-1** | **level-1-2** | **level-2**]

no isis csnp-interval *seconds* [**level-1** | **level-1-2** | **level-2**]

Parameters

seconds	Specifies the number of seconds between IS-IS sequence number PDUs on the interface. Valid values are **1** - **600**. The default value is **10** seconds.
level-1	(Optional) Specifies that the CSNP interval is applied to level 1 for the interface.
level-1-2	(Optional) Specifies that the CSNP interval is applied to both level 1 and level 2 for the interface (Default).
level-2	(Optional) Specifies that the IS-IS CSNP interval is applied to level 2 for the interface.

Defaults

If an IS-IS level is not specified, the level type defaults to both level 1 and level 2.

Mode

Interface configuration.

Usage

Designated Routers (DRs) send out CSNP packets on the interface to maintain database synchronization.

The “no” form of this command resets the CSNP interval to the default value of 10 seconds for the interface.

Example

This example shows how to configure the IS-IS complete sequence number PDU interval to 15 seconds:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 100
S Chassis(rw-config-intf-vlan.0.100)->isis csnp-interval 15
S Chassis(rw-config-intf-vlan.0.100)->
```

isis hello-interval

Use this command to configure the IS-IS Hello Protocol Data Units (IIH) interval for the interface.

Syntax

```
isis hello-interval {seconds | minimal} [level-1 | level-1-2 | level-2]
no isis hello-interval seconds [level-1 | level-1-2 | level-2]
```

Parameters

seconds	Specifies the number of seconds between IS-IS IIH PDUs on the interface. Valid values are **1** - **600**. The default value is **10** seconds.
minimal	Sets the hello interval such that the resulting hold time is **1** second.
level-1	(Optional) Specifies that the hello interval is applied to level 1 for the interface.
level-1-2	(Optional) Specifies that the hello interval is applied to both level 1 and level 2 for the interface (Default).
level-2	(Optional) Specifies that the IS-IS hello interval is applied to level 2 for the interface.

Defaults

If an IS-IS level is not specified, the level type defaults to both level 1 and level 2.

Mode

Interface configuration.

Usage

The advertised holdtime in the hello packet is set to three times the hello interval seconds. The holdtime multiplier can be changed using “isis hello-multiplier” on page 75-30. Topological changes are detected faster with a smaller hello interval, but there is more routing traffic.

The “no” form of this command resets the hello interval to the default value of **10** seconds for the interface.

Example

This example shows how to configure the IS-IS hello interval to **15** seconds:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 100
S Chassis(rw-config-intf-vlan.0.100)->isis hello-interval 15
S Chassis(rw-config-intf-vlan.0.100)->
```

isis hello-multiplier

Use this command to configure the number of hello packets a neighbor must miss before the router declares the adjacency down for the interface.

Syntax

isis hello-multiplier *multiplier* [**level-1** | **level-1-2** | **level-2**]

no isis hello-multiplier *multiplier* [**level-1** | **level-1-2** | **level-2**]

Parameters

multiplier	Specifies the number of hello packets a neighbor must miss before the router declares the adjacency down. Valid values are **2** - **100**. The default value is **3**.
level-1	(Optional) Specifies that the hello multiplier is applied to level 1 for the interface.
level-1-2	(Optional) Specifies that the hello multiplier is applied to both level 1 and level 2 for the interface (Default).
level-2	(Optional) Specifies that the IS-IS hello multiplier is applied to level 2 for the interface.

Defaults

If an IS-IS level is not specified, the level type defaults to both level 1 and level 2.

Mode

Interface configuration.

Usage

The “no” form of this command resets the hello multiplier to the default value of 3 hello packets for the interface.

Example

This example shows how to configure the number of missed hello packets before declaring the adjacency down to 5:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 100
S Chassis(rw-config-intf-vlan.0.100)->isis hello-multiplier 5
S Chassis(rw-config-intf-vlan.0.100)->
```

isis hello-padding

Use this command to configure IS-IS hello padding on an interface.

Syntax

isis hello-padding

no isis hello-padding

Parameters

None.

Defaults

None.

Mode

Interface configuration.

Usage

IS-IS hello packets by default are padded to the MTU size. Hello padding allows for early detection of errors that result from transmission problems with large frames or errors that result from mismatched MTUs on an interface.

Disabling hello padding lowers network bandwidth usage.

The "no" form of this command disables hello padding on the interface.

Example

This example shows how to disable hello padding on VLAN 100:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 100
S Chassis(rw-config-intf-vlan.0.100)->no isis hello-padding
S Chassis(rw-config-intf-vlan.0.100)->
```

isis lsp-mtu

Use this command to configure the maximum PDU size for PDUs on the interface.

Syntax

isis lsp-mtu *size*

no isis lsp-mtu *size*

Parameters

size	Specifies the maximum size of PDUs allowed on the interface. Valid values are **1000** - **5000** bytes. The default value is **1490** bytes.

Defaults

None.

Mode

Interface configuration.

Usage

The "no" form of this command resets the maximum PDU size allowed for the interface to the default value of 1490 bytes.

Example

This example shows how to configure the maximum allowed PDU size for VLAN **100** to **2500** bytes:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 100
S Chassis(rw-config-intf-vlan.0.100)->isis lsp-mtu 2500
S Chassis(rw-config-intf-vlan.0.100)->
```

isis lsp-throttle

Use this command to configure minimum interval between the transmission of Link-State Packets (LSPs).

Syntax

isis lsp-throttle *interval*

no isis lsp-throttle *interval*

Parameters

interval	Specifies the minimum interval in milli-seconds between the transmission of LSPs. Valid values are **1** - **65535** milli-seconds. The default value is **30** milli-seconds.

Defaults

None.

Mode

Interface configuration.

Usage

The “no” form of this command resets the minimum interval in milli-seconds between the transmission of LSPs to the default value of 30 milli-seconds.

Example

This example shows how to configure the minimum interval between the transmission of LSPs to 3 seconds:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 100
S Chassis(rw-config-intf-vlan.0.100)->isis lsp-throttle 3000
S Chassis(rw-config-intf-vlan.0.100)->
```

isis metric

Use this command to configure the cost of using the interface.

Syntax

isis metric *cost* [**level-1** | **level-1-2** | **level-2**]

no isis metric *cost* [**level-1** | **level-1-2** | **level-2**]

Parameters

cost	Specifies the cost of using the interface. Valid values are **1** - **16777215**. The default value is **10**.
level-1	(Optional) Specifies that the configured cost is applied to level 1 for the interface.
level-1-2	(Optional) Specifies that the configured cost is applied to both level 1 and level 2 for the interface (Default).
level-2	(Optional) Specifies that the configured cost is applied to level 2 for the interface.

Defaults

If an IS-IS level is not specified, the level type defaults to both level 1 and level 2.

Mode

Interface configuration.

Usage

The “no” form of this command resets the interface cost to the default value of **10**.

Example

This example shows how to configure the cost of VLAN **100** to **15** for level 1:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 100
S Chassis(rw-config-intf-vlan.0.100)->isis metric 15 level-1
S Chassis(rw-config-intf-vlan.0.100)->
```

isis network-point-to-point

Use this command to configure a two device network that uses broadcast media and IS-IS to function as a point-to-point link.

Syntax

isis network-point-to-point

no isis network-point-to-point

Parameters

None.

Defaults

None.

Mode

Interface configuration.

Usage

This command configures the interface to be part of a two device network that uses broadcast media and IS-IS routing to function as a point-to-point link instead of a broadcast link. Network point-to-point mode causes the system to issue packets point-to-point rather than as broadcasts for the interface.

The “no” form of this command disables network point-to-point functionality on the interface.

Example

This example shows how to enable VLAN 100 for network point-to-point:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 100
S Chassis(rw-config-intf-vlan.0.100)->isis network-point-to-point
S Chassis(rw-config-intf-vlan.0.100)->
```

isis passive-interface

Use this command to suppress IS-IS packets from being transmitted by the interface and received packets from being processed on the interface.

Syntax

isis passive-interface

no isis passive-interface

Parameters

None.

Defaults

None.

Mode

Interface configuration.

Usage

The “no” form of this command disables passive interface mode on the interface.

Example

This example shows how to enable passive-interface mode on VLAN 100:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 100
S Chassis(rw-config-intf-vlan.0.100)->isis passive-interface
```

```
S Chassis(rw-config-intf-vlan.0.100)->
```

isis password

Use this command to configure an authentication password for the interface.

Syntax

isis password *password* [**level-1** | **level-2**]

no isis password *password* [**level-1** | **level-2**]

Parameters

password	Specifies an authentication password for the interface.
level-1	(Optional) Specifies that the configured password is applied to level 1 for the interface.
level-2	(Optional) Specifies that the configured password is applied to level 2 for the interface.

Defaults

If an IS-IS level is not specified, the level type defaults to both level 1 and level 2.

Mode

Interface configuration.

Usage

Entering a password on an interface overrides any device level key chain or password configuration for the interface. Both a key chain and password can not coexist on an interface. If a key chain configuration already exists on the interface, it must be removed before configuring an interface level password.

The “no” form of this command removes the IS-IS password configuration on the interface.

Example

This example shows how to configure the authentication password for VLAN **100** to **password**:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 100
S Chassis(rw-config-intf-vlan.0.100)->isis password password
S Chassis(rw-config-intf-vlan.0.100)->
```

isis priority

Use this command to configure the priority used to determine which router on a LAN is the designated router.

Syntax

isis priority *priority* [**level-1** | **level-1-2** | **level-2**]

no isis priority *priority* [**level-1** | **level-1-2** | **level-2**]

Parameters

priority	Specifies the interface priority used in selecting the designated router. Valid values are **0** - **127**. The default value is **64**.
level-1	(Optional) Specifies that the configured priority is applied to level 1 for the interface.
level-1-2	(Optional) Specifies that the configured priority is applied to both level 1 and level 2 for the interface (Default).
level-2	(Optional) Specifies that the configured priority is applied to level 2 for the interface.

Defaults

If an IS-IS level is not specified, the level type defaults to both level 1 and level 2.

Mode

Interface configuration.

Usage

The priority is used to determine the designated router. The router with the highest priority becomes the designated router. IS-IS does not support the concept of a backup designated router. Setting the priority to 0 does not prevent this system from becoming the designated router. If priorities are equal, the interface with the highest MAC address breaks the tie.

The "no" form of this command resets the interface priority to the default value of **64**.

Example

This example shows how to configure VLAN **100** for a priority of 80:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 100
S Chassis(rw-config-intf-vlan.0.100)->isis priority 80
S Chassis(rw-config-intf-vlan.0.100)->
```

isis retransmit-interval

Use this command to configure the minimum interval between retransmissions of the same LSP.

Syntax

isis retransmit-interval *interval*

no isis retransmit-interval *interval*

Parameters

interval	Specifies the minimum interval between retransmissions of the same LSP in seconds. Valid values are **1** - **300**. The default value is **5**.

Defaults

None.

Mode

Interface configuration.

Usage

The retransmit interval should be greater than the expected round-trip delay between any two routers on the attached network. Retransmissions occur when LSPs are dropped. Higher retransmission values have little effect on reconvergence. The more neighbors routers have, and the more paths over which LSPs can be flooded, the higher this value can be made.

The "no" form of this command resets the retransmit interval to the default value of **5** seconds.

Example

This example shows how to configure the retransmit interval to **10** seconds for VLAN **100**:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 100
S Chassis(rw-config-intf-vlan.0.100)->isis retransmit-interval 10
S Chassis(rw-config-intf-vlan.0.100)->
```

Show Commands

For information about...	Refer to page...
show isis database	75-37
show isis hostname	75-39
show isis lsp-log	75-40
show isis neighbors	75-40
show isis topology	75-41

show isis database

Use this command to display IS-IS database information for the router.

Syntax

show isis database [**lsp** *lsp*] | [**level-1**] | [**level-2**] | [**detail**] | [**verbose**]

Parameters

lsp *lsp*	(Optional) Displays the IS-IS database information for the specified LSP in the format *xxxx.xxxx.xxxx.x-x*.
level-1	(Optional) Displays level 1 type IS-IS database information only.
level-2	(Optional) Displays level 2 type IS-IS database information only.
detail	(Optional) Displays a detailed level of IS-IS database information.
verbose	(Optional) Displays a verbose level of IS-IS database information.

Defaults

If no option is specified, all IS-IS database information displays for both level 1 and level 2.

Mode

All command modes.

Examples

This example shows how to display IS-IS database information:

```
S Chassis(rw)->show isis database
IS-IS Level-1 Link State Database:
LSPID             LSP Seq Num   LSP Checksum  LSP Holdtime   ATT/P/OL
4444.4444.4444.0-0       0x76           0x92E6        1055         0/0/0
4444.4444.4444.0-1       0x74           0x924         651          0/0/0
.
.
.
4444.4444.4444.0-7       0x97           0x629D        989          0/0/0
IS-IS Level-2 Link State Database:
LSPID             LSP Seq Num   LSP Checksum  LSP Holdtime   ATT/P/OL
4444.4444.4444.0-0       0x73           0x90f3        924          0/0/0
4444.4444.4444.0-1       0xf2           0x70c7        986          0/0/0
4444.4444.4444.0-2       0x7d           0xfc1f        906          0/0/0
.
.
.
4444.4444.5555.0-2 0xb0           0x69c3        986          0/0/0
```

This example shows how to display IS-IS database information for LSP **4444.4444.4444.0-0**:

```
S Chassis(rw)->show isis database lsp 4444.4444.4444.0-0
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num   LSP Checksum
4444.4444.4444.0-0       0X75          0X94E5
  NLPID:     0XCC 0X8E
  Area Address:     48.0001
  Area Address:     49.0001
  NLPID:     0XCC 0X8E
  Area Address:     48.0001
  Area Address:     49.0001
  NLPID:     0XCC 0X8E
  Area Address:     48.0001
  Area Address:     49.0001
  NLPID:     0XCC 0X8E
  Area Address:     48.0001
  Area Address:     49.0001
  NLPID:     0XCC 0X8E
  Area Address:     48.0001
  Area Address:     49.0001
```

```
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num   LSP Checksum
  NLPID:     0XCC 0X8E
  Area Address:     48.0001
  Area Address:     49.0001
  NLPID:     0XCC 0X8E
  Area Address:     48.0001
  Area Address:     49.0001
  NLPID:     0XCC 0X8E
  Area Address:     48.0001
  Area Address:     49.0001
  NLPID:     0XCC 0X8E
  Area Address:     48.0001
  Area Address:     49.0001
  NLPID:     0XCC 0X8E
  Area Address:     48.0001
  Area Address:     49.0001
S Chassis(rw)->
```

show isis hostname

Use this command to display the hostname per LSP ID.

Syntax

show isis hostname

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display IS-IS hostnames:

```
S Chassis(rw)->show isis hostname

Level      System ID          Dynamic Hostname
1           4444.4444.4444         44.44.44.44
2           4444.4444.4444         44.44.44.44
1           AAAA.AAAA.AAAA         7.7.7.7
2           AAAA.AAAA.AAAA         7.7.7.7
1           AAAA.AABB.BBBB         77.77.77.77
```

```
1           BBBB.BBAA.AAAA         88.88.88.88
S Chassis(rw)->
```

show isis lsp-log

Use this command to display the frequency and reason for LSP changes on an interface.

Syntax

show isis lsp-log

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display IS-IS hostnames:

```
S Chassis(rw)->show isis lsp-log
LAN Level 1 LSP Log:
Count             Interface         Triggers
  153                 100      ADJCHG NUMADJ DIS
  157                 100      ADJCHG NUMADJ DIS
  5                   500      ADJCHG NUMADJ DIS
  5                   500      ADJCHG NUMADJ DIS
  16                  700      ADJCHG NUMADJ DIS
  7                   700      ADJCHG DIS
  3                   901      ADJCHG NUMADJ DIS
  3                   1000     ADJCHG NUMADJ DIS
.
.
.
S Chassis(rw)->
```

show isis neighbors

Use this command to display IS-IS router neighbors.

Syntax

show isis neighbors

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display IS-IS neighbors:

```
S Chassis(rw)->show isis neighbors
System ID      Type   Interface    IP Address                    State   Holdtime   Circuit Id
4444.4444.4444   L1    vlan.0.500    23.0.0.44                    UP       24      AAAAAAAAAAAA
4444.4444.4444   L1    vlan.0.500    fe80::21f:45ff:fe4d:8768      UP       24      AAAAAAAAAAAA
BBBB.BBBB.BBBB   L1    vlan.0.500    23.0.0.8                     UP       25      AAAAAAAAAAAA
BBBB.BBBB.BBBB   L1    vlan.0.500    fe80::21f:45ff:fe62:98ee     UP       25      AAAAAAAAAAAA
4444.4444.4444   L2    vlan.0.500    23.0.0.44                    UP       29      AAAAAAAAAAAA
4444.4444.4444   L2    vlan.0.500    fe80::21f:45ff:fe4d:8768     UP       29      AAAAAAAAAAAA
BBBB.BBBB.BBBB   L2    vlan.0.500    23.0.0.8                     UP       26      AAAAAAAAAAAA
BBBB.BBBB.BBBB   L2    vlan.0.500    fe80::21f:45ff:fe62:98ee     UP       26      AAAAAAAAAAAA
BBBB.BBAA.AAAA   L1    vlan.0.700    6.6.6.88                     UP       7       BBBBBBAAAAAA
BBBB.BBAA.AAAA   L1    vlan.0.700    fe80::a8bb:ccff:fe06:688     UP       7       BBBBBBAAAAAA
S Chassis(rw)->
```

show isis topology

Use this command to display the IS-IS topology.

Syntax

show isis topology

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the IS-IS topology:

```
S Chassis(rw)->show isis topology
IS-IS paths to level-1 routers:
SystemId           Hostname         RouterID
4444.4444.4444     44.44.44.44
AAAA.AAAA.AAAA     7.7.7.7
AAAA.AABB.BBBB     77.77.77.77
```

```
BBBB.BBAA.AAAA      88.88.88.88
BBBB.BBBB.BBBB      8.8.8.8
DDCC.DDCC.DDCC      177.177.177.177
DDDD.DDDD.DDDD      188.188.188.188
S Chassis(rw)->
```

76

VRRP Commands

This chapter describes the Virtual Router Redundancy Protocol (VRRP) set of commands and how to use them. For information about configuring VRRP, refer to the "Virtual Router Redundancy Protocol (VRRP) Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
vrrp create	76-1
vrrp address	76-2
vrrp primary-address	76-3
vrrp priority	76-4
vrrp accept-mode	76-5
vrrp advertise-interval	76-6
vrrp authentication	76-7
vrrp critical-ip	76-7
vrrp enable	76-9
vrrp interface-up-delay	76-10
vrrp fabric-route-mode	76-10
vrrp host-mobility	76-11
vrrp host-mobility-acl	76-12
host-mobility timeout	76-13
vrrp preempt	76-14
vrrp preempt-delay	76-14
show ip vrrp	76-15

vrrp create

Creates a vrid instance for this interface

Syntax

vrrp create *vrid version*

no vrrp create *vrid version*

Parameters

vrid	Specifies the Virtual Router ID (VRID) to be used on this interface. Valid Values: **1** - **255**. Default Value: None.
version	Specifies the VRRP protocol version for this instance. Valid Values: • **v2-IPv4** - Supports version 2 of the VRRP protocol, RFC 2338 • **v3-IPv4** Supports version 3 of the VRRP protocol for IPv4, RFC 5798 • **v3-IPv6** - Supports version 3 of the VRRP protocol for IPv6, RFC 5798

Defaults

None.

Mode

Interface configuration mode.

Usage

This command must be executed to create an instance of VRRP on a routing interface (VLAN) before any other VRRP settings can be configured.

Up to 8 virtual router IDs can be associated with a given interface.

Up to 1024 VRRP sessions are supported per device.

The “no” form of this command removes the VRRP session.

Example

This example creates a VRRP instance 1 for the IPv4 version 2 VRRP protocol on VLAN 20:

```
S Chassis(rw)->configure
S Chassis(rw)-config)->interface vlan 20
S Chassis(rw)-config-intf-vlan.0.20)->vrrp create 1 v2-ipv4
S Chassis(rw)-config-intf-vlan.0.20)->
```

vrrp address

Adds an IP address to the associate list for this VRRP session.

Syntax

vrrp address *vrid ip-address* [**enable** | **disable**]

no vrrp address *vrid ip-address* [**enable** | **disable**]

Parameters

vrid	Specifies a unique Virtual Router ID (VRID) associated with this routing interface.
ip-address	Specifies the virtual router IP address to associate with the router.

enable | **disable**	Enables or disables the IP address for the VRRP session. If not specified, the default is enable. • **enable** - Address is active in the virtual address list that is being managed by the VRRP router. • **disable** - Address is not active in the virtual address list. A disabled address is not backed up by a VRRP router.

Defaults

If neither enable or disable are specified, the configuration defaults to enable.

Mode

Interface configuration mode.

Usage

If the virtual router IP address is the same as the interface (VLAN) address owned by a VRRP router, then the router owning the address becomes the master. The master sends an advertisement to all other VRRP routers declaring its status and assumes responsibility for forwarding packets associated with its virtual router ID (VRID).

If the virtual router IP address is not owned by any of the VRRP routers, then the routers compare their priorities and the higher priority owner becomes the master. If priority values are the same, then the VRRP router with the higher IP address is selected master. For details on using the **vrrp priority** command, refer to "vrrp priority" on page 76-4.

A virtual router IP address can be either an address configured on the routing interface or an address that falls within the range of any networks configured on the routing interface.

Up to 128 IPv4 and 64 IPv6 IP addresses are supported per interface.

The "no" form of this command clears the VRRP address configuration.

Example

This example adds the 20.20.20.1 IP address to the VRRP 1 instance:

```
S Chassis(rw)->configure
S Chassis(rw)-config)->interface vlan 20
S Chassis(rw)-config-intf-vlan.0.20)->vrrp create 1 v2-ipv4
S Chassis(rw)-config-intf-vlan.0.20)->vrrp address 1 20.20.20.1
S Chassis(rw)-config-intf-vlan.0.20)->
```

vrrp primary-address

Specifies the primary address for this virtual router.

Syntax

vrrp primary-address *vrid ip-address*

no vrrp primary-address *vrid ip-address*

Parameters

vrid	Specifies a unique Virtual Router ID (VRID) associated with this routing interface.

ip-address	Specifies the virtual router IP address to associate with the router.

Defaults

None.

Mode

Interface configuration mode.

Usage

This command sets the primary IP address that the specified VRID will use to a subnet address on the interface.

Note: When configuring an IPv6 VRRP link local address, all link local addresses must match on all routers running the same VRRP instance in a LAN segment. Only one link local address on a VRRP instance will be active at any given time.

The "no" form of this command clears the VRRP primary address configuration.

This example sets the 20.20.20.2 IP address as the primary address for the VRRP 1 instance:

```
S Chassis(rw)->configure
S Chassis(rw)-config)->interface vlan 20
S Chassis(rw)-config-intf-vlan.0.20)->vrrp create 1 v2-ipv4
S Chassis(rw)-config-intf-vlan.0.20)->vrrp primary-address 1 20.20.20.2
S Chassis(rw)-config-intf-vlan.0.20)->
```

vrrp priority

Configures the priority for this VRRP instance.

Syntax

vrrp priority *vrid priority*

no vrrp priority *vrid priority*

Parameters

vrid	Specifies a Virtual Router ID (VRID) associated with this priority.
priority	Specifies the VRRP priority value to associate with the *vrid*. Valid values are from **1** to **254**, with the highest value setting the highest priority. Priority value of **255** is reserved for the VRRP router that owns the IP address associated with the virtual router. Priority **0** is reserved for signaling that the master has stopped working and the backup router must transition to master state. Default: **100**.

Defaults

None.

Mode

Interface configuration mode.

Usage

The “no” form of this command clears the VRRP priority configuration.

Example

This example sets the priority for VRRP instance **1** to **5**:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 20
S Chassis(rw)-config-intf-vlan.0.20)->vrrp create 1 v2-ipv4
S Chassis(rw)-config-intf-vlan.0.20)->vrrp address 1 20.20.20.1
S Chassis(rw-config-intf-vlan.0.20)->vrrp priority 1 5
S Chassis(rw-config-intf-vlan.0.20)->
```

vrrp accept-mode

Enables the master of the VRID to accept IP packets destined for the IP addresses in the associated list, even if the router is not the owner of those addresses.

Syntax

vrrp accept-mode *vrid*

no vrrp accept-mode *vrid*

Parameters

vrid	Specifies the VRRP instance.

Defaults

None.

Mode

Interface configuration mode.

Usage

The master will accept IP packets for the configured associated list even if the device is not the owner.

Enabling accept mode on a VRID will allow the router to be managed by the addresses in the associate list when it is not the owner of those addresses. If accept mode is not enabled, then only ARP packets are replied back, all other packets are dropped that are destined for an IP address in the associate list when it is not the owner. If the router is the owner of the IP Addresses in the associate list then the command has no effect.

Example

This example enables the master of VRID 1 to accept IP packets for the its associated IP address list:

```
S Chassis(rw)->
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 20
S Chassis(rw-config-intf-vlan.0.20)->vrrp accept-mode 1
```

```
S Chassis(rw-config-intf-vlan.0.20)->
```

vrrp advertise-interval

Sets the advertise interval for a VRRP instance.

Syntax

vrrp advertise-interval *vrid* {**seconds** *interval* | **centiseconds** *interval*}

no vrrp advertise-interval *vrid interval*

Parameters

vrid	Specifies the virtual router ID used on this interface. Valid Values: 1-255. Default Value: None.
seconds *interval*	Specifies the advertise interval in seconds for VRRP version 2 or 3. Valid values are **1** - **255**.The default value is **1** second.
centiseconds *interval*	Specifies the advertise interval in centi-seconds for VRRP version 3. Valid values are **20** - **4095**.The default value is **1** second.

Defaults

None.

Mode

Interface configuration mode.

Usage

All routers with the same VRID must be configured with the same advertisement interval.

VRRP advertisements are sent by the master router to other routers participating in the VRRP master selection process, informing them of its configured values. Once the master is selected, then advertisements are sent every advertising interval to let other VRRP routers in this VLAN/VRID know the router is still acting as master of the VLAN/VRID.

The “no” form of this command resets the VRRP advertise interval value to the default of **1** second.

Example

This example sets the advertise interval for VRRP instance **1** to **2** seconds for VRRP protocol version 2:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 20
S Chassis(rw)-config-intf-vlan.0.20)->vrrp create 1 v2-ipv4
S Chassis(rw)-config-intf-vlan.0.20)->vrrp address 1 20.20.20.1
S Chassis(rw-config-intf-vlan.0.20)->vrrp advertise-interval 1 seconds 2
S Chassis(rw-config-intf-vlan.0.20)->
```

vrrp authentication

Sets the VRRP authentication values for the interface

Syntax

vrrp authentication {**simple** *password* | **md5** *password* [**hmac-96**]}

no vrrp authentication

Parameters

simple *password*	Specifies a simple plain text password. Valid Values: 1 - 8 characters in length.
md5 *password*	Specifies an 128-bit encrypted MD5 password.
hmac-96	(Optional) Specifies that the MD5 password should be 96-bit encrypted.

Defaults

If the hmac-96 option is not specified with the md5 option, 128-bit password encryption is used.

Mode

Interface configuration mode.

Usage

Only VRRP sessions running version 2 support authentication.

The “no” form of this command clears the MD5 authentication.

Example

This example sets VRRP authentication to a simple clear text password of **document**:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 20
S Chassis(rw)-config-intf-vlan.0.20)->vrrp create 1 v2-ipv4
S Chassis(rw)-config-intf-vlan.0.20)->vrrp address 1 20.20.20.1
S Chassis(rw-config-intf-vlan.0.20)->vrrp authentication simple document
S Chassis(rw-config-intf-vlan.0.20)->
```

vrrp critical-ip

Defines a local or remote interface IP address that will prevent the VRRP master router from functioning properly should its underlying interface fail.

Syntax

vrrp critical-ip *vrid ip-address* [*priority*] [**enable** | **disable**] [**remote** [**probe-name** *probe-name*]]

no vrrp critical-ip *vrid ip-address* [*priority*] [**enable** | **disable**] [**remote** [**probe-name** *probe-name*]]

Parameters

vrid	Specifies the virtual router ID to be used on this interface. Valid Values: **1** - **255**. Default Value: None.
ip-address	Specifies the critical-IP address for this interface.
priority	(Optional) Specifies the amount to decrement the VRID operational priority if the interface goes down. Default value: **10**.
enable | **disable**	(Optional) Specifies whether the specified critical-IP address is enabled or disabled in the critical-IP address list.
remote	(Optional) Specifies that the critical-IP address is a remote address. If **probe-name** *probe-name* is not specified, the default **$vrrp_default** ICMP probe is used by default.
remote probe-name *probe-name*	(Optional) Specifies an administratively configured ICMP probe that will monitor a remote critical-IP interface.

Defaults

- If the *priority* is not specified, then a default value of 10 will be used.
- If neither **enabled** or **disabled** is specified, the critical-IP address is enabled in the critical-IP address list by default.
- If **remote** is not specified, the critical-IP address is assumed to be a local IP address, and the default probe is not used.
- If a probe is not specified, and the critical-IP address is a remote address, the **$vrrp_default** default ICMP probe is used.

Mode

Interface configuration mode.

Usage

A critical-IP address defines an interface that will prevent the master router from functioning properly if the interface were to fail. A critical-IP interface is typically an internet facing interface and does not include the VRRP configured interface between hosts and a VRRP master or backup first-hop router. An IP address of an interface connecting a master router to a router configured for internet access would be considered a critical-IP address for VRRP routing.

The default priority setting is enabled. Setting the critical-IP address priority to enabled signals that the critical-IP will affect the operational priority for the VRID. Setting the priority to disabled signals the critical-IP interface state will have no effect on the operational priority for the VRID.

If the critical-IP interface goes down with priority configured and enabled, the operational priority for the VRID to which this critical-IP address is associated is decremented by the value of the priority specified in this command.

An ICMP probe can be assigned to monitor a remote critical IP interface. The remote keyword must be specified. An ICMP probe is not configurable for a local critical-IP address. If the **remote** keyword is specified, and a probe is not specified, the default **$vrrp_default** ICMP probe is used.

Up to 2048 critical-IP addresses can be configured on a device, and up to 10 critical-IP addresses can be configured per VRID.

If the critical-IP address is configured on a router where the VRID IP address is owned by that router, the critical-IP configuration is ignored.

The “no” form of this command clears the critical-IP address or the specified optional parameter.

Example

This example sets the remote IP address **20.20.20.2** on VLAN **20** as the critical-IP address for VRRP instance **1**, sets the decrement operational priority to **100** should the interface go down, and assigns ICMP probe **ICMP-VRRP** to monitor the interface:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 20
S Chassis(rw-config-intf-vlan.0.20)->vrrp critical-ip 1 20.20.20.2 100 remote
probe-name ICMP-VRRP enable
S Chassis(rw-config-intf-vlan.0.20)->no shutdown
S Chassis(rw-config-intf-vlan.0.20)->
```

vrrp enable

Enables the specified VRRP instance.

Syntax

vrrp enable *vrid*

no vrrp enable *vrid*

Parameters

vrid	Specifies the VRRP instance to enable.

Defaults

None.

Mode

Interface configuration mode.

Usage

Before enabling VRRP, you must set the other options described in this section. Once enabled, you cannot make any configuration changes to VRRP without first disabling the interface, using the **no vrrp enable** command.

The “no” form of this command disables VRRP on an interface.

Example

This example enables VRRP instance 1 on interface VLAN 20:

```
S Chassis(rw)->
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 20
S Chassis(rw)-config-intf-vlan.0.20)->vrrp create 1 v2-ipv4
S Chassis(rw)-config-intf-vlan.0.20)->vrrp address 1 20.20.20.1
S Chassis(rw-config-intf-vlan.0.20)->vrrp enable 1
S Chassis(rw-config-intf-vlan.0.20)->
```

vrrp interface-up-delay

Configures a VRID state interface down to interface up transition delay period.

Syntax

vrrp interface-up-delay *vrid seconds*

no vrrp interface-up-delay *vrid*

Parameters

vrid	Specifies the VRRP instance for this delay setting.
seconds	Specifies the number of seconds to set for the transition delay from VRID state interface down to interface up. Valid Values: **0** - **900**. Default Value: **0**.

Defaults

None.

Mode

Interface configuration mode.

Usage

The interface-up-delay is typically used to delay startup of the VRRP state machines while other protocols are transitioning. For example, you may want to prevent the VRRP state machines from processing a VRRP packet on the network while ports on that interface have not fully transitioned to forwarding from the STP protocol. By setting the interface-up-delay, the user can configure VRRP to start its protocol state machines after the STP protocol has had a chance to transition all forwarding packets.

The “no” form of this command sets the interface-up delay to the default value of **0** seconds.

Example

This example sets the interface-up-delay for VRID **1** on interface VLAN **20** to **10** seconds:

```
S Chassis(rw)->
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 20
S Chassis(rw)-config-intf-vlan.0.20)->vrrp interface-up-delay 1 10
S Chassis(rw)-config-intf-vlan.0.20)->
```

vrrp fabric-route-mode

Enables fabric route mode on a VRRP router.

Syntax

vrrp fabric-route-mode *vrid* [**helper-router**]

no vrrp fabric-route-mode *vrid* [**helper-router**]

Parameters

vrid	Specifies the VRRP instance for this fabric route mode configuration.
helper-router	(Optional) Enables the Routing as a Service (RaaS) Helper routing feature on an SPB node.

Defaults

Fabric route mode is disabled.

Mode

Interface configuration mode.

Usage

VRRP fabric route mode provides for sharing of traffic load for VRRP routers by allowing a VRRP instance in backup state to forward IPv4 and IPv6 traffic that is destined for the VRRP Gateway MAC address.

See the "Routing as a Service Configuration" chapter of the *Extreme Networks S-Series Configuration Guide* for Helper router details.

The "no" form of this command sets fabric route mode to the default state of disabled.

Example

This example enables fabric route mode on the VRRP backup router on VRID **1**:

```
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 20
S Chassis(rw)-config-intf-vlan.0.20)->vrrp fabric-route-mode 1
S Chassis(rw)-config-intf-vlan.0.20)->
```

vrrp host-mobility

Enables fabric route host mobility mode on a VRRP router.

Syntax

vrrp host-mobility *vrid*

no vrrp host-mobility *vrid*

Parameters

vrid	Specifies the VRRP instance for this fabric route host mobility mode configuration.

Defaults

Fabric route host mobility mode is disabled.

Mode

Interface configuration mode.

Usage

VRRP fabric route mode provides for sharing of traffic load for VRRP routers by allowing a VRRP instance in backup state to forward IPv4 and IPv6 traffic that is destined for the VRRP Gateway MAC address. Enabling host mobility allows the VRRP router to advertise 32 or 128-bit addresses for routes directly connected to the VRRP router.

Directly connected routes that should or should not take part in host mobility can be optionally restricted by assigning an ACL to the fabric route host mobility configuration using "vrrp host-mobility-acl" on page 76-12.

Should the directly attached device be moved to another VRRP router, upon timing out, the full address is advertised by the new VRRP router enabled for fabric route host mobility.

Directly connected routes are not advertised until redistributed by OSPF using "redistribute" on page 73-7 for IPv4 routes and "redistribute" on page 74-26 for IPv6 routes.

The "no" form of this command sets fabric route mode to the default state of disabled.

Example

This example enables fabric route host mobility mode on the VRRP backup router on VRID **1**:

```
S Chassis(rw)->
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 20
S Chassis(rw)-config-intf-vlan.0.20)->vrrp host-mobility 1
S Chassis(rw)-config-intf-vlan.0.20)->
```

vrrp host-mobility-acl

Assigns an ACL to the host-mobility configuration to define those routes that should or should not take part in host mobility.

Syntax

vrrp host-mobility-acl *vrid acl-name*

no vrrp host-mobility-acl *vrid* [*acl-name*]

Parameters

vrid	Specifies the VRRP instance for this fabric route host mobility mode configuration.

Defaults

If an ACL is not specified using the "no" option, all assigned ACLs are removed from the configuration.

Mode

Interface configuration mode.

Usage

The "no" form of this command removes the specified ACL from the host mobility configuration or all ACLs if no ACL is specified.

Example

This example assigns the **hostMobil1** ACL to the VRID **1** host mobility configuration:

```
S Chassis(rw)->
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 20
S Chassis(rw)-config-intf-vlan.0.20)->vrrp fabric-route-mode 1 host-mobility acl
hostMobil1
S Chassis(rw)-config-intf-vlan.0.20)->
```

host-mobility timeout

Set the age out timer for a fabric route host mobility route that is no longer available.

Syntax

host-mobility timeout *timeout*

Parameters

timeout	Specifies the age out timer in seconds for a fabric route host mobility route that is no longer available. Valid values are **20** - **2147483647** seconds. Default value is **150** seconds.

Defaults

The fabric route host mobility route age out timer defaults to **150** seconds.

Mode

Global configuration mode.

Usage

VRRP fabric route host mobility supports the alternate host route age out mechanism. By default, when a connected device is moved from one VRRP router to another, the original route continues to advertise until the age out timer expires. When a host mobility enabled device is moved to another router, initially both the old and new router continue to advertise their route for the device. When the original VRRP router receives an advertisement of the moved route, it will ignore the remaining age out time and no longer advertise the associated route.

The actual age out time can be up to twice the time specified by this command.

Example

This example sets the fabric route host mobility age out time to 200 seconds:

```
S Chassis(rw)->
S Chassis(rw)->configure
S Chassis(rw-config)->host-mobility timeout 200
S Chassis(rw-config)->
```

vrrp preempt

Enables the VRRP instance to preempt a current master.

Syntax

vrrp preempt *vrid*

no vrrp preempt *vrid*

Parameters

vrid	Specifies the VRRP instance that will be allowed to preempt the current master.

Defaults

None.

Mode

Interface configuration mode.

Usage

The router that owns the virtual router IP address always preempts other routers, regardless of this setting.

Preempt is enabled on VRRP routers by default, which allows a higher priority backup router to preempt a lower priority master.

The “no” form of this command disables preempt mode.

Example

This example enables VRRP instance **1** to preempt the current master:

```
S Chassis(rw)->
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 20
S Chassis(rw-config-intf-vlan.0.20)->vrrp preempt 1
S Chassis(rw-config-intf-vlan.0.20)->
```

vrrp preempt-delay

Sets the amount of time that will expire before this VRRP instance takes control from the current master when preemption is enable.

Syntax

vrrp preempt-delay *vrid delay*

no vrrp preempt-delay *vrid delay*

Parameters

vrid	Specifies the VRRP instance to which the delay will be applied.
delay	Specifies the delay in seconds before this VRID takes control from the current master. Valid Values: **1** - **900** seconds.

Defaults

None.

Mode

Interface configuration mode.

Usage

The router that owns the virtual router IP address always preempts other routers, regardless of this setting.

When preempt mode is enabled this specifies a delay (in seconds) that a higher priority backup router must wait to preempt a lower priority master. For more information on setting preempt status, refer back to "vrrp preempt" on page 76-14. For more information on setting VRRP priority, refer back to "vrrp priority" on page 76-4.

The "no" form of this command clears the preempt delay timer.

Example

This example sets the preempt-delay timer to 60 seconds for VRRP instance 1:

```
S Chassis(rw)->
S Chassis(rw)->configure
S Chassis(rw-config)->interface vlan 20
S Chassis(rw-config-intf-vlan.0.20)->vrrp preempt-delay 1 60
S Chassis(rw-config-intf-vlan.0.20)->
```

show ip vrrp

Displays the VRRP configuration and statistics for this system.

Syntax

show ip vrrp [*interface* [*vrid*]] [**statistics**] [**verbose**]

Parameters

interface	(Optional) Specifies the interface name for VRRP configuration or statistics display.
vrid	(Optional) Specifies a virtual router ID to display that is associated with the specified interface.
statistics	(Optional) Specifies that VRRP statistics should be displayed.
verbose	(Optional) Specifies that full VRRP configuration information should be displayed. Verbose does not affect statistics.

Defaults

- If *interface* is not specified, all configured interfaces are displayed.
- If *vrid* is not specified, all VRIDs associated with this interface will display.
- If **statistics** is not specified, VRRP configuration is displayed.
- If **verbose** is not specified, VRRP configuration summary information is displayed.

Mode

All command modes**.**

Examples

This example displays VRRP information for this system:

```
S Chassis(rw)->show ip vrrp

 Codes: Pri = Operational Priority
        V   = Version of the protocol
        T   = Type (M-Master IP Address, A-Associate IP Address)
        A   = Admin status of Associate address (E-enabled, D-disabled)
        O   = Owner status of Associate address (Y-yes, N-no)

Interface   Vrid State      Pri V T A O IP Address
----------- ---- ---------- --- - - - - ---------------------------------------
vlan.0.2010 1    intfDown   100 2 M - -
                                 A E N 192.168.201.1
vlan.0.2020 1    stopped    0   2 M - - 0.0.0.0
                                 A E N 192.168.202.1


S Chassis(rw)->
```

This example displays VRRP verbose information for this system:

```
S Chassis(rw)->sho ip vrrp verb

Interface: vlan.0.30
VRID: 1
  Version: 2, State: master
  Time of last state transition: MON JUN 03 11:19:53 2013
  Master IP Address : 30.1.1.2
  Primary IP Address: 30.1.1.2
  Virtual MAC Address: 00:00:5E:00:01:01
  Advertisement Interval:   1.00 seconds
  Master Priority: 100, Operational Priority: 100,  Configured Priority: 100
  Accept: no ,  Preempt: yes,  Preempt time:   0 seconds
  Fabric-Route-Mode: yes
  Host-Mobility: yes, State: up, ACL: hosts
  Interface Up Delay:   0 seconds
  Virtual IP Count:   1,  Enabled Virtual IP's:   1,  Critical IP Count:    0
  Virtual IP Addresses                          Admin    State  Owner
   30.1.1.1                                    enabled    up     no
```

```
  Critical IP Addresses:
   Interface                                Critical Priority   Probe        Admin    State
```

This example displays VRRP global and virtual router ID statistics information for this system:

```
S Chassis(rw)->show ip vrrp vlan.0.2010 statistics

Global Statistics
-----------------
Received valid VRRP packets                                  0
Received invalid VRRP version                                0
Received packet with invalid VRID                            0
Received packet with invalid source mac address              0
Received IP checksum errors                                  0
Received VRRP Checksum errors                                0
Received no VRRP interface                                   0
Received no VRID                                             0
Interface up events                                          9
Interface down events                                       11
Interface errors                                             0

VRID Statistics
-----------------

Interface: vlan.0.2010
 VRID:   1
  Received advertisements                0
  Received priority-0                    0
  Transmitted advertisements             0
  Transmitted priority-0                 0
  VRID not enabled                       0
  Transitions to master                  0
  Transitions to backup                  0
  Transitions to init                    1
  Transitions to interface down          1
  Transitions to preempt delay           0
  Transitions to ifUp delay              0
  Transitions to owner mismatch          0
  Virtual IP list errors                 0
  Invalid type                           0
  Invalid packet length                  0
  Invalid destination IP                 0
  Invalid TTL                            0
  Invalid advertisement interval         0
  Invalid authentication type            0
  Authentication errors                  0
```

```
  Authentication mismatches               0

S Chassis(rw)->
```

77

MAC Locking Commands

This chapter describes the MAC locking set of commands and how to use them. For information about configuring MAC locking, refer to the "Security Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show maclock	77-2
set maclock enable	77-4
set maclock disable	77-4
set maclock disable-port	77-5
clear maclock disable-port	77-5
set maclock	77-6
set maclock firstarrival	77-7
clear maclock firstarrival	77-7
set maclock agefirstarrival	77-8
clear maclock agefirstarrival	77-9
set maclock clearonlinkchange	77-9
clear maclock clearonlinkchange	77-10
set maclock move	77-10
set maclock static	77-11
clear maclock static	77-11
set maclock trap	77-12
clear maclock trap	77-12
set maclock syslog	77-13
clear maclock syslog	77-13
clear maclock	77-14

show maclock

Use this command to display the status of MAC locking on one or more ports.

Syntax

show maclock [**stations** [**firstarrival** | **static**]] [*port-string*]

Parameters

stations firstarrival | **static**	(Optional) Display the stations for this device, optionally specifying the first arrival method or statically provisioned.
port-string	(Optional) Displays MAC locking status for specified port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *no option is* specified, MAC locking status will be displayed for all ports.

Mode

All command modes.

Examples

This example shows how to display MAC locking information for ge.2.1 through 5:

```
S Chassis(rw)->show maclock ge.1.1-4

MAC locking is globally disabled.

Port     Port Trap     Syslog   Aging Port     Clr Max Max  Last Violating
Number   Stat Thr|Viol Thr|Viol Stat  Dis|Viol OLC Stc FA   MAC Address
-------- ---- -------- -------- ----  -------- --- --- ---- -----------------
ge.1.1   dis  dis|dis  dis|dis  dis   dis|dis  ena  64  600  00-00-00-00-00-00
ge.1.2   dis  dis|dis  dis|dis  dis   dis|dis  ena  64  600  00-00-00-00-00-00
ge.1.3   dis  dis|dis  dis|dis  dis   dis|dis  ena  64  600  00-00-00-00-00-00
ge.1.4   dis  dis|dis  dis|dis  dis   dis|dis  ena  64  600  00-00-00-00-00-00
```

Table 77-1 provides an explanation of the command output.

Table 77-1 show maclock Output Details

Output Field	What It Displays...
Port Number	Port designation.
Port Stat(us)	Whether MAC locking is enabled (ena) or disabled (dis) on the port. MAC locking is globally disabled by default. For details on enabling MAC locking on the switch and on one or more ports, refer to “set maclock enable” on page 77-4 and “set maclock” on page 77-6.
Trap Thr | Vio	Whether MAC lock threshold (Thr) and violation (Vio) trap messaging is enabled (ena) or disabled (dis) on the port. For details on setting this status, refer to “set maclock trap” on page 77-12.

Table 77-1 show maclock Output Details (continued)

Output Field	What It Displays...
Syslog Thr | Vio	Whether MAC lock threshold (Thr) and violation (Vio) syslog messaging is enabled (ena) or disabled (dis) on the port. For details on setting this status, refer to "set maclock syslog" on page 77-13.
Aging Stat(us)	Whether aging of FirstArrival MAC addresses is enabled (ena) or disabled (dis) on the port. Refer to "set maclock agefirstarrival" on page 77-8.
Port Dis | Viol	Port Dis shows the port's threshold shutdown state, enabled (ena) or disabled (dis). (etsMACLockingThresholdShutdown) Refer to "set maclock disable-port" on page 77-5. Port Viol shows the MAC locking shutown state, enabled (ena) or disabled (dis). (etsMACLockingShutdownState).
Clr OLC	Shows the state of First Arrival MAC address locking clear on link change, enabled (ena) or disabled (dis). Refer to "set maclock clearonlinkchange" on page 77-9.
Max Stc	The maximum static MAC addresses allowed locked to the port. For details on setting this value, refer to "set maclock static" on page 77-11.
Max FA	The maximum end station MAC addresses allowed locked to the port. For details on setting this value, refer to "set maclock firstarrival" on page 77-7.
Last Violating MAC Address	Most recent MAC address(es) violating the maximum static and first arrival value(s) set for the port.

This example shows how to display MAC locking information for the end stations connected to all ports in module 2:

```
S Chassis(rw)->show maclock stations ge.2.*
Port Number   MAC Address         Status          State
-----------  -----------------   --------------  --------------
ge.2.3        00-10-a4-e5-08-4e   active          first learned
ge.2.3        08-00-20-7c-e0-db   active          first learned
ge.2.6        00-60-08-14-4b-15   active          first learned
ge.2.6        08-00-20-20-32-4b   active          first learned
ge.2.9        08-00-20-77-aa-80   active          first learned
ge.2.12       00-03-ba-08-4c-f0   active          first learned
ge.2.14       00-01-f4-2c-ad-b4   active          first learned
```

Table 77-2 provides an explanation of the command output.

Table 77-2 show maclock stations Output Details

Output...	What it displays...
Port Number	Port designation. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
MAC address	MAC address of the end station(s) locked to the port.
Status	Whether the end stations are **active** or **inactive**.
State	Whether the end station locked to the port is a **first learned, first arrival** or **static** connection.

set maclock enable

Use this command to enable MAC locking on one or more ports.

Syntax

set maclock enable [*port-string*]

Parameters

port-string	(Optional) Enables MAC locking on specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, MAC locking will be enabled on all ports.

Mode

All command modes.

Usage

MAC locking is disabled by default at device startup. Configuring one or more ports for MAC locking requires globally enabling it on the device and then enabling it on the desired ports as described in "set maclock" on page 77-6.

When enabled and configured for a specific MAC address and port string, this locks a port so that only designated end station addresses are allowed to participate in frame relay.

Example

This example shows how to enable MAC locking on ge.2.3:

```
S Chassis(rw)->set maclock enable ge.2.3
```

set maclock disable

Use this command to disable MAC locking on one or more ports.

Syntax

set maclock disable [*port-string*]

Parameters

port-string	(Optional) Disables MAC locking on specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, MAC locking will be disabled on all ports.

Mode

All command modes.

Example

This example shows how to disable MAC locking on ge.2.3:

```
S Chassis(rw)->set maclock disable ge.2.3
```

set maclock disable-port

Use this command to configure the disabling of ports when the first arrival threshold is met.

Syntax

set maclock disable-port [*port-string*]

Parameters

port-string	(Optional) Disables the specified port(s) when the first arrival threshold is met. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, all ports are disabled when the first arrival threshold is met.

Mode

All command modes.

Example

This example shows how to disable port ge.2.3 through ge.2.7 when the first arrival threhold is met:

```
S Chassis(rw)->set maclock disable-port ge.2.3-7
```

clear maclock disable-port

Use this command to clear the port disabling configuration of ports when the first arrival threshold is met.

Syntax

clear maclock disable-port [*port-string*]

Parameters

port-string	(Optional) Clears the disable port configuration for specified port(s) when the first arrival threshold is met. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, all disable ports configuraiton for when the first arrival threshold is met is cleared.

Mode

All command modes.

Example

This example shows how to clear the disable port configuration when the first arrival threhold is met for ports ge.2.3 through ge.2.7:

```
S Chassis(rw)->clear maclock disable-port ge.2.3-7
```

set maclock

Use this command to create a static MAC address and enable or disable MAC locking for the specific MAC address and port.

Syntax

set maclock *mac-address port-string* {**create** | **enable** | **disable**}

Parameters

mac-address	Specifies the MAC address for which MAC locking will be created, enabled or disabled.
port-string	Specifies the port on which to create, enable or disable MAC locking. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
create | **enable** | **disable**	Creates, enables or disables MAC locking between the specified MAC address and port. **create** both creates and enables the specified entry.

Defaults

None.

Mode

All command modes.

Usage

Configuring one or more ports for MAC locking requires globally enabling it on the device first using the **set maclock enable** command as described in "set maclock enable" on page 77-4. When globally enabling MAC locking, specifying the port is optional.

In order to statically associate a port to a specific hardware device, create the static configuration using the **set maclock** *mac-address port-string* **create** command. A static MAC lock configuration is active by default.

To set the static MAC lock configuration to inactive, use the **set maclock** *mac-address port-string* **disable** command.

To delete the static configuration, use "clear maclock" on page 77-14, specifying the MAC-address and port-string of the static configuration to delete.

Up to 64 MAC addresses can be locked per port.

When created and enabled, a static MAC lock configuration allows only the end station designated by the MAC address to participate in frame relay.

Examples

This example shows how to enable MAC locking on port ge.2.3 and create a static MAC locking association between MAC address 00-a0-c9-0d-32-11 and port ge.2.3:

```
S Chassis(rw)->set macklock enable ge.2.3
S Chassis(rw)->set maclock 00-a0-c9-0d-32-11 ge.2.3 create
```

This example shows how to set the static MAC locking association between MAC address 00-a0-c9-0d-32-11 and port ge.2.3 to inactive:

```
S Chassis(rw)->set maclock 00-a0-c9-0d-32-11 ge.2.3 disable
```

This example shows how to reset the static MAC locking association between MAC address 00-a0-c9-0d-32-11 and port ge.2.3 to active:

```
S Chassis(rw)->set maclock 00-a0-c9-0d-32-11 ge.2.3 enable
```

set maclock firstarrival

Use this command to configure dynamic MAC locking on a port by restricting MAC locking to a maximum number of end station addresses first connected to that port.

Syntax

set maclock firstarrival *port-string value*

Parameters

port-string	Specifies the port on which to limit MAC locking. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
value	Specifies the number of first arrival end station MAC addresses to be allowed connections to the port. Valid values are **0** to **600**. Default: **600**.

Defaults

None.

Mode

All command modes.

Example

This example shows how to restrict MAC locking to 6 MAC addresses on ge.2.3:

```
S Chassis(rw)->set maclock firstarrival ge.2.3 6
```

clear maclock firstarrival

Use this command to reset the number of first arrival MAC addresses allowed per port to the default value.

Syntax

clear maclock firstarrival *port-string*

Parameters

port-string	Specifies the port on which to reset the first arrival value.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset MAC first arrivals on ge.2.3:

```
S Chassis(rw)->clear maclock firstarrival ge.2.3
```

set maclock agefirstarrival

Use this command to enable or disable first arrival MAC address aging.

Syntax

set maclock agefirstarrival *port-string* {**enable** | **disable**}

Parameters

port-string	Specifies the port on which to enable MAC address aging. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
enable | **disable**	Enables or disables first arrival MAC address aging for the specified port(s).

Defaults

None.

Mode

All command modes.

Usage

If the Filter Database (FDB) entry ages out for this station, the corresponding dynamic MAC locked stations will no longer be MAC locked.

Dynamic MAC locking mode MAC address aging is disabled by default.

Example

This example shows how to enable MAC address aging on port ge.1.1:

```
S Chassis(rw)->set maclock agefirstarrival ge.1.1
```

clear maclock agefirstarrival

Use this command to clear the first arrival MAC address aging configuration for the specified ports.

Syntax

clear maclock agefirstarrival *port-string*

Parameters

port-string	Specifies the port(s) on which to clear MAC address aging configuration. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear MAC address aging configuration on port ge.1.1:

```
S Chassis(rw)->clear maclock agefirstarrival ge.1.1
```

set maclock clearonlinkchange

Use this command to manage the behavior of first arrival MAC locking with link state change.

Syntax

set maclock clearonlinkchange *port-string* {**enable** | **disable**}

Parameters

port-string	Specifies the port or ports on which to apply the command.
enable | **disable**	Enable or disable clearing of first arrival MAC locks with a change in link state.

Defaults

Clear on link change is enabled by default.

Mode

All command modes.

Usage

If you disable clearing of first arrival MAC locking, first arrival MAC addresses will be maintained on a loss of link.

Example

This example shows how to configure a port to maintain first arrival MAC address locks on a port through a link state change.

```
S Chassis(su)->set maclock clearonlinkchange ge.1.1 disable
```

clear maclock clearonlinkchange

Use this command to return the behavior of first arrival MAC locking with link state change to its default value of enabled.

Syntax

clear maclock clearonlinkchange *port-string*

Parameters

port-string	Specifies the port or ports on which to apply the command.

Defaults

Clear on link change is enabled by default.

Mode

All command modes.

Example

This example returns clear on link change to its default value on ge.1.1.

```
S Chassis(su)->clear maclock clearonlinkchange ge.1.1
```

set maclock move

Use this command to move all current first arrival MACs to static entries.

Syntax

set maclock move *port-string*

Parameters

port-string	Specifies the port where all current first arrival MACs will be moved to static entries.

Defaults

None.

Mode

All command modes.

Example

This example shows how to move all current first arrival MACs to static entries on ge.1.3:

```
S Chassis(rw)->set maclock move ge.1.3
```

set maclock static

Use this command to restrict MAC locking on a port to a maximum number of static (management defined) MAC addresses for end stations connected to that port.

Syntax

set maclock static *port-string value*

Parameters

port-string	Specifies the port on which to limit MAC locking.
value	Specifies the number of static MAC addresses to be allowed connections to the port. Valid values are **0** to **64.**

Defaults

None.

Mode

All command modes.

Example

This example shows how to restrict MAC locking to 4 static addresses on ge.2.3:

```
S Chassis(rw)->set maclock static ge.2.3 4
```

clear maclock static

Use this command to reset the number of static MAC addresses allowed per port to the default value.

Syntax

clear maclock static *port-string*

Parameters

port-string	Specifies the port on which to reset the static MAC locking limit.

Defaults

None.

Mode

All command modes.

Usage

Default value for static MAC addresses allowed per port is 64.

Example

This example shows how to reset static MAC locking on ge.2.3:

```
S Chassis(rw)->clear maclock static ge.2.3
```

set maclock trap

Use this command to enable or disable MAC lock trap messaging.

Syntax

set maclock trap *port-string* {**enable** | **disable**}

Parameters

port-string	Specifies the port on which MAC lock trap messaging will be enabled or disabled.
enable | **disable**	Enables or disables MAC lock trap messaging.

Defaults

None.

Mode

All command modes.

Usage

When enabled, this authorizes the device to send an SNMP trap message if an end station is connected that exceeds the maximum values configured using the **set maclock firstarrival** and **set maclock static** commands. Violating MAC addresses are dropped from the device's routing table.

Example

This example shows how to enable MAC lock trap messaging on ge.2.3:

```
S Chassis(rw)->set maclock trap ge.2.3 enable
```

clear maclock trap

Use this command to clear MAC lock trap messaging configuration.

Syntax

clear maclock trap *port-string*

Parameters

port-string	Specifies the port MAC lock trap messaging will be cleared on.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear MAC lock trap messaging on port ge.2.3:

```
S Chassis(rw)->clear maclock trap ge.2.3
```

set maclock syslog

Use this command to enable or disable MAC lock Syslog messaging.

Syntax

set maclock syslog *port-string* {**enable** | **disable**}

Parameters

port-string	Specifies the port on which MAC lock Syslog messaging will be enabled or disabled.
enable | **disable**	Enables or disables MAC lock Syslog messaging.

Defaults

None.

Mode

All command modes.

Usage

When enabled, this authorizes the device to send an SNMP Syslog message if an end station is connected that exceeds the maximum values configured using the **set maclock firstarrival** and **set maclock static** commands. Violating MAC addresses are dropped from the device's routing table.

Example

This example shows how to enable MAC lock Syslog messaging on ge.2.3:

```
S Chassis(rw)->set maclock syslog ge.2.3 enable
```

clear maclock syslog

Use this command to clear MAC lock Syslogmessaging configuration.

Syntax

clear maclock syslog *port-string*

Parameters

port-string	Specifies the port MAC lock Syslog messaging will be cleared on.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear MAC lock Syslog messaging on port ge.2.3:

```
S Chassis(rw)->clear maclock syslog ge.2.3
```

clear maclock

Use this command to clear MAC locking from one or more static MAC addresses.

Syntax

clear maclock {**all** | *mac-address*} *port-string*

Parameters

all	Clears all static MAC locking for one or more ports.
mac-address	Specifies the MAC address for which the MAC locking will be cleared.
port-string	Specifies the port on which to clear MAC locking.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear MAC locking between MAC address 00-a0-c9-0d-32-11 and port ge.2.3:

```
S Chassis(rw)->clear maclock 00-a0-c9-0d-32-11 ge.2.3
```

78

TACACS+ Commands

This chapter describes the TACACS+ set of commands and how to use them. For information about configuring TACACS+, refer to the "Security Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show tacacs	78-1
set tacacs	78-3
show tacacs server	78-3
set tacacs server	78-4
clear tacacs server	78-5
show tacacs session	78-5
set tacacs session	78-6
clear tacacs session authorization	78-8
show tacacs command	78-8
set tacacs command	78-9
show tacacs singleconnect	78-10
set tacacs singleconnect	78-10

show tacacs

Use this command to display the current TACACS+ configuration information and status.

Syntax

```
show tacacs [state]
```

Parameters

state	(Optional) Displays only the TACACS+ client status.

Defaults

If **state** is not specified, all TACACS+ configuration information will be displayed.

Mode

All command modes.

Example

This example shows how to display all TACACS configuration information:

```
S Chassis(ro)->show tacacs
 TACACS+ state:                        enabled
 TACACS+ session accounting state:     disabled
 TACACS+ command authorization state:  disabled
 TACACS+ command accounting state:     disabled
 TACACS+ single-connect state:         disabled
 TACACS+ service:                      exec
 TACACS+ session authorization A-V pairs:
         access level attribute                          value
         read-only   'priv-lvl'                          '0'
         read-write  'priv-lvl'                          '1'
         super-user  'priv-lvl'                          '15'
 TACACS+ Server  IP Address       Port   Timeout  Status
 --------------  ---------------  -----  -------  -------
   1               10.1.26.245     49       10     Active
```

Table 78-1 provides an explanation of the command output.

Table 78-1 show tacacs Output Details

Output...	What it displays...
TACACS+ state	Whether the TACACS+ client is **enabled** or **disabled**.
TACACS+ session accounting state	Whether TACACS+ session accounting is **enabled** or **disabled**.
TACACS+ command authorization state	Whether TACACS+ command authorization is **enabled** or **disabled**.
TACACS+ command accounting state	Whether TACACS+ command accounting is **enabled** or **disabled**.
TACACS+ singleconnect state	Whether TACACS+ singleconnect is **enabled** or **disabled**. When enabled, the TACACS+ client sends multiple requests over a single TCP connection.
TACACS+ service	The name of the service that is requested by the TACACS+ client for session authorization. “exec” is the default service name.
TACACS+ session authorization A-V pairs	Displays the attribute – value pairs that are mapped to the Extreme Networks **read-only**, **read-write**, and **super-user** access privilege levels for the service requested for session authorization. The attribute names and values shown in the example above are the default values.
TACACS+ Server	Displays the TACACS+ server information used by the TACACS+ client.

set tacacs

Use this command to enable or disable the TACACS+ client.

Syntax

```
set tacacs {enable | disable}
```

Parameters

enable | **disable**	Enables or disables the TACACS+ client.

Defaults

None.

Mode

All command modes.

Usage

The TACACS+ client can be enabled on the switch anytime, with or without a TACACS+ server online. If the TACACS+ server is offline and TACACS+ is enabled, the login authentication is switched to RADIUS or local, if enabled.

Examples

This example shows how to enable the TACACS+ client.

```
S Chassis(rw)->set tacacs enable
```

show tacacs server

Use this command to display the current TACACS+ server configuration.

Syntax

```
show tacacs server {index | all}
```

Parameters

index	Display the configuration of the TACACS+ server identified by *index*. The value of *index* can range from 1 to 2,147,483,647.
all	Display the configuration for all configured TACACS+ servers.

Defaults

None.

Mode

All command modes.

Example

This example displays configuration information for all configured TACACS+ servers.

```
S Chassis(ro)->show tacacs server all
 TACACS+ Server  IP Address       Port   Timeout  Status
 --------------  ---------------  -----  -------  -------
 1               192.168.10.10    49     10       Active
 2               192.168.1.116    49     10       Active
```

set tacacs server

Use this command to configure the TACACS+ server(s) to be used by the TACACS+ client.

Syntax

set tacacs server {*index* [*ipaddress port* [*secret*]] | **all timeout** *timeout*}

Parameters

all	Specify the timeout value for all configured TACACS+ servers.
index	Configure the TACACS+ server identified by *index*. The value of *index* can range from **1** to **2147483647**.
timeout *seconds*	Set the timeout value for the specified server(s) in seconds. The value of *seconds* can range from **1** to **180** seconds. The default timeout value is **10** seconds.
ipaddress	Specify the IP address of the TACACS+ server.
port	Specify the TCP port for the TACACS+ server. The value of *port* can range from **0** to **65535**, but typically, port **49** is specified.
secret	Specify the secret for the TACACS+ server.

Defaults

None.

Mode

All command modes.

Usage

You can configure the timeout value for all configured servers or a single server, or you can configure the IP address, TCP port, and secret for a single server.

Example

This example configures TACACS+ server 1. The default timeout value of **10** seconds will be applied.

```
S Chassis(rw)->set tacacs server 1 192.168.10.10 49 mysecret
```

clear tacacs server

Use this command to remove one or all configured TACACS+ servers, or to return the timeout value to its default value for one or all configured TACACS+ servers.

Syntax

clear tacacs server {**all** | *index*} [**timeout**]

Parameters

all	Specifies that all configured TACACS+ servers should be affected.
index	Specifies one TACACS+ server to be affected.
timeout	(Optional) Specifies that the timeout value for the specified server(s) is reset to the default value of **10** seconds.

Defaults

If **timeout** is not specified, the affected TACACS+ servers will be removed.

Mode

All command modes.

Usage

If the optional **timeout** parameter is not specified, this command removes the specified or all TACACS+ servers. If the **timeout** parameter is specified, this command resets the timeout value of the TACACS+ server(s) specified to the default value of **10** seconds.

Example

This example removes TACACS+ server **1**.

```
S Chassis(rw)->clear tacacs server 1
```

show tacacs session

Use this command to display the current TACACS+ client session settings.

Syntax

show tacacs session {**authorization** | **accounting**} [**state**]

Parameters

authorization	Display client session authorization settings.
accounting	Display client session accounting settings.
state	(Optional) Display the client session accounting state.

Defaults

If **state** is not specified, all session accounting configuration parameters are displayed (which at this time includes only the enabled/disabled status).

Mode

All command modes.

Examples

This example shows how to display client session authorization information:

```
S Chassis(ro)->show tacacs session authorization
 TACACS+ service:                      exec
 TACACS+ session authorization A-V pairs:
         access level attribute                          value
         read-only   'priv-lvl'                          '0'
         read-write  'priv-lvl'                          '1'
         super-user  'priv-lvl'                          '15'
```

This example shows how to display client session accounting state.

```
S Chassis(ro)->show tacacs session accounting state
 TACACS+ session accounting state:     enabled
```

set tacacs session

Use this command to enable or disable TACACS+ session accounting, or to configure TACACS+ session authorization parameters.

Syntax

set tacacs session accounting {**enable** | **disable**}

set tacacs session {**authorization service** *name* | **read-only** *attribute value* | **read-write** *attribute value* | **super-user** *attribute value*}

Parameters

authorization	Specifies that TACACS+ session authorization service or privilege level is being configured.
service *name*	Specifies the name of the service that the TACACS+ client will request from the TACACS+ server. The *name* specified here must match the name of a service configured on the server.
accounting	Specifies that TACACS+ session accounting service is being enabled or disabled.
read-only *attribute value*	Specifies that the Extreme Networks **read-only** access privilege level should be matched to a privilege level configured on the TACACS+ server by means of an attribute-value pair specified by *attribute* and *value*. By default, *attribute* is “priv-lvl” and *value* is 0.

read-write *attribute value*	Specifies that the Extreme Networks **read-write** access privilege level should be matched to a privilege level configured on the TACACS+ server by means of an attribute-value pair specified by *attribute* and *value*. By default, *attribute* is "priv-lvl" and *value* is 1.
super-user *attribute value*	Specifies that the Extreme Networks **super-user** access privilege level should be matched to a privilege level configured on the TACACS+ server by means of an attribute-value pair specified by *attribute* and *value*. By default, *attribute* is "priv-lvl" and *value* is 15.
enable | **disable**	Enables or disables TACACS+ session accounting.

Defaults

None.

Mode

All command modes.

Usage

When session accounting is enabled, the TACACS+ server will log accounting information, such as start and stop times, IP address of the client, and so forth, for each authorized client session.

When the TACACS+ client is enabled on the Extreme Networks switch (with the **set tacacs enable** command), the session authorization parameters configured with this command are sent by the client to the TACACS+ server when a session is initiated on the Extreme Networks switch. The parameter values must match a service and access level attribute-value pairs configured on the server for the session to be authorized. If the parameter values do not match, the session will not be allowed.

The service name and attribute-value pairs can be any character string, and are determined by your TACACS+ server configuration.

Examples

This example configures the service requested by the TACACS+ client as the service name "basic."

```
S Chassis(rw)->set tacacs session authorization service basic
```

This example maps the Extreme Networks **read-write** access privilege level to an attribute named "priv-lvl" with the value of 5 configured on the TACACS+ server.

```
S Chassis(rw)->set tacacs session authorization read-write priv-lvl 5
```

This example enables TACACS+ session accounting.

```
S Chassis(rw)->set tacacs session accounting enable
```

clear tacacs session authorization

Use this command to return the TACACS+ session authorization settings to their default values.

Syntax

```
clear tacacs session authorization {[service] [read-only] [read-write]
[super-user]}
```

Parameters

authorization	Clears the TACACS+ session authorization parameters.
service	Clears the TACACS+ session authorization service name to the default value of “exec.”
read-only	Clears the TACACS+ session authorization read-only attribute-value pair to their default values of “priv-lvl” and 0.
read-write	Clears the TACACS+ session authorization read-write attribute-value pair to their default values of “priv-lvl” and 1.
super-user	Clears the TACACS+ session authorization super-user attribute-value pair to their default values of “priv-lvl” and 15.

Defaults

At least one of the session authorization parameters must be specified.

Mode

All command modes.

Examples

This example shows how to return only the service name to the default of “exec.”

```
S Chassis(rw)->clear tacacs session authorization service
```

This example shows how to return all the session authorization parameters to their default values.

```
S Chassis(rw)->clear tacacs session authorization service read-only read-write
super-user
```

show tacacs command

Use this command to display the status (enabled or disabled) of TACACS+ accounting or authorization on a per-command basis.

Syntax

```
show tacacs command {accounting | authorization} [state]
```

Parameters

accounting	Display the status of TACACS+ accounting on a per-command basis.
authorization	Display the status of TACACS+ authorization on a per-command basis.
state	(Optional) Specifies that only the status should be displayed.

Defaults

If **state** is not specified, all accounting or authorization configuration parameters are displayed (which at this time includes only the enabled/disabled status).

Mode

All command modes.

Example

This example shows how to display the state of the TACACS+ client's command authorization.

```
S Chassis(rw)->show tacacs command authorization
TACACS+ command authorization state:  enabled
```

set tacacs command

Use this command to enable or disable TACACS+ accounting or authorization on a per-command basis.

Syntax

set tacacs command {**accounting** | **authorization**} {**enable** | **disable**}

Parameters

accounting | **authorization**	Specifies either TACACS+ accounting or authorization to be enabled or disabled.
enable | **disable**	Enable or disable accounting or authorization on a per-command basis.

Defaults

None.

Mode

All command modes.

Usage

In order for per-command accounting or authorization by a TACACS+ server to take place, the command must be executed within an authorized session.

When per-command accounting is enabled, the TACACS+ server will log accounting information, such as start and stop times, IP address of the client, and so forth, for each command executed during the session.

When per-command authorization is enabled, the TACACS+ server will check whether each command is permitted for that authorized session and return a success or fail. If the authorization fails, the command is not executed.

Example

This example shows how to enable TACACS+ authorization on a command basis.

```
S Chassis(rw)->set tacacs command authorization enable
```

show tacacs singleconnect

Use this command to display the current status of the TACACS+ client's ability to send multiple requests over a single TCP connection.

Syntax

```
show tacacs singleconnect [state]
```

Parameters

state	(Optional) Specifies that only the single connection state should be displayed.

Defaults

If **state** is not specified, all single connection configuration parameters are displayed (which at this time includes only the enabled/disabled state).

Mode

All command modes.

Example

This example shows how to display the state of the TACACS+ client's ability to send multiple requests over a single connection.

```
S Chassis(rw)->show tacacs singleconnect
  TACACS+ single-connect state:         enabled
```

set tacacs singleconnect

Use this command to enable or disable the ability of the TACACS+ client to send multiple requests over a single TCP connection.

Syntax

```
set tacacs singleconnect {enable | disable}
```

Parameters

enable | **disable**	Enable or disable the ability to send multiple requests over a single TCP connection.

Defaults

None.

Mode

All command modes.

Usage

When enabled, the TACACS+ client will use a single TCP connection for all requests to a given TACACS+ server.

Examples

This example shows how to disable sending multiple requests over a single connection.

```
S Chassis(rw)->set tacacs singleconnect disable
```

79

Host DoS Commands

This chapter describes the Host Denial of Service (Host DoS) set of commands and how to use them. For information about configuring Host DoS, refer to the "Security Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show hostdos	79-1
hostdos	79-3

show hostdos

Use this command to display Host DoS configuration status or statistics.

Syntax

show hostdos [*mitigation-type*] [**stats**]

Parameters

mitigation-type	(Optional) Specifies a DoS attack mitigation type display. Valid values are: • **spoof** - source-if is not this router interface • **xmasTree** - Inappropriate TCP flags • **icmpFrag** - ICMP with fragments specified • **icmpFlood** - ICMP rate • **icmpSize** - ICMP packet size • **badSip** - SIP==mcast or bcast • **lanD** - DIP==SIP • **smurf** - ICMP echo to directed broadcast • **fraggle** - UDP echo to directed broadcast • **synFlood** - SYN rate • **portScan** - Detect TCP/UDP Port Probes
stats	(Optional) Specifies that all threat statistics should be displayed.

Defaults

- If the *mitigation-type* is not specified and the stats option is specified, statistics for all mitigation-types are displayed.

- If no option is specified, the configuration for all mitigation-types are displayed.

Mode

All command modes.

Examples

This example shows how to display Denial of Service configuration for this device. For details on how to set these parameters, refer to "hostdos" on page 79-3.

```
S Chassis(rw)->show hostDoS
show hostDos
hostDoS is globally enabled
arpNd      is enabled , logging is enabled
badSIP     is disabled, logging is enabled , rate is 0 per-second
fraggle    is disabled, logging is enabled , rate is 0 per-second
icmpFlood  is disabled, logging is enabled , rate is unlimited
icmpFrag   is disabled, logging is enabled , rate is 0 per-second
icmpSize   is disabled, logging is enabled , rate is 0 per-second
icmpSize   max-length is 1024
lanD       is enabled , logging is enabled , rate is 0 per-second
portScan   is disabled, logging is enabled , rate is 0 per-second
smurf      is disabled, logging is enabled , rate is 0 per-second
spoof      is disabled, logging is enabled , rate is 0 per-second
synFlood   is disabled, logging is enabled , rate is unlimited
xmasTree   is disabled, logging is enabled , rate is 0 per-second
S Chassis(rw)->
```

The following example displays statistics for each threat:

```
S Chassis(rw)->show hostDoS stats
 HostDos is globally Enabled
 ------------------------------------------------------------------------
 Threat       Ena     Violation    Last Occurrence
              ble Log   Count    Port       VLAN Date and Time
 ------------------------------------------------------------------------
 arpNd         Y   Y  0          N/A        N/A  N/A
 badSIP        N   Y  0          N/A        N/A  N/A
 fraggle       N   Y  0          N/A        N/A  N/A
 icmpFlood     N   Y  0          N/A        N/A  N/A
 icmpFrag      N   Y  0          N/A        N/A  N/A
 icmpSize      N   Y  0          N/A        N/A  N/A
 lanD          Y   Y  0          N/A        N/A  N/A
 portScan      N   Y  0          N/A        N/A  N/A
 smurf         N   Y  0          N/A        N/A  N/A
 spoof         N   Y  0          N/A        N/A  N/A
 synFlood      N   Y  0          N/A        N/A  N/A
 xmasTree      N   Y  0          N/A        N/A  N/A
```

```
S Chassis(rw)->
```

hostdos

Use this command to configure Host DoS on this device.

Syntax

hostdos {*mitigation-type* | **enable** | **icmp-maxlength** *icmp-maxlength*} [**rate** *count* [**per-second** | **per-minute** | **per-hour** | **per-day**]] [**nolog**]

no hostdos [*mitigation-type*] [**enable** | **disable**]

Parameters

mitigation-type	Specifies an attack type to be mitigated. Valid values are: • **arpNd** – Excessive ARP or ND packets from a single host • **spoof** – Source interface is not this router interface • **xmasTree** – Inappropriate TCP flags • **icmpFrag** – ICMP with fragments specified • **icmpFlood** – ICMP rate • **icmpSize** – ICMP packet size – [**maxlength** *maxlength*] – Maximum ICMP frame size • **badSip** – SIP equals multicast or broadcast • **lanD** – DIP equals SIP • **smurf** – ICMP echo to directed broadcast • **fraggle** – UDP echo to directed broadcast • **synFlood** – SYN rate • **portScan** – Detect TCP/UDP Port Probes
enable	Globally enables Host DoS on this device. Default: **enabled**.
icmp-maxlength *icmp-maxlength*	Sets the max length for icmp packets. Default: **1024**
rate *count* **per-second** | **per-minute** | **per-hour** | **per-day**	(Optional) Specifies the rate at which events will be acted upon (such as the frame being discarded). *count* specifies the number of events allowed per specified time period. Host DoS will act upon any events in excess of the count for the specified time period. Valid values: **0**-**4294967294**. Default: **0**. Default rate interval: **per-second**.
nolog	(Optional) Specifies that logging should be disabled for the specified threat.

Defaults

- If an event rate is not specified, all events are acted upon.
- If the ICMP maxlength is not set, the ICMP maxlength is set to 1024.

Mode

Configuration command, Global configuration.

Usage

A rate count of **0** indicates that all frames that match the enabled threat will be discarded.

The **icmp-maxlength** sets the ICMP maximum frame size. Default value: **1024**.

Host DoS must be enabled globally for any enabled threat to be mitigated. Threats are enabled separately.

Logging for all threats is enabled by default. A threat is logged each time it is acted upon (frame is discarded). Use the **nolog** option to disable logging for the specified threat. To re-enable logging for a specific mitigation type, use the **no hostdos** *mitigation-type* command to reset the mitigation type to its default values which includes logging enabled. You must then re-enable the threat if you wish to resume monitoring that threat.

Example

This example shows how to:

- Globally enables Host Dos on this device
- Enable the checkSpoof mitigation type, with a rate of 5 per-minute
- Enable the XmasTree mitigation type and disable logging for this threat

```
S Chassis(rw-config)->hostdos enable
S Chassis(rw-config)->hostDoS spoof rate 5 per-minute
S Chassis(rw-config)->hostdos xmasTree nolog
S Chassis(rw-config)->show hostDoS
hostDoS is globally enabled
 badSIP     is disabled, logging is enabled, rate is   0 per-second
 fraggle    is disabled, logging is enabled, rate is   0 per-second
 icmpFlood  is disabled, logging is enabled, rate is   0 per-second
 icmpFrag   is disabled, logging is enabled, rate is   0 per-second
 icmpSize   is disabled, logging is enabled, rate is   0 per-second
 icmpSize   max-length is 1024
 lanD       is disabled, logging is enabled, rate is   0 per-second
 portScan   is disabled, logging is enabled, rate is   0 per-second
 smurf      is disabled, logging is enabled, rate is   0 per-second
 spoof      is enabled, logging is enabled, rate is   5 per-minute
 synFlood   is disabled, logging is enabled, rate is   0 per-second
 xmasTree   is enabled, logging is disabled, rate is   0 per-second
S Chassis(rw-config)->
```

80

Flow Setup Throttling (FST) Commands

This chapter describes the Flow Setup Throttling (FST) set of commands and how to use them. For information about configuring Flow Setup Throttling, refer to the "Flow Setup Throttling Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show flowlimit	80-1
set flowlimit	80-3
set flowlimit limit	80-3
clear flowlimit limit	80-4
set flowlimit action	80-5
clear flowlimit action	80-6
show flowlimit class	80-7
set flowlimit port	80-8
set flowlimit port class	80-9
set flowlimit port status	80-9
clear flowlimit port class	80-10
set flowlimit shutdown	80-10
set flowlimit notification	80-11
clear flowlimit notification interval	80-12
clear flowlimit stats	80-12

show flowlimit

Use this command to display flow setup throttling information.

Syntax

show flowlimit [**port** [*port-string*] | **stats** [*port-string*] | **class** [*class*]}

Parameters

port	(Optional) Displays flow setup throttling port settings for one or all ports.
stats	(Optional) Displays flow setup throttling statistics for one or all ports.

port-string	(Optional) Specifies **port** or **stats** information should display for the specified or all ports.
class	(Optional) Displays flow setup throttling class settings.
class	(Optional) Specifies the flow setup throttling class to display: • *class-index* – A user defined classification type represented by a numeric value. • **userport** - An edge port with a single attached user. Class index = 1. • **serverport** - A port with a server attached to it. Class index = 2. • **aggregateduser** - An edge port with multiple users attached to it. Class index = 3 • **interswitchlink** - A high speed interconnect port between switches or routers. Class index = 4. • **unspecified** - A port for which the intended usage is unknown. Class index = 5.

Defaults

- If *port-string* is not specified, **port** or **stats** flow setup throttling information will be displayed for all ports.
- If *class* is not specified, flow setup throttling information displays for all classes.
- If no options are specified, system configuration flow setup throttling information displays.

Mode

All command modes.

Examples

This example shows how to display flow setup throttling information for port 1 on module 2. In this case, it is enabled for FST with an “unspecified” port classification, is currently operational, and has no FST action assigned:

```
S Chassis(rw)->show flowlimit port ge.2.1
Flow setup throttling port configuration:

Port      Class              State    Status               Reason     Layer
--------- ------------------ -------- -------------------- ---------- -----
ge.2.1    unspecified        enabled  operational          noAction   L4
```

This example displays system level flowlimit settings:

```
S Chassis(rw)->show flowlimit
Flow setup throttling system configuration
-----------------------------------------
System state                    :disabled
SNMP notification               :enabled
Interface shutdown              :disabled
Notification interval           :120 seconds
Max supported flow count        :196608 flows
Max supported setup rate        :20000 flows/second
```

```
S Chassis(rw)->
```

This example displays the user port class flow setup throttling settings:

```
S Chassis(rw)->show flowlimit class userport
Flow setup throttling class configuration:
Class              Limit                  Action
------------------ ---------------------- ----------------------------------
userPort           limit1     :4          action1    :notify
                   limit2     :6          action2    :disable,notify
S Chassis(rw)->
```

set flowlimit

Use this command to globally enable or disable flow setup throttling.

Syntax

set flowlimit {**enable** | **disable**}

Parameters

enable | **disable**	Globally enables or disables FST. Flow setup throttling is disabled by default.

Defaults

None.

Mode

All command modes.

Example

This example shows how to globally enable FST:

```
S Chassis(rw)->set flowlimit enable
```

set flowlimit limit

Use this command to set a flow limit that will trigger an action for a port user classification.

Syntax

set flowlimit {**limit1** *limit* | **limit2** *limit*} [class-index | **userport** | **serverport** | **aggregateduser** | **interswitchlink** | **unspecified**]

Parameters

limit1 | **limit2**	Specifies this configuration as limit 1 or 2. Two limits assigned to two actions (describing what will occur when a certain flow limit is reached) can be defined per user classification.
limit	Specifies the number of flows that will trigger the associated action configuration. Valid values are **0** - **4294967295**.

class-index	Specifies a numeric value for the class user classification type. Valid values are from **0** - **4294967295**.
userport | **serverport** | **aggregateduser** | **interswitchlink** | **unspecified**	(Optional) Assigns this limit configuration to the user classification port type: • **userport** - An edge port with a single attached user. • **serverport** - A port with a server attached to it. • **aggregateduser** - An edge port with multiple users attached to it. • **interswitchlink** - A high speed interconnect port between switches or routers. • **unspecified** - A port for which the intended usage is unknown.

Defaults

If classification port type is not specified, the specified limit is applied to all port types.

Mode

All command modes.

Usage

Once configured, this limit can be associated with an action using the **set flowlimit action** command as described in "set flowlimit action" on page 80-5. This limit can be assigned to one or more ports using the **set flowlimit port class** command as described in "set flowlimit port" on page 80-8.

Example

This example shows how to set the flow limit 1 to 12 flows on ports classified as user ports:

```
S Chassis(rw)->set flowlimit limit1 12 userport
```

clear flowlimit limit

Use this command to remove a flow limit configuration.

Syntax

clear flowlimit {**limit1** | **limit2**} [*class-index*]

Parameters

limit1 | **limit2**	Specifies the configuration to be removed as limit 1 or 2.

class-index	Specifies a numeric value or classification type keyword for the class user classification type to assign to this action. Valid values are from **0** - **4294967295** or a classification type keyword: • **userport** - An edge port with a single attached user. Class index = 1. • **serverport** - A port with a server attached to it. Class index = 2. • **aggregateduser** - An edge port with multiple users attached to it. Class index = 3 • **interswitchlink** - A high speed interconnect port between switches or routers. Class index = 4. • **unspecified** - A port for which the intended usage is unknown. Class index = 5.

Defaults

If not specified, the limit will be removed from all port classification types.

Mode

All command modes.

Example

This example shows how to remove flow limit 1 from all port classifications:

```
S Chassis(rw)->clear flowlimit limit1
```

set flowlimit action

Use this command to associate an action with a flow limit. This is the action that will occur once the associated flow limit is reached.

Syntax

set flowlimit {**action1** | **action2**} [**notify**] [**drop**] [**disable**] [*class-index*]

Parameters

action1 | **action2**	Specifies this configuration as action 1 or 2. Two actions describing what will occur when a certain flow limit is reached can be defined per user classification. Action number must correspond to a flow limit configured using the **set flowlimit limit** command as described in "set flowlimit limit" on page 80-3.
notify	(Optional) When flow limit is reached, generates an SNMP trap notification (if the **set flowlimit notification** function is enabled as described in "set flowlimit notification" on page 80-11).
drop	(Optional) When flow limit is reached, drops excess flows and discard packets.
disable	(Optional) When flow limit is reached, disables the interface (if the **set flowlimit shutdown** function is enabled as described in "set flowlimit shutdown" on page 80-10). This will clear all FST settings on the port.

class-index	Specifies a numeric value or classification type keyword for the class user classification type to assign to this action. Valid values are from **0** - **4294967295** or a classification type keyword: • **userport** - An edge port with a single attached user. Class index = 1. • **serverport** - A port with a server attached to it. Class index = 2. • **aggregateduser** - An edge port with multiple users attached to it. Class index = 3 • **interswitchlink** - A high speed interconnect port between switches or routers. Class index = 4. • **unspecified** - A port for which the intended usage is unknown. Class index = 5.

Defaults

If classification port type is not specified, the action is applied to all port classifications.

Mode

All command modes.

Example

This example shows how to set flow limiting action 1 to discard all flows exceeding flow limit 1 on ports classified as user ports:

```
S Chassis(rw)->set flowlimit action1 discard userport
```

clear flowlimit action

Use this command to remove a flow limiting action configuration.

Syntax

clear flowlimit {**action1** | **action2**} [**notify**] [**drop**] [**disable**] [*class-index*]

Parameters

action1 | **action2**	Specifies the configuration to be removed as action 1 or 2.
notify	(Optional) Removes the notify action.
drop	(Optional) Removes the drop action.
disable	(Optional) Removes the disable action.
class-index	Specifies a numeric value or classification type keyword for the class user classification type to assign to this action. Valid values are from **0** - **4294967295** or a classification type keyword: • **userport** - An edge port with a single attached user. Class index = 1. • **serverport** - A port with a server attached to it. Class index = 2. • **aggregateduser** - An edge port with multiple users attached to it. Class index = 3 • **interswitchlink** - A high speed interconnect port between switches or routers. Class index = 4. • **unspecified** - A port for which the intended usage is unknown. Class index = 5.

Defaults

- If an action type is not specified, all action types will be removed.
- If a port type is not specified, the action will be removed from all port classifications.

Mode

All command modes.

Example

This example shows how to remove flow limiting action 1 from all port classifications:

```
S Chassis(rw)->clear flowlimit action1
```

show flowlimit class

Use this command to display flow limiting classification configuration(s).

Syntax

show flowlimit class [*class-index*]

Parameters

class-index	Specifies a numeric value or classification type keyword for the class user classification type to assign to this action. Valid values are from **0** - **4294967295** or a classification type keyword: • **userport** - An edge port with a single attached user. Class index = 1. • **serverport** - A port with a server attached to it. Class index = 2. • **aggregateduser** - An edge port with multiple users attached to it. Class index = 3 • **interswitchlink** - A high speed interconnect port between switches or routers. Class index = 4. • **unspecified** - A port for which the intended usage is unknown. Class index = 5.

Defaults

If port classification type is not specified, information related to all classifications will be displayed.

Mode

All command modes.

Example

This example shows how to show flow limits and associated actions configured for the various port classifications:

```
S Chassis(rw)->show flowlimit class

Flow setup throttling class configuration:
```

```
Class              Limit                 Action
------------------ --------------------- ------------------------------------
userPort           limit1     :800       action1    :notify
                   limit2     :1000      action2    :disable,notify

serverPort         limit1     :5000      action1    :notify
                   limit2     :6000      action2    :disable,notify

aggregatedUserPort limit1     :5000      action1    :notify
                   limit2     :6000      action2    :disable,notify

interSwitchLink    limit1     :14000     action1    :notify
                   limit2     :16000     action2    :disable,notify

unspecified        limit1     :0         action1    :notify
                   limit2     :0         action2    :disable,notify

S Chassis(rw)->
```

set flowlimit port

Use this command to enable or disable flow limiting on one or more port(s).

Syntax

set flowlimit port {**enable** | **disable**} [*port-string*]

Parameters

enable | **disable**	Enables or disables flow limiting on specified ports.
port-string	(Optional) Specifies port(s) on which to configure flow limiting parameters.

Defaults

If *port-string* is not specified, settings will apply to all ports.

Mode

All command modes.

Example

This example shows how to enable flowlimits on the GbE slot 2 ports 3 - 5:

```
S Chassis(rw)->set flowlimit enable ge.2.3-5
```

set flowlimit port class

Use this command to assign a flow limiting user classification to one or more port(s)

Syntax

set flowlimit port class *class-index* [*port-string*]

Parameters

class-index	Specifies a numeric value or classification type keyword for the class user classification type to assign to this action. Valid values are from **0** - **4294967295** or a classification type keyword: • **userport** - An edge port with a single attached user. Class index = 1. • **serverport** - A port with a server attached to it. Class index = 2. • **aggregateduser** - An edge port with multiple users attached to it. Class index = 3 • **interswitchlink** - A high speed interconnect port between switches or routers. Class index = 4. • **unspecified** - A port for which the intended usage is unknown. Class index = 5.
port-string	(Optional) Specifies port(s) on which to configure flow limiting class.

Defaults

If *port-string* is not specified, the specified class setting will apply to all ports.

Mode

All command modes.

Usage

A maximum of 10 user classification types can be defined per port as a combination of numeric values and predefined user classification types. Once a classification is assigned, these ports will be subject to the flow limit configured (with the **set flowlimit limit** command as described in "set flowlimit limit" on page 80-3) and the action configured (with the **set flowlimit action** command as described in "set flowlimit action" on page 80-5).

Entering a predefined user classification type sets the numeric class index value to the value specified in the parameter table.

Example

This example shows how to assign the user port classification type to ports ge.2.3-5:

```
S Chassis(rw)->set flowlimit port class userport ge.2.3-5
```

set flowlimit port status

Use this command to enable an interface previously disabled by a flow limiting action.

Syntax

set flowlimit port status operational [*port-string*]

Parameters

operational	Enables an interface previously disabled by a flow limiting action.
port-string	(Optional) Specifies port(s) on which to change the status to operational.

Defaults

If *port-string* is not specified, the operational status setting will apply to all ports.

Mode

All command modes.

Example

This example shows how to change the currently disabled port ge.2.5 to operational:

```
S Chassis(rw)->set flowlimit port status operational ge.2.5
```

clear flowlimit port class

Use this command to remove flow limiting port classification properties.

Syntax

clear flowlimit port class {*port-string*}

Parameters

port-string	(Optional) Specifies port(s) on which to remove flow limiting classification properties.

Defaults

If *port-string* is not specified, classifications will be removed from all ports.

Mode

All command modes.

Example

This example shows how to clear port classifications from all Gigabit Ethernet ports:

```
S Chassis(rw)->clear flowlimit port class ge.*.*
```

set flowlimit shutdown

Use this command to enable or disable the flow limit shut down function.

Syntax

set flowlimit shutdown {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables the flow limit shut down function.

Defaults

None.

Mode

All command modes.

Usage

When enabled, this allows ports configured with a "disable" action to shut down. For information on using the **set flowlimit limit** command to configure a disable action on a port, refer to "set flowlimit limit" on page 80-3.

Example

This example shows how to enable the flow limit shut down function:

```
S Chassis(rw)->set flowlimit shutdown enable
```

set flowlimit notification

Use this command to enable or disable flow limit notification, or to set a notification interval.

Syntax

set flowlimit notification {**disable** | **enable** | *interval*}

Parameters

disable | **enable**	Disables or enables SNMP notification.
interval	Specifies a notification interval (in seconds) for SNMP trap messages. Valid values are **0** - **4294967295**. Default: **120** seconds

Defaults

None.

Mode

All command modes.

Usage

When enabled, this allows ports configured with a "trap" action to send an SNMP trap message when a specified flow limit is reached.

Example

This example shows how to enable the flow limit notification function:

```
S Chassis(rw)->set flowlimit notification enable
```

clear flowlimit notification interval

Use this command to reset the SNMP flow limit notification interval to the default value of 120 seconds.

Syntax

clear flowlimit notification interval

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the SNMP flow limit notification interval:

```
S Chassis(rw)->clear flowlimit notification interval
```

clear flowlimit stats

Use this command to reset flow limit statistics counters on one or more port(s).

Syntax

clear flowlimit stats [*port-string*]

Parameters

port-string	(Optional) Resets flow limiting statistics on specific port(s).

Defaults

If *port-string* is not specified, statistics will be cleared on all ports.

Mode

All command modes.

Example

This example shows how to clear flow limit statistics counters on port 5:

```
S Chassis(rw)->clear flowlimit stats ge.1.5
```

81

Access Control List Commands

This chapter describes the Access Control List (ACL) set of commands and how to use them. For information about configuring ACLs, refer to the "Access Control List Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
Named Access Control Lists	81-1
Access Control List Entry Configuration Commands	81-5
Displaying and Applying Access Control List Commands	81-18

Named Access Control Lists

This section details ACL commands used to create, copy, and append named standard and extended IP ACLs. The commands used to configure named ACLs are:

For information about...	Refer to page...
ip access-list standard	81-1
ip access-list extended	81-2
ip access-list copy to	81-3
ip access-list append to	81-4
ip access-list check	81-4

ip access-list standard

Use this command to enter access list configuration mode for a standard ACL.

Syntax

ip access-list standard {*access-list-number | name*}

no ip access-list {*access-list-number | name*}

Parameters

*access-list-number	name*	Specifies a standard or extended access list number or name. When entering a number value, standard access list valid values are from **1** to **99**.

Defaults

None.

Mode

Configuration command, Global configuration.

Usage

The **ip access-list standard** command enters the rule configuration command mode for the specified standard ACL. Standard ACLs specify a source address.

A standard ACL MIB does not exist.

There are two ways to identify an ACL: a number or a name. The use of a number is for IPv4 ACLs only. Standard IPv4 ACL numbers range from 1 to 99. Names must start with an alpha character. A name may be quoted, as the quotes are stripped, but spaces are not supported the quoted string. A name cannot be one of the **show access-lists** keywords **brief** or **applied**, or any prefix thereof such as **?br?** or **?app?**. Names can be up to 64 characters in length.

Restrictions defined by an access list are applied by using the **ip access-group** command ("ip access-group" on page 81-18).

Note: An "implicit deny" is hard coded at the end of all ACLs. The implicit deny blocks anything not explicitly permitted within the ACL, including routing protocols and management connections.

The "no" form of this command removes the specified access list.

Example

This example creates standard access list 1, if it does not already exist, and enters access list 1 configuration mode:

```
S Chassis(rw-config)->ip access-list standard 1
S Chassis(rw-cfg-std-acl)->
```

ip access-list extended

Use this command to enter access list configuration mode for extended ACLs.

Syntax

```
ip access-list extended {access-list-number | name}
no ip access-list {access-list-number | name}
```

Parameters

access-list-number | *name*	Specifies a standard or extended access list number or name. When entering a number value, standard access list valid values are from **1** to **99**. Extended access list valid values are from **100** to **199**.

Defaults

None.

Mode

Configuration command, Global configuration.

Usage

The **ip access-list extended** command enters the rule configuration command mode for the specified extended access-list. Extended access-lists specify both a source and destination address.

There are two ways to identify an ACL: a number or a name. The use of a number is for IPv4 ACLs only. Extended IPv4 ACL numbers range from 100 to 199. Names must start with an alpha character. A name may be quoted, as the quotes are stripped, but spaces are not supported the quoted string. A name cannot be one of the **show access-lists** keywords **brief** or **applied**, or any prefix thereof such as **?br?** or **?app?**. Names can be up to 64 characters in length.

Restrictions defined by an access list are applied by using the **ip access-group** command ("ip access-group" on page 81-18).

Note: An "implicit deny" is hard coded at the end of all ACLs. The implicit deny blocks anything not explicitly permitted within the ACL, including routing protocols and management connections.

The "no" form of this command removes the specified access list.

Example

This example creates extended access list 100, if it does not already exist, and enters access list 100 configuration mode:

```
S Chassis(rw-config)->ip access-list extended 100
S Chassis(rw-cfg-ext-acl)->
```

ip access-list copy to

Use this command to copy a pre-existing ACL to a new ACL.

Syntax

ip access-list {**standard** | **extended**} {*access-list-number* | *name*} **copy to** {*access-list-number* | *name*}

Parameters

standard | **extended**	Specifies whether the access list is a standard or extended access list.
access-list-number | *name*	Specifies a standard or extended access list number or name. When entering a number value, standard access list valid values are from **1** to **99**. Extended access list valid values are from **100** to **199**.

Defaults

None.

Mode

Configuration command, Global configuration**.**

Usage

When copying an access list, the access list to copy must already exist. When copying an access list, the access list the original is being copied to must not already exist.

ACL names can be up to 64 characters in length.

Example

This example creates standard access list 2 and copys standard access list 1 to it:

```
S Chassis(rw-config)->ip access-list standard 1 copy to 2
S Chassis(rw-config)->
```

ip access-list append to

Use this command to append the specified access list to another access list.

Syntax

ip access-list {**standard** | **extended**} {*access-list-number* | *name*} **append to** {*access-list-number* | *name*}

Parameters

standard | **extended**	Specifies whether the access list is a standard or extended access list.
access-list-number | *name*	Specifies a standard or extended access list number or name. When entering a number value, standard access list valid values are from **1** to **99**. Extended access list valid values are from **100** to **199**.
append to *access-list-number* | *name*	Appends this entire standard or extended access list to the specified pre-existing access list.

Defaults

None.

Mode

Configuration command, Global configuration**.**

Usage

When appending an access list, both the ACL to append and the ACL to append to must already exist.

Example

This example appends standard access list 1 to a pre-existing standard access list 3:

```
S Chassis(rw-config)->ip access-list standard 1 append to 3
S Chassis(rw-config)->
```

ip access-list check

Use this command to check the efficiency of an access list.

Syntax

ip access-list {**standard** | **extended**} {*access-list-number* | *name*} **check**

Parameters

standard | **extended**	Specifies whether the access list is a standard or extended access list.
access-list-number | *name*	Specifies a standard or extended access list number or name. When entering a number value, standard access list valid values are from **1** to **99**. Extended access list valid values are from **100** to **199**.

Defaults

None.

Mode

Configuration command, Global configuration.

Usage

This command checks the efficiency of an access-list by determining if any rules are hidden by preceding rules.

Example

This example checks the efficiency of standard access list 1:

```
S Chassis(rw-config)->ip access-list standard 1 check
access-list 1 is efficient -- no rules are hidden by preceding rules.
S Chassis(rw-config)->
```

Access Control List Entry Configuration Commands

This section details ACL commands used to configure deny or permit ACL entries, log, delete, insert, replace or move an ACL entry, or create an ACL comment entry. The commands used to configure named ACL entries are:

For information about...	Refer to page...
permit	81-6
deny	81-9
log	81-12
delete	81-12
insert before	81-13
replace	81-15
move before	81-16
remark	81-17

permit

Use this command to create a permit access list rule entry.

Syntax

Standard IP Access List:

permit {*source source-wildcard* | **any** | **host** *ip-address*]} [**log** | **log-verbose**]

Extended IP Access List:

permit {*protocol-num* | **ip** | **ah** | **esp** | **gre**} {*source source-wildcard* | **any** | **host** *ip-address*} {*destination destination-host wildcard* | **any** | **host** *ip-address*} [**dscp** *code*] [**precedence** *value*] [**tos** *value*] [**log** | **log-verbose**]

permit tcp {*source source-wildcard* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *source-port*] [**range** *start-port end-port*] {*destination destination-host wildcard* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *dest-port*] [**range** *start-port end-port*] [**established**] [**dscp** *code*] [**precedence** *value*] [**tos** *value*] [**log** | **log-verbose**]

permit udp {*source source-wildcard* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *source-port*] [**range** *start-port end-port*] {*destination destination-host wildcard* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *dest-port*] [**range** *start-port end-port*] [**dscp** *code*] [**precedence** *value*] [**tos** *value*] [**log** | **log-verbose**]

permit icmp {*source source-wildcard* | **any** | **host** *ip-address*} {*destination destination-host wildcard* | **any** | **host** *ip-address*} [**msg** *icmp-msg*] [**dscp** *code*] [**precedence** *value*] [**tos** *value*] [**log** | **log-verbose**]

Parameters

protocol-num	Specifies an IPv4 protocol for which to permit access. Valid values are protocol numbers from 0 - 255.
ip	Specifies any IPv4 protocol (0 - 255)
ah	Specifies the Authentication Header protocol
esp	Specifies the Encapsulation Security Payload protocol
gre	Specifies the Generic Router Encapsulation protocol
tcp	Specifies the Transmission Control Protocol
udp	Specifies the User Datagram Protocol
icmp	Specifies the IP Internet Control Message Protocol
source	Specifies the IPv4 address of the network or host from which the packet will be sent.
source-wildcard	Specifies the bits to ignore in the *source* address.
destination	Specifies the IPv4 address of the network or host to which the packet will be sent.
destination-wildcard	Specifies the bits to ignore in the *destination* address.
any	Specifies that any source or destination (extended access list only) address applies to this rule entry.
host *ip-address*	Specifies a specific host address that will be applied to this rule entry.
msg *icmp-msg*	(Optional) Specifies a single ICMP message type by entering a keyword. Supported message type keywords are provided in Table 81-1 on page 81-8.

eq | **neq** | **gt** | **lt** {*source-port* | *dest-port*}	(Optional) Specifies that a source or destination port is permitted. The meaning of the keywords are: • **eq** - permits the specified source or destination port • **gt** - permits source or destination ports greater than the value specified • **lt** - permits source or destination ports less than the value specified • **neq** - permits source or destination ports that are not equal to the value specified
range *start-port end-port*	(Optional) Specifies a range of source or destination ports permitted.
established	(Optional) Specifies that only established TCP connections are permitted. A match is made if ACK or RST bits are set.
dscp *code*	(Optional) Specifies a DiffServe Code Point (DSCP) value to match against this packet's DSCP code. Valid values are **0** - **63**, or one of the following keywords: • **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **af44**, – Assured Forwarding • **be** – best effort • **cs1** - **cs7** – Class Selector • **ef** – Expedited Forwarding
precedence *value*	(Optional) Specifies an IP Precedence value. Valid values are **0** - **7**, or in order from high to low: **critical**, **flash**, **flash-override**, **immediate**, **internet**, **network**, **priority**, **routine**.
tos *value*	(Optional) Specifies a Type of Service (ToS) value. Valid values are **0** - **15**, or **max-reliability**, **max-throughput**, **min-delay**, **min-monetary-cost**, **normal**.
log | **log-verbose**	(Optional) Enables syslog or verbose syslog messaging for an ACL rule hit.

Defaults

- If the **msg** option is not specified for an ICMP rule, all ICMP message types are permitted.
- If the log or log-verbose options are not specified, syslog messaging does not occur for an ACL rule hit.
- If DSCP code is not specified, none is applied to the permit entry.
- If a precedence value is not specified, none is applied to the permit entry.
- If a ToS value is not specified, none is applied to the permit entry.

Mode

Configuration command, standard or extended access list configuration.

Usage

Entering any IPv4 protocol number will configure the permit entry for the specified protocol, but will limit configurable parameters to the list in the *protocol-num* syntax. Specifying the **tcp**, **udp**, or **icmp** keywords will provide the extended parameter set listed in the syntax for these keywords.

Access list logging is throttled to 1 log message per second. If there are multiple access list rules with logging enabled (log or log-verbose), and more then one frame is transmitted per second that can hit those rules, only the first frame will generate a message. Logging is sampling and does not report every time that a rule with logging enabled is hit.

Source and destination wildcard provides an inverted mask (specifies the don't care bits as 1s). 0.0.0.0 specifies an exact match.

The any option is short hand for 0.0.0.0 255.255.255.255.

Table 81-1 contains supported ICMP message types with message codes and descriptions.

Table 81-1 ICMP Message Types

Message Type	Message Code and Description
information-reply	(16,0) Information replies
information-request	(15,0) Information requests
ipv6-i-am-here	(34,0) IPv6 I Am Here
ipv6-where-are-you	(33,0) IPv6 Where are you
mask-reply	(18,0) Mask replies
mask-request	(17,0) Mask requests
mobile-redirect	(32,0) Mobile host redirect
mobile-reg-reply	(36,0) Mobile registration reply
mobile-reg-request	(35,0) Mobile registration request
net-redirect	(5,0) Network redirect
net-tos-redirect	(5,2) Net redirect for TOS
net-tos-unreachable	(3,11) Network unreachable for TOS
net-unreachable	(3,0) Net unreachable
network-unknown	(3,6) Network unknown
no-room-for-option	(12,2) Parameter required but no room
option-missing	(12,1) Parameter required but not present
packet-too-big	(3,4) Fragmentation needed and DF set
parameter-problem	(12,0) Parameter problem indicated
port-unreachable	(3,3) Port unreachable
precedence-unreachable	(3,15) Precedence cutoff
protocol-unreachable	(3,20) Protocol unreachable
reassembly-timeout	(11,1) Reassembly timeout
router-advertisement	(9,0) Router discovery advertisements
router-solicitation	(10,0) Router discovery solicitations
source-quench	(4,0) Source quenches
source-route-failed	(3,5) Source route failed
timestamp-reply	(14,0) Timestamp replies
timestamp-request	(13,0) Timestamp requests

Table 81-1 ICMP Message Types

Message Type	Message Code and Description
traceroute	(30,0) Traceroute
ttl-exceeded	(11,0) Time-to-live exceeded

Examples

This example enters configuration mode for standard access list 2 and configures a permit entry for source address 10.0.0.1 with a source wildcard of `0.0.255.255`:

```
S Chassis(rw-config)->ip access-list standard 2
S Chassis(rw-cfg-std-acl)->permit 10.0.0.1 0.0.255.255
S Chassis(rw-cfg-std-acl)->
```

This example enters configuration mode for extended access list 120 and configures a permit entry for the IP protocol with a source address 20.0.0.1 and source wildcard of 0.0.255.255 and a destination address of any:

```
S Chassis(rw-config)->ip access-list extended 120
S Chassis(rw-cfg-ext-acl)->permit ip 20.0.0.1 0.0.255.255 any
S Chassis(rw-cfg-ext-acl)->
```

This example enters configuration mode for extended access list 130 and configures a permit entry for the ICMP protocol with a source network address of 120.50.0.1 and source wildcard of 0.0.255.255 and a destination address of 120.60.0.1 and destination wildcard of 0.0.255.255 and a router advertisement ICMP message type:

```
S Chassis(rw-config)->ip access-list extended 130
S Chassis(rw-cfg-ext-acl)->>permit icmp 120.50.0.1 0.0.255.255 120.60.0.1
0.0.255.255 msg router-advertisement
S Chassis(rw-cfg-ext-acl)-
```

deny

Use this command to create a deny access list rule entry.

Syntax

Standard IP Access List:

deny {*source source-wildcard* | **any** | **host** *ip-address*]} [**log** | **log-verbose**]

Extended IP Access List:

deny {*protocol-num* | **ip** | **ah** | **esp** | **gre**} {*source source-wildcard* | **any** | **host** *ip-address*} {*destination destination-host wildcard* | **any** | **host** *ip-address*} [**dscp** *code*] [**precedence** *value*] [**tos** *value*] [**log** | **log-verbose**]

deny tcp {*source source-wildcard* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *source-port*] [**range** *start-port end-port*] {*destination destination-host wildcard* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *dest-port*] [**range** *start-port end-port*] [**established**] [**dscp** *code*] [**precedence** *value*] [**tos** *value*] [**log** | **log-verbose**]

deny udp {*source source-wildcard* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *source-port*] [**range** *start-port end-port*] {*destination destination-host wildcard* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *dest-port*] [**range** *start-port end-port*] [**dscp** *code*] [**precedence** *value*] [**tos** *value*] [**log** | **log-verbose**]

```
deny icmp {source source-wildcard | any | host ip-address} {destination
destination-host wildcard | any | host ip-address} [msg icmp-msg] [dscp code]
[precedence value] [tos value] [log | log-verbose]
```

Parameters

protocol-num	Specifies an IPv4 protocol for which to deny access. Valid values are protocol numbers from 0 - 255.
ip	Specifies any IPv4 protocol (0 - 255)
ah	Specifies the Authentication Header protocol
esp	Specifies the Encapsulation Security Payload protocol
gre	Specifies the Generic Router Encapsulation protocol
tcp	Specifies the Transmission Control Protocol
udp	Specifies the User Datagram Protocol
icmp	Specifies the IP Internet Control Message Protocol
source	Specifies the IPv4 address of the network or host from which the packet is sent.
source-wildcard	Specifies the bits to ignore in the *source* address.
destination	Specifies the IPv4 address of the network or host to which the packet will be sent.
destination-wildcard	Specifies the bits to ignore in the *destination* address.
any	Specifies that any source or destination (extended access list only) address applies to this rule entry.
host *ip-address*	Specifies a specific host address that will be applied to this rule entry.
msg *icmp-msg*	(Optional) Specifies a single ICMP message type by entering a keyword. Supported message type keywords are provided in Table 81-1 on page 81-8.
eq | **neq** | **gt** | **lt** {*source-port* | *dest-port*}	(Optional) Specifies that a source or destination port is permitted. The meaning of the keywords are: • **eq** - permits the specified source or destination port • **gt** - permits source or destination ports greater than the value specified • **lt** - permits source or destination ports less than the value specified • **neq** - permits source or destination ports that are not equal to the value specified
range *start-port end-port*	(Optional) Specifies a range of source or destination ports permitted.
established	(Optional) Specifies that only established TCP connections are permitted. A match is made if ACK or RST bits are set.

dscp *code*	(Optional) Specifies a DiffServe Code Point (DSCP) value to match against this packet's DSCP code. Valid values are **0** - **63**, or one of the following keywords: • **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **af44**, – Assured Forwarding • **be** – best effort • **cs1** - **cs7** – Class Selector • **ef** – Expedited Forwarding
precedence *value*	(Optional) Specifies an IP Precedence value. Valid values are **0** - **7**, or in order from high to low: **critical**, **flash**, **flash-override**, **immediate**, **internet**, **network**, **priority**, **routine**.
tos *value*	(Optional) Specifies a Type of Service (ToS) value. Valid values are **0** - **15**, or **max-reliability**, **max-throughput**, **min-delay**, **min-monetary-cost**, **normal**.
log | **log-verbose**	(Optional) Enables syslog or verbose syslog messaging for an ACL rule hit.

Defaults

- If the **msg** option is not specified for an ICMP rule, all ICMP message types are denied.
- If the log or log-verbose options are not specified, syslog messaging does not occur for an ACL rule hit.
- If DSCP code is not specified, none is applied to the deny entry.
- If a precedence value is not specified, none is applied to the deny entry.
- If a ToS value is not specified, none is applied to the deny entry.

Mode

Configuration command, standard or extended access list configuration.

Usage

Entering any IPv4 protocol number will configure the deny entry for the specified protocol, but will limit configurable parameters to the list in the *protocol-num* syntax. Specifying the **tcp**, **udp**, or **icmp** keywords will provide the extended parameter set listed in the syntax for these keywords.

Access list logging is throttled to 1 log message per second. If there are multiple access list rules with logging enabled (log or log-verbose), and more then one frame is transmitted per second that can hit those rules, only the first frame will generate a message. Logging is sampling and does not report every time that a rule with logging enabled is hit.

Source and destination wildcard masks are inverted. That is, they specify the "don't care" bits as 1.

The **any** option is short hand for 0.0.0.0 255.255.255.255.

Examples

This example enters configuration mode for standard access list 2 and configures a deny entry for source address 10.0.0.1 with a source wildcard of `0.0.255.255`:

```
S Chassis(rw-config)->ip access-list standard 2
S Chassis(rw-cfg-std-acl)->deny 10.0.0.1 0.0.255.255
S Chassis(rw-cfg-std-acl)->
```

This example enters configuration mode for extended access list 120 and configures a deny entry for the IP protocol with a source address 20.0.0.1 and source wildcard of 0.0.255.255 and a destination address of any and destination wildcard of 0.0.0.255:

```
S Chassis(rw-config)->ip access-list extended 120
S Chassis(rw-cfg-ext-acl)->deny ip 20.0.0.1 0.0.255.255 any 0.0.0.255
S Chassis(rw-cfg-ext-acl)->
```

log

Use this command to enable a standard or detailed logging access list rule entry.

Syntax

log [*entry* | **implicit** | **all**]

Parameters

entry	(Optional) Specifies a sequence numbered entry to log when a hit occurs. Valid values: **1** - **5000**. Default value: **all**
implicit	(Optional) Specifies the logging of a final implicit deny hit.
all	(Optional) Specifies that all hits are to be logged, including the final implicit deny.

Defaults

If no option is specified, all hits are logged, including the final implicit deny.

Mode

Configuration command, standard or extended access list configuration.

Usage

ACL logging is throttled to 1 log message per second. If there are multiple ACL rules with logging enabled (log or log-verbose), and more then one frame is transmitted per second that can hit those rules, only the first frame will generate a message. Logging is sampling and does not report every time that a rule with logging enabled is hit.

Example

This example enters configuration mode for standard access list 2 and enables standard logging for a final implicit deny hit:

```
S Chassis(rw-config)->ip access-list standard 2
S Chassis(rw-cfg-std-acl)->log implicit
S Chassis(rw-cfg-std-acl)->
```

delete

Use this command to delete a pre-existing access list rule entry or range of entries.

Syntax

delete {*entry* | **from** *entry* **to** *entry*}

Parameters

entry | **from** *entry* **to** *entry*]	(Optional) Specifies an entry or range of entries to delete. When deleting a range of entries, **from** specifies the beginning of the range, and **to** specifies the end of the range inclusive. An entry is a valid pre-existing access list rule from **1** to **5000**.

Defaults

None.

Mode

Configuration command, standard or extended access list configuration.

Examples

This example enters configuration mode for standard access list 2 and deletes rule entry 20:

```
S Chassis(rw-config)->ip access-list standard 2
S Chassis(rw-cfg-std-acl)->delete 20
S Chassis(rw-cfg-std-acl)->
```

This example enters configuration mode for standard access list 2 and deletes rule entry 10 - 12:

```
S Chassis(rw-config)->ip access-list standard 2
S Chassis(rw-cfg-std-acl)->delete from 10 to 12
S Chassis(rw-cfg-std-acl)->
```

insert before

Use this command to insert an access list rule entry.

Syntax

Standard IP Access List:

insert before *entry* {**remark** "*text*" | {**permit** | **deny**} {*source source-wildcard* | **any** | **host** *ip-address*} [**log** | **log-verbose**]}

Extended IP Access List:

insert before *entry* {**remark "text"** | {**permit** | **deny**} *protocol* {*source source-wildcard* | **any** | **host** *ip-address*} {*destination destination-wildcard* | **any** | **host** *ip-address*} [**log** | **log-verbose**] [**dscp** *dscp-code*] [**precedence** *precedence*] [**tos** *tos*]}

Parameters

entry	Specifies an entry to place the inserted rule before. An entry is a valid pre-existing access list rule or the explicit deny which is the default entry **1**.
remark *text*	(Optional) Specify a text remark that will be associated with this ACL. Valid values: Up to 64 characters within double quotes (**""**).
deny | **permit** *protocol*	Denies or permits access if specified conditions are met. For *protocol* details see "permit" on page 81-6 or "deny" on page 81-9.

source	Specifies the IP address or range of the network or host from which the packet will be sent.
source-wildcard	Specifies the bits to ignore in the *source* address.
destination	Specifies the IP address or range of the network or host to which the packet will be sent.
destination-wildcard	Specifies the bits to ignore in the *destination* address.
any	Specifies that any source or destination (extended access list only) address applies to this rule entry.
host *ip-address*	Specifies a specific host address that will be applied to this rule entry.
log | **log-verbose**	(Optional) Enable syslog for ACL entry hits. **log** enables standard syslog messaging on an access list rule hit and **log-verbose** enables a detailed level syslog messaging on an access list rule hit.
dscp *dscp-code*	(Optional) Specifies a diffserve code point number of name. Valid values are **0** - **63**, or **be**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **af44**, **ef**
precedence *precedence*	(Optional) Specifies the IP precedence number or an IP precedence name. Valid values are **0** - **7**, or in order from high to low: **critical**, **flash**, **flash-override**, **immediate**, **internet**, **network**, **priority**, **routine**.
tos *tos*	(Optional) Specifies the IP Type of Service number or name. Valid values are **0** - **15**, or **max-reliability**, **max-throughput**, **min-delay**, **min-monetary-cost**, **normal**.

Defaults

- If **remark** is not specified, no remark is configured.
- If **log** or **log-verbose** are not specified, logging is not enabled.
- If **dscp** is not specified, a diffserve-code is not associated with this access list.
- If **precedence** is not specified, a precedence is not associated with this access list.
- If **tos** is not specified, a ToS is not associated with this access list.

Mode

Configuration command, standard or extended access list configuration.

Usage

ACL logging is throttled to 1 log message per second. If there are multiple ACL rules with logging enabled (log or log-verbose), and more then one frame is transmitted per second that can hit those rules, only the first frame will generate a message. Logging is sampling and does not report every time that a rule with logging enabled is hit.

Examples

This example enters configuration mode for standard access list **2** and inserts a permit IP protocol for source address **125.50.0.5** with a source wildcard of **0.0.0.255** before entry **10**:

```
S Chassis(rw-config)->ip access-list standard 2
S Chassis(rw-cfg-std-acl)->insert before 10 permit ip 125.50.0.5 0.0.0.255
S Chassis(rw-cfg-std-acl)->
```

replace

Use this command to replace an access list entry with a remark, permit or deny entry.

Syntax

Standard IP Access List:

replace *entry* {**remark "text"** | {**permit** | **deny**} {*source source-wildcard* | **any** | **host** *ip-address*}} [**log** | **log-verbose**]

Extended IP Access List:

replace *entry* {**remark "***text***"**| {**permit** | **deny**} *protocol* {*source source-wildcard* | **any** | **host** *ip-address*} {*destination destination-wildcard* | **any** | **host** *ip-address*} [**log** | **log-verbose**] [**dscp** *dscp-code* | **precedence** *precedence* | **tos** *tos*]}

Parameters

entry	Specify the entry to be replaced with the rule defined by this command.
remark *text*	Specify a text remark that will replace the specified entry. Valid values: Up to 64 characters within double quotes (**“”**).
deny | **permit** *protocol*	Specifies a deny or permits entry for this replacement entry. For *protocol* details see “permit” on page 81-6 or “deny” on page 81-9.
source	Specifies the IP address or range of a network or host from which the packet will be sent.
source-wildcard	Specifies the bits to ignore in the *source* address.
destination	Specifies the IP address or range of a network or host to which the packet will be sent.
destination-wildcard	Specifies the bits to ignore in the *destination* address.
any	Specifies that any source or destination (extended access list only) address applies to this rule entry.
host *ip-address*	Specifies a specific host address that will be applied to this rule entry.
log | **log-verbose**	(Optional) Enable syslog for ACL entry hits. **log** enables standard syslog messaging on an access list rule hit and **log-verbose** enables a detailed level syslog messaging on an access list rule hit.
dscp *dscp-code*	(Optional) Specifies a diffserve code point number of name. Valid values are **0** - **63**, or **be**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **af44**, **ef**
precedence *precedence*	(Optional) Specifies the IP precedence number or an IP precedence name. Valid values are **0** - **7**, or in order from high to low: **critical**, **flash**, **flash-override**, **immediate**, **internet**, **network**, **priority**, **routine**.
tos *tos*	(Optional) Specifies the IP Type of Service number or name. Valid values are **0** - **15**, or **max-reliability**, **max-throughput**, **min-delay**, **min-monetary-cost**, **normal**.

Defaults

- If **remark** is not specified, no remark is configured.
- If **log** or **log-verbose** are not specified, logging is not enabled.
- If **dscp** is not specified, a diffserve-code is not associated with this access list.

- If **precedence** is not specified, a precedence is not associated with this access list.
- If **tos** is not specified, a ToS is not associated with this access list.

Mode

Configuration command, standard or extended access list configuration.

Usage

ACL logging is throttled to 1 log message per second. If there are multiple ACL rules with logging enabled (log or log-verbose), and more then one frame is transmitted per second that can hit those rules, only the first frame will generate a message. Logging is sampling and does not report every time that a rule with logging enabled is hit.

Example

This example replaces entry 1 of access list 10 with a permit any source address :

```
S Chassis(rw-config)->ip access-list standard 10
S Chassis(rw-cfg-std-acl)->replace 1 permit any
S Chassis(rw-cfg-std-acl)->
```

move before

Use this command to move a pre-existing access list rule entry or range to the specified location in the access list.

Syntax

move before *entry1* **from** *entry2* **to** *entry3*

Parameters

entry1	Specifies a pre-existing access list entry before which entry range *entry2* to *entry3* will be moved.
entry2	Specifies a pre-existing access list entry that begins the range of entries that will be moved before *entry1*.
entry3	Specifies a pre-existing access list entry that ends the range of entries that will be moved before *entry1*.

Defaults

None.

Mode

Configuration command, standard or extended access list configuration.

Examples

This example enters configuration mode for standard access list 2 and moves rule entry 20 before rule entry 10:

```
S Chassis(rw-config)->ip access-list standard 2
S Chassis(rw-cfg-std-acl)->move before 10 from 20 to 20
S Chassis(rw-cfg-std-acl)->
```

This example enters configuration mode for standard access list 2 and moves rule entries 10 - 12 before rule entry 5:

```
S Chassis(rw-config)->ip access-list standard 2
S Chassis(rw-cfg-std-acl)->move before 5 from 10 to 12
S Chassis(rw-cfg-std-acl)->
```

remark

Use this command to enter a text comment into the access list at the next entry.

Syntax

remark "*text*"

Parameters

text	Specifies the text of up to 64 characters within double quotes (“”) to be entered as the next access list entry

Defaults

None.

Mode

Configuration command, standard or extended access list configuration.

Usage

Use the move before command on page 81-16 change a remark entry location.

Example

This example enters configuration mode for standard access list 10 and enters a remark specifying that the following entry permits any source address for this access list. The remark entry is followed by the permit any entry:

```
S Chassis(rw-cfg-std-acl)->show access-lists 10
Standard IP access list 10  (1 entries)
  -- implicit deny all --
S Chassis(rw-cfg-std-acl)->remark "The following entry permits any source
address."
S Chassis(rw-cfg-std-acl)->permit any
S Chassis(rw-cfg-std-acl)->show access-lists 10
Standard IP access list 10  (3 entries)
  1 "The following entry permits any source address."
  2 permit any
  -- implicit deny all --
S Chassis(rw-cfg-std-acl)->
```

Displaying and Applying Access Control List Commands

This section details ACL commands used to display ACL configuration and counters, clear ACL counters, and apply ACLs to an interface. The commands used to display and apply ACL entries are:

For information about...	Refer to page...
ip access-group	81-18
ip host-access	81-19
show access-lists	81-19
show access-lists applied	81-21
clear access-lists counters	81-22

ip access-group

Use this command to apply access restrictions to inbound or outbound frames on an interface when operating in router mode.

Syntax

ip access-group {*access-list-number* | *name*} {**in** | **out**} [**all-traffic** | **routed-traffic**]

no ip access-group {*access-list-number* | *name*} {**in** | **out**} [**all-traffic** | **routed-traffic**]

Parameters

access-list-number | *name*	Specifies the number or name of the access list to be applied to the access list. This is either a decimal number from **1** to **199** or a alpha-numeric text name of up to 64 characters.
in	Filters inbound frames.
out	Filters outbound frames.
all-traffic	(Optional) Specifies that the assigned ACL is applied to all traffic on the interface, not just the routed traffic.
routed-traffic	(Optional) Specifies that the assigned ACL is applied only to the routed traffic on the interface. (Default)

Defaults

If the traffic type is not specified, the ACL is applied only to routed traffic.

Mode

Configuration command, Interface configuration.

Usage

ACLs must be applied per routing interface. An ACL can either be applied to inbound or outbound frames. An ACL can be applied before it is created. The uncreated applied ACL will have no affect.

By default, an IPv4 ACL is only applied to routed traffic. To apply the IPv4 ACL to all traffic, use the **all-traffic** option.

The "no" form of this command removes the specified access list.

Example

This example shows how to apply access list 1 for all inbound frames on VLAN 1. Through the definition of access list 1, only frames with source 192.5.34.0 will be routed. All the frames with other sources received on VLAN 1 are dropped:

```
S Chassis(rw-config)->access-list 1 permit 192.5.34.0 0.0.0.255
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip access-group 1 in
```

ip host-access

Use this command to apply access restrictions to host services.

Syntax

ip host-access {*access-list-number* | *name*}

no ip host-access {*access-list-number* | *name*}

Parameters

access-list-number | *name*	Specifies the number or name of the access list. This is either a decimal number from **1** to **199** or a alpha-numeric text name of up to 64 characters.

Defaults

None.

Mode

Configuration command.

Usage

The "no" form of this command removes the specified access list.

Example

This example shows how to apply access list host1 to host services for this device:

```
S Chassis(rw-config)->ip host-access host1
S Chassis(rw-config)->
```

show access-lists

Use this command to display configured IP access lists configuration.

Syntax

show access-lists [*access-list-number* | *name*] [**from** *start-range* **to** *end-range*]] [**brief**]

Parameters

access-list-number	(Optional) Displays access list information for a specific access list. Valid values are between **1** and **199**.
name	(Optional) Displays access list information for a specific access list name.
from *start-range* **to** *end-range*	(Optional) Specifies a sequential range of ACL rules to display for the specified access list.
brief	(Optional) Displays a summary version of the specified context.

Defaults

If an option is not specified, the entire table of access lists will be displayed.

Mode

All command modes.

Examples

This example shows how to display IP access list number 101. This is an extended access list, which permits or denies ICMP, UDP and IP frames based on restrictions configured with the one of the **access list** commands:

```
S Chassis(rw-config)->show access-lists 101
Extended IP access list 101  (6 entries)
  1 permit icmp  host 18.2.32.130  any
  2 permit udp  host 198.92.32.130  host 171.68.225.126  eq 8080
  3 deny   ip  150.136.0.0  0.0.255.255  224.0.0.0  15.255.255.255
  4 deny   ip  11.6.0.0  0.1.255.255  224.0.0.0  15.255.255.255
  5 deny   ip  172.24.24.0  0.0.1.255  224.0.0.0  15.255.255.255
  -- implicit deny all --
```

This example shows how to display the brief form of applied IP access lists for this system:

```
S Chassis(rw-config)->show access-lists brief
IPv4 Access List (last 49 chars)                 Type Ents Deny count
------------------------------------------------ ---- ---- --------------------
1                                                std     7 0
2                                                std     2 0
3                                                std     2 0
This_is_an_extended_access_list_with_a_long_name ext     2 0
abcde                                            std     1 0
denyall                                          std     3 0
fred                                             ext     2 0

S Chassis(rw-config)->
```

show access-lists applied

Use this command to display applied IP access lists.

Syntax

show access-lists applied [**host** | **interfaces** [**vlan** | **inbound** | **outbound** | **in-and-out**]]

Parameters

host	(Optional) Displays access list information for all applied ingress to host services.
interfaces	(Optional) Displays access list information for all applied access list interface types or the specified interface type.
vlan	(Optional) Displays access list information for VLAN interfaces.
inbound	(Optional) Displays access list information for inbound interfaces.
outbound	(Optional) Displays access list information for outbound interfaces.
in-and-out	(Optional) Displays access list information for both inbound and outbound interfaces.

Defaults

If no option is applied, the entire table of applied access lists will be displayed.

Mode

All command modes.

Usage

ACL names may be up to 64 characters in length, but there is only room to display 32 characters (show applied) or 49 characters (show brief) on a single 80-character line. Names up to and including the maximum length will be displayed in their entirety. Names longer than the maximum display length will be displayed with an asterisk character followed by the last 31 or 48 characters of the name.

If an access list displays as ** unconfigured **, it means that the ACL applied to the interface or host has not yet been created. This is allowed, but the applied ACL will have no effect on traffic, since the ACL doesn't really exist yet.

Example

This example shows how to display applied IP access lists for this system:

```
S Chassis(rw-config)->show access-lists applied
Interface   IPv4 Access List (last 32 chars) Dir  Type Ents Deny count
----------- ------------------------------- ---- ---- ---- --------------------
Host        hostList                         ** unconfigured **
vlan.0.11   1                               in   std     7 0
vlan.0.13   *ed_access_list_with_a_long_name in   ext     2 0
vlan.0.13   nolist                          ** unconfigured **
S Chassis(rw-config)->
```

clear access-lists counters

Use this command to clear access list display counters.

Syntax

clear access-lists counters [{*access-list-number* | *name*} | **applied** [**host** | **interfaces** [**vlan** *vlan-id*] [**inbound** | **outbound** | **in-and-out**]]

Parameters

access-list-number | *name*	(Optional) Clears display counters for the specified access list number or name.
applied host | **interfaces**	(Optional) Clears display counters for applied host or interface statistics only.
vlan | **inbound** | **outbound** | **in-and-out**	(Optional) Clears only VLAN, only inbound, only outbound, or both inbound and outbound.

Defaults

If no option is specified, the clear action is applied to all access lists.

Mode

All command modes.

Example

This example clears the display counters for access list 10:

```
S Chassis(rw-config)->clear access-lists counters 10
S Chassis(rw-config)->
```

82

IPv6 Access Control List Commands

This chapter describes the IPv6 Access Control List (ACL) set of commands and how to use them. For information about configuring access lists, refer to the "Access List Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
Named Access Control Lists	82-1
Access Control List Entry Configuration Commands	82-5
Displaying and Applying Access Control List Commands	82-21

Named Access Control Lists

This section details access list commands used to create, copy, and append named standard and extended IPv6 access lists. The commands used to configure named access lists are:

For information about...	Refer to page...
ipv6 access-list standard	82-1
ipv6 access-list extended	82-2
ipv6 access-list copy to	82-3
ipv6 access-list append to	82-3
ipv6 access-list check	82-4

ipv6 access-list standard

Use this command to enter access list configuration mode for a standard IPv6 access list.

Syntax

ipv6 access-list standard *name*

no ipv6 access-list *name*

Parameters

name	Specifies a standard access list name.

Defaults

None.

Mode

Global configuration.

Usage

The **ipv6 access-list standard** command enters the rule configuration command mode for the specified standard IPv6 access list. Standard IPv6 access lists specify a source address.

A standard access list MIB does not exist.

You specify a name to identify a new ACL. A name may be quoted, as the quotes are stripped, but spaces are not supported in the quoted string. A name cannot be one of the **show access-lists** keywords **brief** or **applied**, or any prefix thereof such as **?br?** or **?app?**. Names can be up to 64 characters in length.

Restrictions defined by an access list are applied to an interface using the **ipv6 access-group** command ("ipv6 access-group" on page 82-22).

The **no ipv6 access-list standard** command deletes the specified access list.

Example

This example creates standard access list **ipv6list1**, if it does not already exist, and enters configuration mode for the specified list:

```
S Chassis(rw-config)->ipv6 access-list standard ipv6list1
S Chassis(su-cfg-ipv6-std-acl)->
```

ipv6 access-list extended

Use this command to enter access list configuration mode for extended IPv6 access lists.

Syntax

ipv6 access-list extended *name*

no ipv6 access-list *name*

Parameters

name	Specifies an extended access list name.

Defaults

None.

Mode

Global configuration.

Usage

The **ipv6 access-list extended** command enters the rule configuration command mode for the specified extended access list. Extended access lists specify both a source and destination address.

You specify a name to identify a new ACL. A name may be quoted, as the quotes are stripped, but spaces are not supported in the quoted string. A name cannot be one of the **show access-lists** keywords **brief** or **applied**, or any prefix thereof such as **?br?** or **?app?**. Names can be up to 64 characters in length.

Restrictions defined by an access list are applied to an interface using the **ipv6 access-group** command ("ipv6 access-group" on page 82-22).

The “no” form of this command removes the specified access list.

Example

This example creates extended IPv6 access list **extend10**, if it does not already exist, and enters access list **extend10** configuration mode:

```
S Chassis(su-config)->ipv6 access-list extended extend10
S Chassis(su-cfg-ipv6-ext-acl)->
```

ipv6 access-list copy to

Use this command to copy a pre-existing IPv6 access list to a new IPv6 access list.

Syntax

ipv6 access-list {**standard** | **extended**} *name* **copy to** *name*

Parameters

standard | **extended**	Specifies whether the access list is a standard or extended access list.
name	Specifies a standard or extended access name.

Defaults

None.

Mode

Global configuration**.**

Usage

When copying an access list, the access list to copy must already exist, and the access list the original is being copied to must not already exist.

Access list names can be up to 64 characters in length.

Example

This example creates standard IPv6 access list **acl2** and copys the already existing standard IPv6 access list **acl1** to it:

```
S Chassis(rw-config)->ipv6 access-list standard acl1 copy to acl2
S Chassis(rw-config)->
```

ipv6 access-list append to

Use this command to append the specified IPv6 access list to another IPv6 access list.

Syntax

ipv6 access-list {**standard** | **extended**} *name* **append to** *name*

Parameters

standard | **extended**	Specifies whether the IPv6 access list is a standard or extended IPv6 access list.
name	Specifies a standard or extended access name.

Defaults

None.

Mode

Configuration command, Global configuration.

Usage

This command appends the first access list specified to the second access list specified. When appending an IPv6 access list, both the access list to append and the access list to append to must already exist.

Example

This example appends standard IPv6 access list **acl1** to a pre-existing standard IPv6 access list **acl3**:

```
S Chassis(rw-config)->ipv6 access-list standard acl1 append to acl3
S Chassis(rw-config)->
```

ipv6 access-list check

Use this command to check the efficiency of an IPv6 access list.

Syntax

ipv6 access-list {**standard** | **extended**} *name* **check**

Parameters

standard | **extended**	Specifies whether the access list is a standard or extended access list.
name	Specifies a standard or extended access list name.

Defaults

None.

Mode

Configuration command, Global configuration.

Usage

This command checks the efficiency of an IPv6 access-list by determining if any rules are hidden by preceding rules.

Example

This example checks the efficiency of standard access list **acl1**:

```
S Chassis(rw-config)->ipv6 access-list standard acl1 check
access-list acl1 is efficient -- no rules are hidden by preceding rules.
S Chassis(rw-config)->
```

Access Control List Entry Configuration Commands

This section details access list commands used to configure deny or permit access list entries, log, delete, insert, replace or move an access list entry, or create an access list comment entry. The commands used to configure access list entries are:

For information about...	Refer to page...
permit	82-5
deny	82-9
log	82-12
delete	82-13
insert before	82-14
name	82-16
replace	82-17
move before	82-20
remark	82-21

permit

Use this command to create a permit IPv6 access list rule entry.

Syntax

Standard IPv6 Access List:

permit {*source-address/length* | **any** | **host** *ip-address*]} [**log** | **log-verbose**]

Extended IPv6 Access List:

permit {*protocol-num* | **ipv6** | **ah** | **esp** | **gre**} {*source-address/length* | **any** | **host** *ip-address*} {*destination-address/length* | **any** | **host** *ip-address*} [**dscp** *code*] [**traffic-class** *value*] [**flow-label** *value*] [**log** | **log-verbose**] [**routing**] [**routing-type** *type*] [**mobility**] [**mobility-type** *type*]

permit tcp {*source-address/length* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *source-port*] [**range** *start-port end-port*] {*destination-address/length* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *dest-port*] [**range** *start-port end-port*] [**established**] [**dscp** *code*] [**traffic-class** *value*] [**flow-label** *value*] [**log** | **log-verbose**] [**routing**] [**routing-type** *type*] [**mobility**] [**mobility-type** *type*]

permit udp {*source-address/length* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *source-port*] [**range** *start-port end-port*] {*destination-address/length* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *dest-port*] [**range** *start-port end-port*] [**dscp** *code*] [**traffic-class** *value*] [**flow-label** *value*] [**log** | **log-verbose**] [**routing**] [**routing-type** *type*] [**mobility**] [**mobility-type** *type*]

```
permit icmpv6 {source-address/length | any | host ip-address}
{destination-address/length | any | host ip-address} [icmpv6-type [icmpv6-code] |
msg icmpv6-msg] [dscp code] [traffic-class value] [flow-label value] [log |
log-verbose] [routing] [routing-type type] [mobility] [mobility-type type]
```

Parameters

protocol-num	Specifies an IP protocol for which to permit access. Valid values are protocol numbers from 0 - 255.
ipv6	Specifies any IPv6 protocol (0 - 255)
ah	Specifies the Authentication Header protocol
esp	Specifies the Encapsulation Security Payload protocol
gre	Specifies the Generic Router Encapsulation protocol
tcp	Specifies the Transmission Control Protocol
udp	Specifies the User Datagram Protocol
icmpv6	Specifies the IPv6 Internet Control Message Protocol
source-address/length	Specifies the source network address and length from which the packet will be sent.
dest-address/length	Specifies the destination network address and length (extended IPv6 access list only).
any	Specifies that any source or destination (extended IPv6 access list only) address applies to this rule entry.
host *ip-address*	Specifies a specific host address that will be applied to this rule entry.
icmpv6-type [*icmpv6-code*]	(Optional) Specifies an ICMPv6 message type, optionally followed by an ICMPv6 message code. Valid values for both ICMPv6 message type and message codes are **0** - **255**. See usage section for more information.
msg *icmpv6-msg*	(Optional) Specifies a single ICMPv6 message type by entering a keyword. Supported message type keywords are provided in Table 82-1 on page 82-8.
eq | **neq** | **gt** | **lt** {*source-port* | *dest-port*}	(Optional) Specifies that a source or destination port is permitted. The meaning of the keywords are: • **eq** - permits the specified source or destination port • **gt** - permits source or destination ports greater than the value specified • **lt** - permits source or destination ports less than the value specified • **neq** - permits source or destination ports that are not equal to the value specified
range *start-port end-port*	(Optional) Specifies a range of source or destination ports permitted.
established	(Optional) Specifies that only established TCP connections are permitted. A match is made if ACK or RST bits are set.

dscp *code*	(Optional) Specifies a DiffServe Code Point (DSCP) value to match against this packet's DSCP code. Valid values are **0** - **63**, or one of the following keywords: • **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **af44**, – Assured Forwarding • **be** – best effort • **cs1** - **cs7** – Class Selector • **ef** – Expedited Forwarding
traffic-class *value*	(Optional) Specifies a Type of Service (ToS) value. Valid values are **0** - **255**.
flow-label *value*	(Optional) Specifies a value that matches the flow label field value of the IPv6 packet header. Valid values are **0** to **1048575**.
log | **log-verbose**	Enables syslog or verbose syslog messaging for an access list rule hit.
routing	(Optional) Specifies that the routing extension header within each IPv6 packet header should be matched against the source-routed packet.
routing-type *type*	(Optional) Specifies the routing header type value that will be matched against the packet's routing extension header. Valid values are **0** - **255**.
mobility	(Optional) Specifies that the IPv6 packet will be matched against the mobility extension header within each IPv6 packet header.
mobility-type *type*	(Optional) Specifies the mobility header type to match against the mobility-type extension header within each IPv6 packet header. Valid values are **0** - **255**.

Defaults

If any optional parameter is not entered, no matching against that parameter is performed.

Mode

Standard or extended IPv6 access list configuration .

Usage

Entering any IPv6 protocol number will configure the permit entry for the specified protocol, but will limit configurable parameters to the list in the *protocol-num* syntax. Specifying the **tcp**, **udp**, or **icmpv6** keywords will provide the extended parameter set listed in the syntax for these keywords.

Access list logging is throttled to 1 log message per second. If there are multiple access list rules with logging enabled (log or log-verbose), and more then one frame is transmitted per second that can hit those rules, only the first frame will generate a message. Logging is sampling and does not report every time that a rule with logging enabled is hit.

If you did not turn on logging when creating a permit rule, you can turn on logging within the access list for a specific rule or all rules using the **log** command. See "log" on page 82-12 for command details.

When using the *icmpv6-type* [*icmpv6-code*] parameter syntax you must enter a numeric value. See the ICMPv6 parameters assignments page on the http://www.iana.org site for a complete listing of ICMPv6 message type and code numeric values, as well as the associated RFC. When using the **msg** *icmpv6-msg* parameter syntax, you must enter a single supported keyword to specify an ICMPv6 message type. Supported ICMPv6 message type keywords are listed in Table 82-1 on page 82-8. Supported ICMPv6 message type keywords also display when entering a **?** after the **msg** parameter.

Table 82-1 contains supported ICMP message types with message codes and descriptions.

Table 82-1 ICMP Message Types

Message Type Keyword	Message Code and Description
address-unreachable	(001,003) Address is unreachable, unspecified reason
admin-prohibited	(001,001) Administratively prohibited
bad-header-field	(004,000) Erroneous header field encountered
bad-ipv6-option	(004,002) Unrecognized IPv6 option encountered
bad-next-header-type	(004,001) Unrecognized Next Header type encountered
beyond-scope	(001,002) Beyond scope of source address
dest-unreachable	(001,000) No route to destination
echo-reply	(129,000) Echo reply
echo-request	(128,000) Echo request
home-agent-disc-req	(144,000) Home agent address discovery request
home-agent-disc-resp	(145,000) Home agent address discovery reply
inverse-nd-na	(142,000) Inverse neighbor-discovery advertisement
inverse-nd-ns	(141,000) Inverse neighbor-discovery solicitation
mld-done	(132,000) Multicast listener done
mld-report	(131,000) Multicast listener report
mld-query	(130,000) Multicast listener query
mobile-prefix-advert	(147,000) Mobile prefix advertisement
mobile-prefix-solicit	(146,000) Mobile prefix solicitation
nd-na	(135,000) Neighbor advertisement
nd-ns	(136,000) Neighbor solicitation
node-info-query-addrv4	(139,002) ICMP node information query for IPv4 address
node-info-query-addrv6	(139,000) ICMP node information query for IPv6 address
node-info-query-name	(139,001) ICMP node information query for name
node-info-resp-refused	(140,001) ICMP node information response refused
node-info-resp-success	(140,000) ICMP node information response succeeded
node-info-resp-unknown	(140,002) ICMP node information response Qtype unknown
packet-too-big	(002,000) Packet is too big
port-unreachable	(001,004) Specified port is not reachable
reassembly-timeout	(003,001) Fragment reassembly time exceeded
redirect-message	(137,000) Redirect Message
reject-route	(001,006) Route to destination rejected
router-advertisement	(134,000) Router advertisement
router-renumber-cmd	(138,000) Router renumbering command
router-renumber-result	(138,001) Router renumbering result

Table 82-1 ICMP Message Types (continued)

Message Type Keyword	Message Code and Description
router-renumber-reset	(138,255) Router renumbering sequence number reset
router-solicitation	(133,000) Router solicitation
src-addr-policy-fail	(001,005) Source addr failed ingress/egress policy
ttl-exceeded	(003,000) Time-to-live exceeded

Examples

This example enters configuration mode for standard IPv6 access list **acl2** and configures a permit entry for source address **2001:1234:50:0:21f:45ff:fe3d:21be/64**:

```
S Chassis(rw-config)->ipv6 access-list standard acl2
S Chassis(rw-cfg-ipv6-std-acl)->permit 2001:1234:50:0:21f:45ff:fe3d:21be/64
S Chassis(rw-cfg-ipv6-std-acl)->
```

This example enters configuration mode for extended IPv6 access list **acl120** and configures a permit entry for the IP protocol with a source address **2001:1234:50:0:21f:45ff:fe3d:21aa/64** and a destination address of any:

```
S Chassis(rw-config)->ipv6 access-list extended acl120
S Chassis(rw-cfg-ipv6-ext-acl)->permit ipv6 2001:1234:50:0:21f:45ff:fe3d:21aa/64
any
S Chassis(rw-cfg-ipv6-ext-acl)->
```

This example enters configuration mode for extended IPv6 access list **acl130** and configures a permit entry for the ICMP protocol with a source network address of **2001:1234:0:0:21f::50/64** and a destination address of 2001:2345:50:0:21f:45ff:fe3d:21ba/64 and a router discovery advertisement ICMP message type:

```
S Chassis(rw-config)->ipv6 access-list extended acl130
S Chassis(rw-cfg-ipv6-ext-acl)->permit icmpv6 2001:1234:0:0:21f::50/64
2001:2345:50:0:21f:45ff:fe3d:21ba/64 msg router-advertisement
S Chassis(rw-cfg-ipv6-ext-acl)->
```

deny

Use this command to create a deny IPv6 access list rule entry.

Syntax

Standard IPv6 Access List:

deny {*source-address/length* | **any** | **host** *ip-address*]} [**log** | **log-verbose**]

Extended IPv6 Access List:

deny {*protocol-num* | **ipv6** | **ah** | **esp** | **gre**} {*source-address/length* | **any** | **host** *ip-address*} {*destination-address/length* | **any** | **host** *ip-address*} [**dscp** *code*] [**traffic-class** *value*] [**flow-label** *value*] [**log** | **log-verbose**] [**routing**] [**routing-type** *type*] [**mobility**] [**mobility-type** *type*]

deny tcp {*source-address/length* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *source-port*] [**range** *start-port end-port*] {*destination-address/length* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *dest-port*] [**range** *start-port end-port*]

[**established**] [**dscp** *code*] [**traffic-class** *value*] [**flow-label** *value*] [**log** | **log-verbose**] [**routing**] [**routing-type** *type*] [**mobility**] [**mobility-type** *type*]

deny udp {*source-address/length* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *source-port*] [**range** *start-port end-port*] {*destination-address/length* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *dest-port*] [**range** *start-port end-port*] [**dscp** *code*] [**traffic-class** *value*] [**flow-label** *value*] [**log** | **log-verbose**] [**routing**] [**routing-type** *type*] [**mobility**] [**mobility-type** *type*]

deny icmpv6 {*source-address/length* | **any** | **host** *ip-address*} {*destination-address/length* | **any** | **host** *ip-address*} [*icmpv6-type* [*icmpv6-code*] | **msg** *icmpv6-msg*] [**dscp** *code*] [**traffic-class** *value*] [**flow-label** *value*] [**log** | **log-verbose**] [**routing**] [**routing-type** *type*] [**mobility**] [**mobility-type** *type*]

Parameters

protocol-num	Specifies an IP protocol for which to deny access. Valid values are protocol numbers from 0 - 255.
ipv6	Specifies any IPv6 protocol (0 - 255).
ah	Specifies the Authentication Header protocol.
esp	Specifies the Encapsulation Security Payload protocol.
gre	Specifies the Generic Router Encapsulation protocol.
tcp	Specifies the Transmission Control Protocol.
udp	Specifies the User Datagram Protocol.
icmpv6	Specifies the IPv6 Internet Control Message Protocol.
source-address/length	Specifies the source network address and length from which the packet will be sent.
dest-address/length	Specifies the destination network address and length (extended IPv6 access list only).
any	Specifies that any source or destination (extended IPv6 access list only) address applies to this rule entry.
host *ip-address*	Specifies a specific host address that will be applied to this rule entry.
icmpv6-type [*icmpv6-code*]	(Optional) Specifies an ICMPv6 message type, optionally followed by an ICMPv6 message code. Valid values for both ICMPv6 message type and message codes are **0** - **255**. See usage section for more information.
msg *icmpv6-msg*	(Optional) Specifies an ICMPv6 type by entering a keyword. Supported values are provided in Table 82-1 on page 82-8.
eq | **neq** | **gt** | **lt** {*source-port* | *dest-port*}	(Optional) Specifies that a source or destination port is denied. The meaning of the keywords are: • **eq** – Denies the specified source or destination port • **gt** – Denies source or destination ports greater than the value specified • **lt** – Denies source or destination ports less than the value specified • **neq** – Denies source or destination ports that are not equal to the value specified
range *start-port end-port*	(Optional) Specifies a range of source or destination ports denied.
established	(Optional) Specifies that only established TCP connections are denied. A match is made if ACK or RST bits are set.

dscp *code*	(Optional) Specifies a DiffServe Code Point (DSCP) value to match against this packet's DSCP code. Valid values are **0** - **63**, or one of the following keywords: • **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **af44**, – Assured Forwarding • **be** – best effort • **cs1** – **cs7** – Class Selector • **ef** – Expedited Forwarding
traffic-class *value*	(Optional) Specifies a Type of Service (ToS) value. Valid values are **0** - **255**.
flow-label *value*	(Optional) Specifies a value that matches the flow label field value of the IPv6 packet header. Valid values are **0** to **1048575**.
log | **log-verbose**	Enables syslog or verbose syslog messaging for an access list rule hit.
routing	(Optional) Specifies that the routing extension header within each IPv6 packet header should be matched against the source-routed packet.
routing-type *type*	(Optional) Specifies the routing header type value that will be matched against the packet's routing extension header. Valid values are **0** - **255**.
mobility	(Optional) Specifies that the IPv6 packet will be matched against the mobility extension header within each IPv6 packet header.
mobility-type *type*	(Optional) Specifies the mobility header type to match against the mobility-type extension header within each IPv6 packet header. Valid values are **0** - **255**.

Defaults

If any optional parameter is not entered, no matching against that parameter is performed.

Mode

Standard or extended IPv6 access list configuration .

Usage

Entering any IPv6 protocol number will configure the deny entry for the specified protocol, but will limit configurable parameters to the list in the *protocol-num* syntax. Specifying the **tcp**, **udp**, or **icmpv6** keywords will provide the extended parameter set listed in the syntax for these keywords.

Access list logging is throttled to 1 log message per second. If there are multiple access list rules with logging enabled (log or log-verbose), and more then one frame is transmitted per second that can hit those rules, only the first frame will generate a message. Logging is sampling and does not report every time that a rule with logging enabled is hit.

If you did not turn on logging when creating a deny rule, you can turn on logging within the access list for a specific rule or all rules using the **log** command. See "log" on page 82-12 for command details.

When using the *icmpv6-type* [*icmpv6-code*] parameter syntax you must enter a numeric value. See the ICMPv6 parameters assignments page on the http://www.iana.org site for a complete listing of ICMPv6 message type and code numeric values, as well as the associated RFC. When using the **msg** *icmpv6-msg* parameter syntax, you must enter a single supported keyword to specify an ICMPv6 message type. Supported ICMPv6 message type keywords are listed in Table 82-1 on

page 82-8. Supported ICMPv6 message type keywords also display when entering a **?** after the **msg** parameter.

Examples

This example enters configuration mode for standard IPv6 access list **acl2** and configures a deny entry for source address **fe80:0:0:0:21f:45ff:fe3d:21be/64**:

```
S Chassis(rw-config)->ipv6 access-list standard acl2
S Chassis(rw-cfg-ipv6-std-acl)->deny fe80:0:0:0:21f:45ff:fe3d:21be/64
S Chassis(rw-cfg-ipv6-std-acl)->
```

This example enters configuration mode for extended IPv6 access list **acl120** and configures a deny entry for the IP protocol with a source address **fe80:0:0:0:21f:45ff:fe3d:21aa/64** and a destination address of any:

```
S Chassis(rw-config)->ipv6 access-list extended acl120
S Chassis(rw-cfg-ipv6-ext-acl)->deny ipv6 fe80:0:0:0:21f:45ff:fe3d:21aa/64 any
S Chassis(rw-cfg-ipv6-ext-acl)->
```

log

Use this command to enable a standard or detailed logging IPv6 access list rule entry.

Syntax

log {*entry* | **implicit_permit_nd-na** | **implicit_permit_nd-ns** | **implicit_deny** | **all**}

Parameters

entry	Specifies a sequence numbered entry to log when a hit occurs. Valid values: **1** - **5000**. Default value: **all**
implicit_permit_nd-na	Specifies the logging of a neighbor advertisement hit.
implicit_permit_nd-ns	Specifies the logging of a neighbor solicitation hit.
implicit_deny	Specifies the logging of an implicit deny rule hit.
all	Specifies that all hits are to be logged, including the final implicit deny.

Defaults

None.

Mode

Standard or extended IPv6 access list configuration .

Usage

You can also turn on logging for each access list permit or deny rule when you configure the access list entry, using either the **log** or **log-verbose** parameters. When turning on logging within an access list rule configuration, all hits for that rule will be logged. The **log** command allows for turning on logging after a rule has been configured. The logging behavior is based upon the entry or keyword specified. If logging is already turned on for a permit or deny rule, The **log** command access list entry for that rule is redundant.

Access list logging is throttled to 1 log message per second. If there are multiple access list rules with logging enabled (log or log-verbose), and more then one frame is transmitted per second that can hit those rules, only the first frame will generate a message. Logging is sampling and does not report every time that a rule with logging enabled is hit.

Example

This example enters configuration mode for standard IPv6 access list **acl2** and enables standard logging for a final implicit deny hit:

```
S Chassis(rw-config)->ipv6 access-list standard acl2
S Chassis(rw-cfg-ipv6-std-acl)->log implicit_deny
S Chassis(rw-cfg-ipv6-std-acl)->
```

delete

Use this command to delete a pre-existing IPv6 access list rule entry or range of entries.

Syntax

delete {*entry* | **from** *entry* **to** *entry*}

Parameters

entry | **from** *entry* **to** *entry*]	(Optional) Specifies an entry or range of entries to delete. When deleting a range of entries, **from** specifies the beginning of the range, and **to** specifies the end of the range inclusive. An entry is a valid pre-existing IPv6 access list rule from **1** to **5000**.

Defaults

None.

Mode

Standard or extended IPv6 access list configuration .

Examples

This example enters configuration mode for standard IPv6 access list **acl2** and deletes rule entry **20**:

```
S Chassis(rw-config)->ipv6 access-list standard acl2
S Chassis(rw-cfg-ipv6-std-acl)->delete 20
S Chassis(rw-cfg-ipv6-std-acl)->
```

This example enters configuration mode for standard IPv6 access list **acl2** and deletes rule entry **10** - **12**:

```
S Chassis(rw-config)->ipv6 access-list standard acl2
S Chassis(rw-cfg-ipv6-std-acl)->delete from 10 to 12
S Chassis(rw-cfg-ipv6-std-acl)->
```

insert before

Use this command to insert an IPv6 access list rule entry.

Syntax

Standard IP Access List:

insert before *entry* {**remark** *text* | {**permit** | **deny**}} {*source-address/length* | **any** | **host** *ip-address*]} [**log** | **log-verbose**]

Extended IP Access List:

insert before *entry* {**remark "text"** | {**permit** | **deny**}} {*protocol-num* | **ipv6** | **ah** | **esp** | **gre**} {*source-address/length* | **any** | **host** *ip-address*} {*destination-address/length* | **any** | **host** *ip-address*} [**dscp** *code*] [**traffic-class** *value*] [**flow-label** *value*] [**log** | **log-verbose**] [**routing**] [**routing-type** *type*] [**mobility**] [**mobility-type** *type*]

insert before *entry* {**remark "***text***"** | {**permit** | **deny**}} **tcp** {*source-address/length* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *source-port*] [**range** *start-port end-port*] {*destination-address/length* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *dest-port*] [**range** *start-port end-port*] [**established**] [**dscp** *code*] [**traffic-class** *value*] [**flow-label** *value*] [**log** | **log-verbose**] [**routing**] [**routing-type** *type*] [**mobility**] [**mobility-type** *type*]

insert before *entry* {**remark "text"** | {**permit** | **deny**}} **udp** {*source-address/length* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *source-port*] [**range** *start-port end-port*] {*destination-address/length* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *dest-port*] [**range** *start-port end-port*] [**dscp** *code*] [**traffic-class** *value*] [**flow-label** *value*] [**log** | **log-verbose**] [**routing**] [**routing-type** *type*] [**mobility**] [**mobility-type** *type*]

insert before *entry* {**remark "text"** | {**permit** | **deny**}} **icmpv6** {*source-address/length* | **any** | **host** *ip-address*} {*destination-address/length* | **any** | **host** *ip-address*} [*icmpv6-type* [*icmpv6-code*] | **msg** *icmpv6-msg*] [**dscp** *code*] [**traffic-class** *value*] [**flow-label** *value*] [**log** | **log-verbose**] [**routing**] [**routing-type** *type*] [**mobility**] [**mobility-type** *type*]

Parameters

entry	Specifies an entry to place the inserted rule before. An entry is a valid pre-existing IPv6 access list rule or the explicit deny which is the default entry **1**.
remark *text*	Specify a text remark that will be associated with this access list. Valid values: Up to 64 characters in quotes.
deny | **permit**	Denies or permits access if specified conditions are met.
protocol-num	Specifies an IP protocol for which to permit or deny access. Valid values are protocol numbers from 0 - 255.
ipv6	Specifies any IPv6 protocol (0 - 255).
ah	Specifies the Authentication Header protocol.
esp	Specifies the Encapsulation Security Payload protocol.
gre	Specifies the Generic Router Encapsulation protocol.
tcp	Specifies the Transmission Control Protocol.
udp	Specifies the User Datagram Protocol.
icmpv6	Specifies the IPv6 Internet Control Message Protocol.

source-address/length	Specifies the source network address and length from which the packet will be sent.
dest-address/length	Specifies the destination network address and length (extended IPv6 access list only).
any	Specifies that any source or destination (extended IPv6 access list only) address applies to this rule entry.
host *ip-address*	Specifies a specific host address that will be applied to this rule entry.
icmpv6-type [*icmpv6-code*]	(Optional) Specifies an ICMPv6 message type, optionally followed by an ICMPv6 message code. Valid values for both ICMPv6 message type and message codes are **0** - **255**. See usage section for more information.
msg *icmpv6-msg*	(Optional) Specifies an ICMPv6 type by entering a keyword. Supported values are provided in Table 82-1 on page 82-8.
eq | **neq** | **gt** | **lt** {*source-port* | *dest-port*}	(Optional) Specifies that a source or destination port is permitted or denied. The meaning of the keywords are: • **eq** - permits or denies the specified source or destination port • **gt** - permits or denies source or destination ports greater than the value specified • **lt** - permits or denies source or destination ports less than the value specified • **neq** - permits or denies source or destination ports that are not equal to the value specified
range *start-port end-port*	(Optional) Specifies a range of source or destination ports permitted or denied.
established	(Optional) Specifies that only established TCP connections are permitted or denied. A match is made if ACK or RST bits are set.
dscp *code*	(Optional) Specifies a DiffServe Code Point (DSCP) value to match against this packet's DSCP code. Valid values are **0** - **63**, or one of the following keywords: • **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **af44**, – Assured Forwarding • **be** – best effort • **cs1** - **cs7** – Class Selector • **ef** – Expedited Forwarding
traffic-class *value*	(Optional) Specifies a Type of Service (ToS) value. Valid values are **0** - **255**.
flow-label *value*	(Optional) Specifies a value that matches the flow label field value of the IPv6 packet header. Valid values are **0** to **1048575**.
log | **log-verbose**	Enables syslog or verbose syslog messaging for an access list rule hit.
routing	(Optional) Specifies that the routing extension header within each IPv6 packet header should be matched against the source-routed packet.
routing-type *type*	(Optional) Specifies the routing header type value that will be matched against the packet's routing extension header. Valid values are **0** - **255**.
mobility	(Optional) Specifies that the IPv6 packet will be matched against the mobility extension header within each IPv6 packet header.

mobility-type *type*	(Optional) Specifies the mobility header type to match against the mobility-type extension header within each IPv6 packet header. Valid values are **0** - **255**.

Defaults

If any optional parameter is not entered, no matching against that parameter is performed.

Mode

Standard or extended IPv6 access list configuration .

Usage

Entering any IPv6 protocol number will configure the permit or deny entry for the specified protocol, but will limit configurable parameters to the list in the *protocol-num* syntax. Specifying the **tcp**, **udp**, or **icmpv6** keywords will provide the extended parameter set listed in the syntax for these keywords.

Access list logging is throttled to 1 log message per second. If there are multiple access list rules with logging enabled (log or log-verbose), and more then one frame is transmitted per second that can hit those rules, only the first frame will generate a message. Logging is sampling and does not report every time that a rule with logging enabled is hit.

If you did not turn on logging when creating a permit or deny rule, you can turn on logging within the access list for a specific rule or all rules using the **log** command. See "log" on page 82-12 for command details.

When using the *icmpv6-type* [*icmpv6-code*] parameter syntax you must enter a numeric value. See the ICMPv6 parameters assignments page on the http://www.iana.org site for a complete listing of ICMPv6 message type and code numeric values, as well as the associated RFC. When using the **msg** *icmpv6-msg* parameter syntax, you must enter a single supported keyword to specify an ICMPv6 message type. Supported ICMPv6 message type keywords are listed in Table 82-1 on page 82-8. Supported ICMPv6 message type keywords also display when entering a **?** after the **msg** parameter.

Examples

This example enters configuration mode for extended IPv6 access list **acl10** and inserts a rule before entry **10** that permits packets with a source address for host **2002:100::50** and a destination address of **2001:100::100:25/64** with a ToS value of **6**:

```
S Chassis(rw-config)->ipv6 access-list standard acl10
S Chassis(rw-cfg-ipv6-ext-acl)->insert before 10 permit host 2002:100::50
2001:100::100:25/64 traffic-class 6
S Chassis(rw-cfg-ipv6-ext-acl)->
```

name

Use this command to display the name of the access list for this configuration context.

Syntax

```
name
```

Parameters

None.

Defaults

None.

Mode

Configuration command, standard or extended IPv6 access list configuration .

Example

This example enters configuration mode for standard IPv6 access list **ipv6list1** and displays the name of this access list:

```
S Chassis(su-config)->ipv6 access-list standard  ipv6list1
S Chassis(su-cfg-ipv6-std-acl)->name
Configuring access list:  ipv6list1.
S Chassis(su-cfg-ipv6-std-acl)->
```

replace

Use this command to replace an IPv6 access list entry with a remark, permit or deny entry.

Syntax

Standard IP Access List:

replace *entry* {**remark** *text* | {**permit** | **deny**}} {*source-address/length* | **any** | **host** *ip-address*]} [**log** | **log-verbose**]

Extended IP Access List:

replace *entry* {**remark** "**text**" | {**permit** | **deny**}} {*protocol-num* | **ipv6** | **ah** | **esp** | **gre**} {*source-address/length* | **any** | **host** *ip-address*} {*destination-address/length* | **any** | **host** *ip-address*} [**dscp** *code*] [**traffic-class** *value*] [**flow-label** *value*] [**log** | **log-verbose**] [**routing**] [**routing-type** *type*] [**mobility**] [**mobility-type** *type*]

replace *entry* {**remark** "*text*" | {**permit** | **deny**}} **tcp** {*source-address/length* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *source-port*] [**range** *start-port end-port*] {*destination-address/length* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *dest-port*] [**range** *start-port end-port*] [**established**] [**dscp** *code*] [**traffic-class** *value*] [**flow-label** *value*] [**log** | **log-verbose**] [**routing**] [**routing-type** *type*] [**mobility**] [**mobility-type** *type*]

replace *entry* {**remark** "**text**" | {**permit** | **deny**}} **udp** {*source-address/length* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *source-port*] [**range** *start-port end-port*] {*destination-address/length* | **any** | **host** *ip-address*} [{**eq** | **neq** | **gt** | **lt**} *dest-port*] [**range** *start-port end-port*] [**dscp** *code*] [**traffic-class** *value*] [**flow-label** *value*] [**log** | **log-verbose**] [**routing**] [**routing-type** *type*] [**mobility**] [**mobility-type** *type*]

replace *entry* {**remark** "**text**" | {**permit** | **deny**}} **icmpv6** {*source-address/length* | **any** | **host** *ip-address*} {*destination-address/length* | **any** | **host** *ip-address*} [*icmpv6-type* [*icmpv6-code*] | **msg** *icmpv6-msg*] [**dscp** *code*] [**traffic-class** *value*] [**flow-label** *value*] [**log** | **log-verbose**] [**routing**] [**routing-type** *type*] [**mobility**] [**mobility-type** *type*]

Parameters

entry	Specifies an entry to replace with the entry configured in this command. An entry is a valid pre-existing IPv6 access list rule or the explicit deny which is the default entry **1**.

remark *text*	Specify a text remark that will be associated with this access list. Valid values: Up to 64 characters in quotes.
deny | **permit**	Denies or permits access if specified conditions are met.
protocol-num	Specifies an IP protocol for which to permit or deny access. Valid values are protocol numbers from 0 - 255.
ipv6	Specifies any IPv6 protocol (0 - 255).
ah	Specifies the Authentication Header protocol.
esp	Specifies the Encapsulation Security Payload protocol.
gre	Specifies the Generic Router Encapsulation protocol.
tcp	Specifies the Transmission Control Protocol.
udp	Specifies the User Datagram Protocol.
icmpv6	Specifies the IPv6 Internet Control Message Protocol.
source-address/length	Specifies the source network address and length from which the packet will be sent.
dest-address/length	Specifies the destination network address and length (extended IPv6 access list only).
any	Specifies that any source or destination (extended IPv6 access list only) address applies to this rule entry.
host *ip-address*	Specifies a specific host address that will be applied to this rule entry.
icmpv6-type [*icmpv6-code*]	(Optional) Specifies an ICMPv6 message type, optionally followed by an ICMPv6 message code. Valid values for both ICMPv6 message type and message codes are **0** - **255**. See usage section for more information.
msg *icmpv6-msg*	(Optional) Specifies an ICMPv6 type by entering a keyword. Supported values are provided in Table 82-1 on page 82-8.
eq | **neq** | **gt** | **lt** {*source-port* | *dest-port*}	(Optional) Specifies that a source or destination port is permitted or denied. The meaning of the keywords are: • **eq** - permits or denies the specified source or destination port • **gt** - permits or denies source or destination ports greater than the value specified • **lt** - permits or denies source or destination ports less than the value specified • **neq** - permits or denies source or destination ports that are not equal to the value specified
range *start-port end-port*	(Optional) Specifies a range of source or destination ports permitted or denied.
established	(Optional) Specifies that only established TCP connections are permitted or denied. A match is made if ACK or RST bits are set.

dscp *code*	(Optional) Specifies a DiffServe Code Point (DSCP) value to match against this packet's DSCP code. Valid values are **0** - **63**, or one of the following keywords: • **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **af44**, – Assured Forwarding • **be** – best effort • **cs1** - **cs7** – Class Selector • **ef** – Expedited Forwarding
traffic-class *value*	(Optional) Specifies a Type of Service (ToS) value. Valid values are **0** - **255**.
flow-label *value*	(Optional) Specifies a value that matches the flow label field value of the IPv6 packet header. Valid values are **0** to **1048575**.
log | **log-verbose**	Enables syslog or verbose syslog messaging for an access list rule hit.
routing	(Optional) Specifies that the routing extension header within each IPv6 packet header should be matched against the source-routed packet.
routing-type *type*	(Optional) Specifies the routing header type value that will be matched against the packet's routing extension header. Valid values are **0** - **255**.
mobility	(Optional) Specifies that the IPv6 packet will be matched against the mobility extension header within each IPv6 packet header.
mobility-type *type*	(Optional) Specifies the mobility header type to match against the mobility-type extension header within each IPv6 packet header. Valid values are **0** - **255**.

Defaults

If any optional parameter is not entered, no matching against that parameter is performed.

Mode

Standard or extended IPv6 access list configuration .

Usage

Entering any IPv6 protocol number will configure the permit or deny entry for the specified protocol, but will limit configurable parameters to the list in the *protocol-num* syntax. Specifying the **tcp**, **udp**, or **icmpv6** keywords will provide the extended parameter set listed in the syntax for these keywords.

Access list logging is throttled to 1 log message per second. If there are multiple access list rules with logging enabled (log or log-verbose), and more then one frame is transmitted per second that can hit those rules, only the first frame will generate a message. Logging is sampling and does not report every time that a rule with logging enabled is hit.

If you did not turn on logging when creating a permit or deny rule, you can turn on logging within the access list for a specific rule or all rules using the **log** command. See "log" on page 82-12 for command details.

When using the *icmpv6-type* [*icmpv6-code*] parameter syntax you must enter a numeric value. See the ICMPv6 parameters assignments page on the http://www.iana.org site for a complete listing of ICMPv6 message type and code numeric values, as well as the associated RFC. When using the **msg** *icmpv6-msg* parameter syntax, you must enter a single supported keyword to specify an ICMPv6 message type. Supported ICMPv6 message type keywords are listed in Table 82-1 on

page 82-8. Supported ICMPv6 message type keywords also display when entering a **?** after the **msg** parameter.

Example

This example replaces entry **1** of IPv6 access list **acl10** with a permit any source address :

```
S Chassis(rw-config)->ipv6 access-list standard acl10
S Chassis(rw-cfg-ipv6-std-acl)->replace 1 permit any
S Chassis(rw-cfg-ipv6-std-acl)->
```

move before

Use this command to move a pre-existing IPv6 access list rule entry or range to the specified location in the IPv6 access list.

Syntax

move before *entry1* **from** *entry2* **to** *entry3*

Parameters

entry1	Specifies the entry for which the specified range of entries will be moved before.
entry2	Specifies the beginning entry for the range of entries to be moved.
entry3	Specifies the last entry for the range of entries to be moved.

Defaults

None.

Mode

Standard or extended IPv6 access list configuration .

Examples

This example enters configuration mode for standard IPv6 access list **acl2** and moves rule entry **20** before rule entry **10**:

```
S Chassis(rw-config)->ipv6 access-list standard acl2
S Chassis(rw-cfg-ipv6-std-acl)->move before 10 from 20 to 20
S Chassis(rw-cfg-ipv6-std-acl)->
```

This example enters configuration mode for standard IPv6 access list **acl2** and moves rule entries **10** - **12** before rule entry **5**:

```
S Chassis(rw-config)->ipv6 access-list standard acl2
S Chassis(rw-cfg-ipv6-std-acl)->move before 5 from 10 to 12
S Chassis(rw-cfg-ipv6-std-acl)->
```

remark

Use this command to enter a text comment into the IPv6 access list as the next entry.

Syntax

remark "*text*"

Parameters

text	Specifies the text to be entered as the next IPv6 access list entry

Defaults

None.

Mode

Configuration command, standard or extended IPv6 access list configuration .

Usage

All text strings with spaces must be within double quotes.

Use the move before command on page 82-20 to change a remark entry location.

Example

This example enters configuration mode for standard IPv6 access list **acl10** and enters a remark specifying that the following entry permits any source address for this IPv6 access list. The remark entry is followed by the permit any entry:

```
S Chassis(rw-cfg-ipv6-std-acl)->show access-lists acl10
Standard IP access list acl10  (1 entries)
  -- implicit deny all --
S Chassis(rw-cfg-ipv6-std-acl)->remark "The following entry permits any source
address."
S Chassis(rw-cfg-ipv6-std-acl)->permit any
S Chassis(rw-cfg-ipv6-std-acl)->show access-lists acl10
Standard IP access list acl10  (3 entries)
  1 "The following entry permits any source address."
  2 permit any
  -- implicit deny all --
S Chassis(rw-cfg-ipv6-std-acl)->
```

Displaying and Applying Access Control List Commands

This section details access list commands used to display access list configuration and counters, clear access list counters, and apply access lists to an interface. The commands used to display and apply access list entries are:

For information about...	Refer to page...
ipv6 access-group	82-22

For information about...	Refer to page...
ipv6 host-access	82-23
show access-lists	82-23
show access-lists applied	82-24
clear access-lists counters	82-25

ipv6 access-group

Use this command to apply access restrictions to inbound or outbound frames on an interface when operating in router mode.

Syntax

ipv6 access-group *name* {**in** | **out**} [**all-traffic** | **routed-traffic**]

no ipv6 access-group *name* {**in** | **out**} [**all-traffic** | **routed-traffic**]

Parameters

name	Specifies the name of the IPv6 access list to be applied to the interface.
in	Filters inbound frames.
out	Filters outbound frames.
all-traffic	(Optional) Specifies that the assigned ACL is applied to all traffic on the interface, not just the routed traffic.
routed-traffic	(Optional) Specifies that the assigned ACL is applied only to the routed traffic on the interface. (Default)

Defaults

None.

Mode

Interface configuration**.**

Usage

Access lists must be applied per routing interface. An entry (rule) can either be applied to inbound or outbound frames. An access list can be applied before it is created. The uncreated applied access list will have no affect.

By default, an IPv6 ACL is only applied to routed traffic. To apply the IPv6 ACL to all traffic, use the **all-traffic** option.

The **no ipv6 access-group** command removes the specified access list from this interface.

Example

This example shows how to apply the standard access list **acl10** for all inbound frames on VLAN **50**. Based upon the definition of access list **acl10**, only frames with source

fe80:0:0:0:21f:45ff:fe3d:21aa/64 are routed. All the frames with other sources received on VLAN **50** are dropped:

```
S Chassis(su-config)->ipv6 access-list standard acl10
S Chassis(su-cfg-ipv6-std-acl)->permit fe80:0:0:0:21f:45ff:fe3d:21aa/64 log
S Chassis(su-cfg-ipv6-std-acl)->exit
S Chassis(su-config)->interface vlan 50
S Chassis(su-config-intf-vlan.0.50)->ipv6 access-group acl10 in
S Chassis(su-config-intf-vlan.0.50)->
```

ipv6 host-access

Use this command to apply access restrictions to host services.

Syntax

ip host-access *name*

no ip host-access *name*

Parameters

name	Specifies the name of the access list.

Defaults

None.

Mode

Configuration command.

Usage

The **no ipv6 host-access** command removes the specified host services access list.

Example

This example shows how to apply access list host1 to host services for this device:

```
S Chassis(rw-config)->ipv6 host-access host1
S Chassis(rw-config)->
```

show access-lists

Use this command to display configured IP access list configurations.

Syntax

show access-lists [*name*] [**from** *start-range* **to** *end-range*]] [**brief**]

Parameters

name	(Optional) Displays access list information for a specific access list name.

from *start-range* **to** *end-range*	(Optional) Specifies a sequential range of access list rules to display for the specified access list.
brief	(Optional) Displays a summary version of the specified context.

Defaults

If an option is not specified, the entire table of access lists will be displayed.

Mode

All command modes.

Examples

This example shows how to display IPv6 access list number acl10. This is an extended access list, which permits or denies ICMP, UDP and IP frames based on restrictions configured with one of the IPv6 access list commands:

```
S Chassis(rw-config)->show access-lists acl10
Standard IPv6 access list acl10  (5 entries)
  1 permit fe80::/64  log
  2 permit a6ac::/32
  -- implicit permit nd-na --
  -- implicit permit nd-ns --
  -- implicit deny all --
```

This example shows how to display the brief form of IPv6 access lists for this system:

```
S Chassis(rw-config)->show access-lists brief

IPv6 Access List (last 49 chars)                 Type Ents Deny count
------------------------------------------------ ---- ---- --------------------
acl10                                            std     5 0
```

show access-lists applied

Use this command to display configured IP or IPv6 access lists.

Syntax

show access-lists applied [**host** | **interfaces** [**vlan** | **inbound** | **outbound** | **in-and-out**]]

Parameters

host	(Optional) Displays access list information for all applied ingress to host services.
interfaces	(Optional) Displays access list information for all applied access list interface types or the specified interface type.
vlan	(Optional) Displays access list information for VLAN interfaces.
inbound	(Optional) Displays access list information for inbound interfaces.
outbound	(Optional) Displays access list information for outbound interfaces.

in-and-out	(Optional) Displays access list information for both inbound and outbound interfaces.

Defaults

If an option is not specified, the entire table of applied access lists will be displayed.

Mode

All command modes.

Usage

Access list names may be up to 64 characters in length, but there is only room to display 32 characters (show applied) or 49 characters (show brief) on a single 80-character line. Names up to and including the maximum length will be displayed in their entirety. Names longer than the maximum display length will be displayed with an asterisk character followed by the last 31 or 48 characters of the name.

** unconfigured ** means that the access list applied to the interface or host has not yet been created. This is allowed, but the applied access list will have no effect on traffic, since the access list doesn't really exist yet.

Example

This example shows how to display applied IP access lists for this system. :

```
S4 Chassis(rw-config)->show access-lists applied
Interface   IPv6 Access List (last 32 chars) Dir  Type Ents Deny count
----------- -------------------------------- ---- ---- ---- --------------------
vlan.0.50   acl10                            in   std     5 0
S Chassis(rw-config)->
```

clear access-lists counters

Use this command to clear access list display counters.

Syntax

clear access-lists counters [*name* | **applied** [**host** | **interfaces** [**vlan** *vlan-id*] [**inbound** | **outbound** | **in-and-out**]]

Parameters

name	(Optional) Clears display counters for the specified access list name.
applied host | **interfaces**	(Optional) Clears display counters for applied host or interface statistics only.
vlan *vlan-id*	(Optional) Clears display counters for the specified VLAN.
inbound | **outbound** | **in-and-out**	Clears only only inbound, only outbound, or both inbound and outbound counters.

Defaults

If no option is specified, the clear action is applied to all access lists.

Mode

All command modes.

Example

This example clears the display counters for access list **acl10**:

```
S Chassis(rw-config)->clear access-lists counters acl10
S Chassis(rw-config)->
```

83

Layer 2 Access Control List Commands

This chapter describes the Layer 2 Access Control List (L2 ACL) set of commands and how to use them. For information about configuring L2 ACLs, refer to the "Access Control List Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
Named Layer 2 Access Control Lists	83-1
Access Control List Entry Configuration Commands	83-4
Displaying and Applying Access Control List Commands	83-15

Named Layer 2 Access Control Lists

This section details L2 ACL commands used to create, copy, append and check named L2 ACLs. The commands used to configure named ACLs are:

For information about...	Refer to page...
l2 access-list	83-1
l2 access-list copy to	83-2
l2 access-list append to	83-3
l2 access-list check	83-3

l2 access-list

Use this command to enter access list configuration mode for a L2 ACL.

Syntax

l2 access-list *name*

no l2 access-list *name*

Parameters

name	Specifies a L2 ACL name.

Defaults

None.

Mode

Configuration command, Global configuration**.**

Usage

The **l2 access-list** command enters the rule configuration command mode for the specified L2 ACL.

A L2 ACL MIB is not supported.

L2 ACL names must start with an alpha character. A name may be quoted, as the quotes are stripped, but spaces are not supported within the quoted string. A name cannot be one of the **show access-lists** keywords **brief** or **applied**, or any prefix thereof such as **?br?** or **?app?**. Names can be up to 64 characters in length.

Restrictions defined by an access list are applied by using the **l2 access-group** command ("l2 access-group" on page 83-16).

Note: An "implicit deny" is hard coded at the end of all ACLs. The implicit deny blocks anything not explicitly permitted within the ACL, including routing protocols and management connections.

The "no" form of this command removes the specified access list.

Example

This example creates the layer 2 access list list1, if it does not already exist, and enters layer 2 access list list1 configuration mode:

```
S Chassis(rw-config)->l2 access-list list1
S Chassis(rw-cfg-l2-acl-list1)->
```

l2 access-list copy to

Use this command to copy a pre-existing L2 ACL to a new L2 ACL.

Syntax

l2 access-list *name* **copy to** *name*

Parameters

name	Specifies a layer 2 access list name.

Defaults

None.

Mode

Configuration command, Global configuration**.**

Usage

When copying a L2 ACL, the L2 ACL to copy must already exist. When copying a L2 ACL, the access list the original is being copied to must not already exist.

L2 ACL names can be up to 64 characters in length.

Example

This example creates layer 2 access list **list2** and copys the layer 2 access list **list1** to it:

```
S Chassis(rw-config)->l2 access-list list1 copy to list2
S Chassis(rw-config)->
```

l2 access-list append to

Use this command to append the specified L2 ACL to another L2 ACL.

Syntax

l2 access-list *name* **append to** *name*

Parameters

name	Specifies a L2 ACL name to append to the append to named L2 ACL.
append to *name*	Specifies the L2 ACL the first named L2 ACL is appended to.

Defaults

None.

Mode

Configuration command, Global configuration**.**

Usage

When appending a L2 ACL, both the L2 ACL to append and the L2 ACL to append to must already exist.

Example

This example appends L2 ACL list1 to a pre-existing L2 ACL list3:

```
S Chassis(rw-config)->l2 access-list list1 append to list3
S Chassis(rw-config)->
```

l2 access-list check

Use this command to check the efficiency of a layer 2 access list.

Syntax

l2 access-list *name* **check**

Parameters

name	Specifies layer 2 access list name.

Defaults

None.

Mode

Configuration command, Global configuration.

Usage

This command checks the efficiency of the specified layer 2 access-list by determining if any rules are hidden by preceding rules.

Example

This example checks the efficiency of layer 2 access list list1:

```
S Chassis(rw-config)->l2 access-list list1 check
access-list list1 is efficient -- no rules are hidden by preceding rules.
S Chassis(rw-config)->
```

Access Control List Entry Configuration Commands

This section details L2 ACL commands used to configure deny or permit L2 ACL entries, log, delete, insert, replace, or move a L2 ACL entry, or create a L2 ACL comment entry. The commands used to configure named L2 ACL entries are:

For information about...	Refer to page...
permit	83-4
deny	83-6
log	83-8
delete	83-10
insert before	83-10
replace	83-12
move before	83-14
remark	83-15

permit

Use this command to create a permit layer 2 access list rule entry.

Syntax

permit {**any** | **host** *source-macAddr* | *source-macAddr source-wildcard*} [**any** | **host** *destination-macAddr* | *destination-macAddr destination-wildcard*] [**dei**] [**cos** *cos*] [vlan vlan [*vidhi*]] [ethertype data] [**log** | **log-verbose**]

no permit {**any** | **host** *source-macAddr* | *source-macAddr source-wildcard*} [**any** | **host** *destination-macAddr* | *destination-macAddr destination-wildcard*] [**dei**] [**cos** *cos*] [vlan vlan [*vidhi*]] [ethertype data] [**log** | **log-verbose**]

Parameters

any	Specifies that any source MAC address and optionally any destination MAC address is applied to this permit rule entry.

host *source-macAddr*	Specifies a host source MAC address in the formats x:x:x:x:x:x or H.H.H to apply to this permit rule entry.
source-macAddr source-wildcard	Specifies a source MAC address and mask to apply to this permit rule entry, in the formats x:x:x:x:x:x or H.H.H.
host *destination-macAddr*	(Optional) Sepcifies a host destination MAC address in the formats x:x:x:x:x:x or H.H.H to apply to this permit rule entry.
destination-macAddr destination-wildcard	(Optional) Specifies a destination MAC address and mask to apply to this permit rule entry, in the formats x:x:x:x:x:x or H.H.H.
dei	(Optional) Specifies that the drop eligibility indicator in the VLAN tag is applied to this permit rule entry.
cos *cos*	(Optional) Specifies that the indicated class of service value is applied to this permit rule entry.
vlan *vlan*	(Optional) Specifies that the indicated VLAN identifier in the VLAN tag is applied to this permit rule entry or specifies the low end of a range of VLANs to apply to this permit rule entry.
vidhi	(Optional) Specifies the high end of a range of VLAN identifiers in the VLAN tag to apply to this permit rule entry
ethertype *data*	(Optional) Specifies that the indicated Ethernet II type (0x0 - 0xFFFF) to apply to this permit rule entry.
log | **log-verbose**	(Optional) Enables syslog or verbose syslog messaging for an ACL rule hit.

Defaults

- If any destination, a specific destination or host destination MAC address is not specified, no destination address is applied to this permit rule entry.
- If the drop eligibility indicator keyword is not specified, the VLAN tag DEI flag is not applied to this permit rule entry.
- If a CoS is not specified, CoS is not applied to this permit rule entry.
- If a single or range of VLANs is not specified, the VLAN identifier is not applied to this permit rule entry.
- If an Ethernet II type is is not specified, the Ethernet II type is not applied to this permit rule entry.
- If a logging option is not specified, ACL rule logging is not enabled for this permit rule entry.

Mode

Configuration command, L2 ACL configuration mode .

Usage

Access list logging is throttled to 1 log message per second. If there are multiple access list rules with logging enabled (log or log-verbose), and more then one frame is transmitted per second that can hit those rules, only the first frame will generate a message. Logging is sampling and does not report every time that a rule with logging enabled is hit.

Source and destination wildcard provides an inverted mask (specifies the don't care bits as 1s). 00:00:00:00:00:00 specifies an exact match.

The **any** option is short hand for 00:00:00:00:00:00 FF:FF:FF:FF:FF:FF.

The "no" version of this command removes the last (if duplicate entries exist) or the specified (if no duplicate entries exist) permit entry.

Examples

This example enters configuration mode for the list1 L2 ACL and configures a permit entry for packets containing (verbose logging is enabled for this entry):

- Any source address
- A destination host with a MAC address of 00:11:88:fd:8e:f0
- VLANs 11 through 13
- An Ethernet II type 800

```
S Chassis(rw-config)->l2 access-list list1
S Chassis(rw-cfg-l2-acl)->permit any host 00:11:88:fd:8e:f0 vlan 11 13 ethertype
800 log-verbose
S Chassis(rw-cfg-l2-acl)->
```

This example enters configuration mode for the list2 L2 ACL and configures a permit entry for packets containing:

- A source MAC address of 02:02:03:04:05:06 with a mask that ignores the first four hex characters in the address
- A destination host with a MAC address of 00:11:88:fd:8e:f0
- Class of Service 5
- VLANs 11 through 13
- An Ethernet II type 86dd

```
S Chassis(rw-config)->l2 access-list list2
S Chassis(rw-cfg-l2-acl)->permit 02:02:03:04:05:06 ff:ff:00:00:00:00 host
00:11:88:fd:8e:f0 cos 5 vlan 11 13 ethertype 86dd
S Chassis(rw-cfg-l2-acl)->
```

deny

Use this command to create a deny access list rule entry.

Syntax

deny {**any** | **host** *source-macAddr* | *source-macAddr source-wildcard*} [**any** | **host** *destination-macAddr* | *destination-macAddr destination-wildcard*] [**dei**] [**cos** *cos*] [vlan vlan [*vidhi*]] [ethertype data] [**log** | **log-verbose**]

no deny {**any** | **host** *source-macAddr* | *source-macAddr source-wildcard*} [**any** | **host** *destination-macAddr* | *destination-macAddr destination-wildcard*] [**dei**] [**cos** *cos*] [vlan vlan [*vidhi*]] [ethertype data] [**log** | **log-verbose**]

Parameters

any	Specifies that any source MAC address and optionally any destination MAC address is applied to this deny rule entry.
host *source-macAddr*	Specifies a host source MAC address in the formats x:x:x:x:x:x or H.H.H to apply to this deny rule entry.

source-macAddr source-wildcard	Specifies a source MAC address and mask to apply to this deny rule entry, in the formats x:x:x:x:x:x or H.H.H.
host *destination-macAddr*	(Optional) Specifies a destination host MAC address in the formats x:x:x:x:x:x or H.H.H to apply to this deny rule entry.
destination-macAddr destination-wildcard	(Optional) Specifies a destination MAC address and mask to apply to this deny rule entry, in the formats x:x:x:x:x:x or H.H.H.
dei	(Optional) Specifies that the drop eligibility indicator in the VLAN tag is applied to this deny rule entry.
cos *cos*	(Optional) Specifies that the indicated class of service value is applied to this deny rule entry.
vlan *vlan*	(Optional) Specifies that the indicated VLAN identifier in the VLAN tag is applied to this deny rule entry or specifies the low end of a range of VLANs to apply to this deny rule entry.
vidhi	(Optional) Specifies the high end of a range of VLAN identifiers in the VLAN tag to apply to this deny rule entry
ethertype *data*	(Optional) Specifies that the indicated Ethernet II type (0x0 - 0xFFFF) to apply to this deny rule entry.
log | **log-verbose**	(Optional) Enables syslog or verbose syslog messaging for an ACL rule hit.

Defaults

- If any destination, a specific destination, or host destination MAC address is not specified, no destination address is applied to this deny rule entry.
- If the drop eligibility indicator keyword is not specified, the VLAN tag DEI flag is not applied to this deny rule entry.
- If a CoS is not specified, CoS is not applied to this deny rule entry.
- If a single or range of VLANs is not specified, the VLAN identifier is not applied to this deny rule entry.
- If an Ethernet II type is is not specified, the Ethernet II type is not applied to this deny rule entry.
- If a logging option is not specified, ACL rule logging is not enabled for this deny rule entry.

Mode

Configuration command, L2 ACL configuration mode.

Usage

Access list logging is throttled to 1 log message per second. If there are multiple access list rules with logging enabled (log or log-verbose), and more then one frame is transmitted per second that can hit those rules, only the first frame will generate a message. Logging is sampling and does not report every time that a rule with logging enabled is hit.

Source and destination wildcard provides an inverted mask (specifies the don't care bits as 1s). 00:00:00:00:00:00 specifies an exact match.

The **any** option is short hand for 00:00:00:00:00:00 FF:FF:FF:FF:FF:FF.

The "no" version of this command removes the last (if duplicate entries exist) or the specified (if no duplicate entries exist) deny entry with the specified text.

Examples

This example enters configuration mode for the list1 L2 ACL and configures a deny entry for packets containing (verbose logging is enabled for this entry):

- Any source address
- A destination host with a MAC address of 00:22:89:fd:8e:f1
- VLANs 11 through 13
- An Ethernet II type 800

```
S Chassis(rw-config)->l2 access-list list1
S Chassis(rw-cfg-l2-acl)->deny any host 00:22:88:fd:8e:f1 vlan 11 13 ethertype 800 log-verbose
S Chassis(rw-cfg-l2-acl)->
```

This example enters configuration mode for the list2 L2 ACL and configures a deny entry for packets containing:

- A source MAC address of 02:02:01:02:03:04 with a mask that ignores the first four hex characters in the address
- A destination host with a MAC address of 03:13:83:fd:8e:f3
- Class of Service 5
- VLANs 11 through 13
- An Ethernet II type 86dd

```
S Chassis(rw-config)->l2 access-list list2
S Chassis(rw-cfg-l2-acl)->deny 02:02:01:02:03:04 ff:ff:00:00:00:00 host 03:13:83:fd:8e:f3 cos 5 vlan 11 13 ethertype 86dd
S Chassis(rw-cfg-l2-acl)->
```

log

Use this command to generate a Syslog on rule hits.

Syntax

log [*entry* | **implicit** | **all**]

no log [*entry* | **implicit** | **all**]

Parameters

entry	(Optional) Specifies a sequence numbered entry to log when a hit occurs. Valid values: **1** - **5000**. Default value: **all**
implicit	(Optional) Specifies the logging of a final implicit deny hit.
all	(Optional) Specifies that all hits are to be logged, including the final implicit deny.

Defaults

If no option is specified, all hits are logged, including the final implicit deny.

Mode

Configuration command, L2 ACL configuration mode.

Usage

ACL logging is throttled to 1 log message per second. If there are multiple ACL rules with logging enabled (log or log-verbose), and more then one frame is transmitted per second that can hit those rules, only the first frame will generate a message. Logging is sampling and does not report every time that a rule with logging enabled is hit.

The "no" version of this command removes the last (if duplicate entries exist) or the specified (if no duplicate entries exist) log entry.

Example

This example enters configuration mode for L2 ACL list 2 and enables la detailed logging level for a final implicit deny hit:

```
S Chassis(rw-config)->l2 access-list list2
S Chassis(rw-cfg-l2-acl)->log implicit
S Chassis(rw-cfg-l2-acl)->
```

log-verbose

Use this command to generate a detailed Syslog on rule hits.

Syntax

log-verbose [*entry* | **implicit** | **all**]

no log-verbose [*entry* | **implicit** | **all**]

Parameters

entry	(Optional) Specifies a sequence numbered entry to log when a hit occurs. Valid values: **1** - **5000**. Default value: **all**
implicit	(Optional) Specifies the logging of a final implicit deny hit.
all	(Optional) Specifies that all hits are to be logged, including the final implicit deny.

Defaults

If no option is specified, all hits are logged, including the final implicit deny.

Mode

Configuration command, L2 ACL configuration mode.

Usage

ACL logging is throttled to 1 log message per second. If there are multiple ACL rules with logging enabled (log or log-verbose), and more then one frame is transmitted per second that can hit those rules, only the first frame will generate a message. Logging is sampling and does not report every time that a rule with logging enabled is hit.

The "no" version of this command removes the last (if duplicate entries exist) or the specified (if no duplicate entries exist) verbose log entry.

Example

This example enters configuration mode for L2 ACL list 2 and enables a detailed logging level for a final implicit deny hit:

```
S Chassis(rw-config)->l2 access-list list2
S Chassis(rw-cfg-l2-acl)->log-verbose implicit
S Chassis(rw-cfg-l2-acl)->
```

delete

Use this command to delete a pre-existing L2 ACL rule entry or range of entries.

Syntax

delete {*entry* | **from** *entry* **to** *entry*}

Parameters

entry | **from** *entry* **to** *entry*	(Optional) Specifies an entry or range of entries to delete. When deleting a range of entries, **from** specifies the beginning of the range, and **to** specifies the end of the range inclusive. An entry is a valid pre-existing L2 ACL rule from **1** to **5000**.

Defaults

None.

Mode

Configuration command, L2 ACL configuration mode.

Examples

This example enters configuration mode for the L2 ACL list2 and deletes rule entry 10:

```
S Chassis(rw-config)->l2 access-list list2
S Chassis(rw-cfg-l2-acl)->delete 10
S Chassis(rw-cfg-l2-acl)->
```

This example enters configuration mode for the L2 ACL list2 and deletes rule entry 10 - 12:

```
S Chassis(rw-config)->l2 access-list list2
S Chassis(rw-cfg-l2-acl)->delete from 10 to 12
S Chassis(rw-cfg-l2-acl)->
```

insert before

Use this command to insert an access list rule entry.

Syntax

insert before *entry* {**remark** "*text*" | {**permit** | **deny**} {**any** | **host** *source-macAddr* | *source-macAddr source-wildcard*} [**any** | **host** *destination-macAddr* | *destination-macAddr destination-wildcard*] [**dei**] [**cos** *cos*] [vlan vlan [*vidhi*]] [ethertype data] [**log** | **log-verbose**]

Parameters

entry	Specifies an entry to place the inserted rule before. An entry is a valid pre-existing access list rule or the explicit deny which is the default entry **1**.
remark *text*	Specify a text remark that will be associated with this ACL. Valid values: Up to 64 characters within double quotes (**“”**).
deny | **permit**	Denies or permits access if specified conditions are met.
any	Specifies that any source MAC address and optionally any destination MAC address is applied to this permit or deny rule entry.
host *source-macAddr*	Specifies a host source MAC address in the formats x:x:x:x:x:x or H.H.H to apply to this permit or deny rule entry.
source-macAddr source-wildcard	Specifies a source MAC address and mask to apply to this permit or deny rule entry, in the formats x:x:x:x:x:x or H.H.H.
host *destination-macAddr*	(Optional) Sepcifies a host destination MAC address in the formats x:x:x:x:x:x or H.H.H to apply to this permit or deny rule entry.
destination-macAddr destination-wildcard	(Optional) Specifies a destination MAC address and mask to apply to this permit or deny rule entry, in the formats x:x:x:x:x:x or H.H.H.
dei	(Optional) Specifies that the drop eligibility indicator in the VLAN tag is applied to this permit or deny rule entry.
cos *cos*	(Optional) Specifies that the indicated class of service value is applied to this permit or deny rule entry.
vlan *vlan*	(Optional) Specifies that the indicated VLAN identifier in the VLAN tag is applied to this permit rule entry or specifies the low end of a range of VLANs to apply to this permit or deny rule entry.
vidhi	(Optional) Specifies the high end of a range of VLAN identifiers in the VLAN tag to apply to this permit or deny rule entry
ethertype *data*	(Optional) Specifies that the indicated Ethernet II type (0x0 - 0xFFFF) to apply to this permit or deny rule entry.
log | **log-verbose**	(Optional) Enables syslog or verbose syslog messaging for an ACL rule hit.

Defaults

- If any destination, a specific destination or host destination MAC address is not specified, no destination address is applied to the inserted rule entry.
- If the drop eligibility indicator keyword is not specified, the VLAN tag DEI flag is not applied to the inserted rule entry.
- If a CoS is not specified, CoS is not applied to the inserted rule entry.
- If a single or range of VLANs is not specified, the VLAN identifier is not applied to the inserted rule entry.
- If an Ethernet II type is is not specified, the Ethernet II type is not applied to the inserted rule entry.
- If a logging option is not specified, ACL rule logging is not enabled for the inserted rule entry.

Mode

Configuration command, L2 ACL configuration mode.

Usage

ACL logging is throttled to 1 log message per second. If there are multiple ACL rules with logging enabled (log or log-verbose), and more then one frame is transmitted per second that can hit those rules, only the first frame will generate a message. Logging is sampling and does not report every time that a rule with logging enabled is hit.

Examples

This example inserts the remark "I am a remark entry at sequence number 17" in the L2 ACL list1:

```
S Chassis(rw-config)->l2 access-list list1
S Chassis(rw-cfg-l2-acl)->insert before 17 remark "I am a remark entry at sequence number 17"
```

This example enters configuration mode for the list1 L2 ACL and inserts at list sequence 5 a permit entry for packets containing (verbose logging is enabled for the inserted entry):

- Any source address
- A destination host with a MAC address of 00:11:88:fd:8e:f0
- VLANs 11 through 13
- An Ethernet II type 800

```
S Chassis(rw-config)->l2 access-list list1
S Chassis(rw-cfg-l2-acl)->insert before 5 permit any host 00:11:88:fd:8e:f0 vlan 11 13 ethertype 800 log-verbose
S Chassis(rw-cfg-l2-acl)->
```

replace

Use this command to replace an L2 ACL entry with a remark, permit or deny entry.

Syntax

replace *entry* {**remark "text"** | {**permit** | **deny**} {**any** | **host** *source-macAddr* | *source-macAddr source-wildcard*} [**any** | **host** *destination-macAddr* | *destination-macAddr destination-wildcard*] [**dei**] [**cos** *cos*] [vlan vlan [*vidhi*]] [ethertype data] [**log** | **log-verbose**]

Parameters

entry	Specify the entry to be replaced with the rule defined by this command.
remark *text*	Specify a text remark that will replace the specified entry. Valid values: Up to 64 characters within double quotes (**""**).
deny | **permit**	Specifies a deny or permits entry for this replacement entry.
any	Specifies that any source MAC address and optionally any destination MAC address is applied to this permit or deny rule entry.
host *source-macAddr*	Specifies a host source MAC address in the formats x:x:x:x:x:x or H.H.H to apply to this permit or deny rule entry.
source-macAddr source-wildcard	Specifies a source MAC address and mask to apply to this permit or deny rule entry, in the formats x:x:x:x:x:x or H.H.H.
host *destination-macAddr*	(Optional) Sepcifies a host destination MAC address in the formats x:x:x:x:x:x or H.H.H to apply to this permit or deny rule entry.

destination-macAddr destination-wildcard	(Optional) Specifies a destination MAC address and mask to apply to this permit or deny rule entry, in the formats x:x:x:x:x:x or H.H.H.
dei	(Optional) Specifies that the drop eligibility indicator in the VLAN tag is applied to this permit or deny rule entry.
cos *cos*	(Optional) Specifies that the indicated class of service value is applied to this permit or deny rule entry.
vlan *vlan*	(Optional) Specifies that the indicated VLAN identifier in the VLAN tag is applied to this permit rule entry or specifies the low end of a range of VLANs to apply to this permit or deny rule entry.
vidhi	(Optional) Specifies the high end of a range of VLAN identifiers in the VLAN tag to apply to this permit or deny rule entry
ethertype *data*	(Optional) Specifies that the indicated Ethernet II type (0x0 - 0xFFFF) to apply to this permit or deny rule entry.
log | **log-verbose**	(Optional) Enables syslog or verbose syslog messaging for an ACL rule hit.

Defaults

- If any destination, a specific destination or host destination MAC address is not specified, no destination address is applied to the replaced rule entry.
- If the drop eligibility indicator keyword is not specified, the VLAN tag DEI flag is not applied to the replaced rule entry.
- If a CoS is not specified, CoS is not applied to the replaced rule entry.
- If a single or range of VLANs is not specified, the VLAN identifier is not applied to the replaced rule entry.
- If an Ethernet II type is is not specified, the Ethernet II type is not applied to the replaced rule entry.
- If a logging option is not specified, ACL rule logging is not enabled for the replaced rule entry.

Mode

Configuration command, L2 ACL configuration mode.

Usage

ACL logging is throttled to 1 log message per second. If there are multiple ACL rules with logging enabled (log or log-verbose), and more then one frame is transmitted per second that can hit those rules, only the first frame will generate a message. Logging is sampling and does not report every time that a rule with logging enabled is hit.

Example

This example replaces the current entry at sequence 17 with the remark “I am a remark entry at sequence number 17” in the L2 ACL list1:

```
S Chassis(rw-config)->l2 access-list list1
S Chassis(rw-cfg-l2-acl)->replace 17 remark “I am a remark entry at sequence
number 17”
```

This example enters configuration mode for the list1 L2 ACL and replaces the curren entry at list sequence 5 with a permit entry for packets containing (verbose logging is enabled for the inserted entry):

- Any source address
- A destination host with a MAC address of 00:11:88:fd:8e:f0
- VLANs 11 through 13
- An Ethernet II type 800

```
S Chassis(rw-config)->l2 access-list list1
S Chassis(rw-cfg-l2-acl)->replace 5 permit any host 00:11:88:fd:8e:f0 vlan 11 13
ethertype 800 log-verbose
S Chassis(rw-cfg-l2-acl)->
```

move before

Use this command to move a pre-existing L2 ACL rule entry or range to the specified location in the access list.

Syntax

move before *entry1* **from** *entry2* **to** *entry3*

Parameters

entry1	Specifies a pre-existing access list entry before which entry range *entry2* to *entry3* will be moved.
entry2	Specifies a pre-existing access list entry that begins the range of entries that will be moved before *entry1*.
entry3	Specifies a pre-existing access list entry that ends the range of entries that will be moved before *entry1*.

Defaults

None.

Mode

Configuration command, L2 ACL configuration mode.

Examples

This example enters configuration mode for L2 ACL list2 and moves rule entry 20 before rule entry 10:

```
S Chassis(rw-config)->l2 access-list list2
S Chassis(rw-cfg-l2-acl)->move before 10 from 20 to 20
S Chassis(rw-cfg-l2-acl)->
```

This example enters configuration mode for L2 ACL list2 and moves rule entries 10 - 12 before rule entry 5:

```
S Chassis(rw-config)->l2 access-list list2
S Chassis(rw-cfg-l2-acl)->move before 5 from 10 to 12
S Chassis(rw-cfg-l2-acl)->
```

remark

Use this command to enter a text comment into the L2 ACL at the next entry.

Syntax

remark "*text*"

no remark "*text*"

Parameters

text	Specifies the text of up to 64 characters within double quotes (“”) to be entered as the next L2 ACL entry.

Defaults

None.

Mode

Configuration command, L2 ACL configuration mode.

Usage

Use the move before command on page 83-14 change a remark entry location.

The “no” version of this command removes the last (if duplicate entries exist) or the specified (if no duplicate entries exist) remark entry with the specified text.

Example

This example enters configuration mode for L2 ACL list1 and enters a remark specifying that the following entry permits any source address for this access list. The remark entry is followed by the permit any entry:

```
S Chassis(rw-config)->l2 access-list list1
S Chassis(rw-cfg-l2-acl)->remark "The following entry permits any source address."
S Chassis(rw-cfg-l2-acl)->permit any
S Chassis(rw-cfg-l2-acl)->
```

Displaying and Applying Access Control List Commands

This section details ACL commands used to display ACL configuration and counters, clear ACL counters, and apply ACLs to an interface. The commands used to display and apply ACL entries are:

For information about...	Refer to page...
l2 access-group	83-16
show access-lists l2	83-16
show access-lists applied	83-17
clear access-lists counters	83-18

l2 access-group

Use this command to apply L2 access restrictions to inbound or outbound frames on an interface.

Syntax

l2 access-group *name* {**in** | **out**}

no l2 access-group *name* {**in** | **out**}

Parameters

name	Specifies the L2 ACL to be applied to the access group. This is an alpha-numeric text name of up to 64 characters.
in	Filters inbound frames.
out	Filters outbound frames.

Defaults

None.

Mode

Configuration command, Interface configuration**.**

Usage

L2 ACLs must be applied per VLAN interface. An L2 ACL can either be applied to inbound or outbound frames. An L2 ACL can be applied before it is created. The uncreated applied L2 ACL will have no affect.

The “no” form of this command removes the specified L2 ACL from the access group.

Example

This example shows how to apply L2 ACL list1 for all inbound frames on VLAN 1:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->l2 access-group list1 in
```

show access-lists l2

Use this command to display configured L2 ACL configuration.

Syntax

show access-lists [*name*] **l2** [**brief**]

Parameters

name	(Optional) Displays access list information for a specific access list name.
brief	(Optional) Displays a summary version of the specified context.

Defaults

- If an L2 ACL name is not specified, the entire table of access lists will be displayed.

- If the **brief** option is not specified, a detailed level of information is displayed.

Mode

All command modes.

Examples

This example shows how to display a summary level information for L2 ACLs configured on the device:

```
S Chassis(rw-config)->show access-lists l2 brief

L2 Access List (last 49 chars)                    Type Ents Deny count
------------------------------------------------- ---- ---- --------------------
l2acl                                             l2    11  6
```

This example shows how to display a detailed level of information for L2 ACLs configured on the device:

```
S Chassis(rw-config)->show access-lists l2
L2 access list l2acl  (11 entries)  (6 deny hits)
  1 deny   host 0001.0700.0305  any log
  2 permit any  any dei log
  3 permit host 0001.0700.0300  any log
  4 deny   host 0001.0700.0301  any log
  5 deny   host 0001.0700.0302  any log
  6 deny   host 0001.0700.0306  any log
  7 deny   host 0001.0700.0307  any log
  8 deny   host 0001.0700.0308  any log
  9 deny   host 0001.0700.0303  any log
  10 deny   host 0001.0700.0304  any log
  -- implicit deny all --   log  (6 hits)
S Chassis(rw-config)->
```

show access-lists applied

Use this command to display applied IP access lists.

Syntax

show access-lists applied [**host** | **interfaces** [*vlan-string* | **vlan** *vlan*] [inbound] [outbound] [in-and-out]]

Parameters

host	(Optional) Displays access list information for all applied ingress to host services.
interfaces	(Optional) Displays access list information for all applied access list interface types or the specified interface type.
vlan	(Optional) Displays access list information for VLAN interfaces.
inbound	(Optional) Displays access list information for inbound interfaces.

outbound	(Optional) Displays access list information for outbound interfaces.
in-and-out	(Optional) Displays access list information for both inbound and outbound interfaces.

Defaults

If no option is applied, the entire table of applied access lists will be displayed.

Mode

All command modes.

Usage

ACL names may be up to 64 characters in length, but there is only room to display 32 characters (show applied) or 49 characters (show brief) on a single 80-character line. Names up to and including the maximum length will be displayed in their entirety. Names longer than the maximum display length will be displayed with an asterisk character followed by the last 31 or 48 characters of the name.

If an access list displays as ** unconfigured **, it means that the ACL applied to the interface or host has not yet been created. This is allowed, but the applied ACL will have no effect on traffic, since the ACL doesn't really exist yet.

Example

This example shows how to display applied IP access lists for this system:

```
S Chassis(rw-config)->show access-lists applied

Interface    L2 Access List (last 32 chars)   Dir  Type Ents Deny count
-----------  -------------------------------- ---- ---- ---- ------------------
vlan.0.90    l2acl1                           in   ext  11   6
vlan.0.102   l2acl2                           in    ** unconfigured **
S Chassis(rw-config)->
```

clear access-lists counters

Use this command to clear access list display counters.

Syntax

clear access-lists counters [*name* | **applied** [**host** | **interfaces** [**vlan** *vlan-id*] [**inbound** | **outbound** | **in-and-out**]]

Parameters

name	(Optional) Clears display counters for the specified access list number or name.
applied interfaces	(Optional) Clears display counters for applied host or interface statistics only.
vlan | **inbound** | **outbound** | **in-and-out**	(Optional) Clears only VLAN, only inbound, only outbound, or both inbound and outbound.

Defaults

If no option is specified, the clear action is applied to all access lists.

Mode

All command modes.

Example

This example clears the display counters for L2 ACL list2:

```
S Chassis(rw-config)->clear access-lists counters list2
S Chassis(rw-config)->
```

84

VRF Access Control List Commands

This chapter describes how to apply access lists to traffic routed between VRFs set of commands and how to use them. For information about configuring VRF ACLs, refer to the "Access Control List Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
vrf-access	84-1
ip access-group from-vrf	84-2
ip access-group from-any-vrf	84-3
ip access-group to-vrf	84-3
ip access-group to-any-vrf	84-4
ipv6 access-group from-vrf	84-5
ipv6 access-group from-any-vrf	84-5
ipv6 access-group to-vrf	84-6
ipv6 access-group to-any-vrf	84-7

vrf-access

Use this command to enter the VRF access configuration mode.

Syntax

```
vrf-access
no vrf-access
```

Parameters

None.

Defaults

None.

Mode

Configuration command, VRF configuration.

Usage

Within VRF access configuration mode you can apply access lists to VRF access groups for the restriction of traffic to and from other VRFs. One ingress and one egress IPv4 and one ingress and one egress IPv6 access group may be applied to a VRF. The same access group may be applied to multiple VRFs.

The “no” form of this command removes all VRF access mode configuration for this VRF.

Example

This example enters configuration mode for VRF **doc** and then enters the VRF access configuration mode for VRF **doc**:

```
S Chassis(su)->router doc
S Chassis(su-doc)->configure
S Chassis(su-doc-config)->vrf-access
S Chassis(su-doc-config)->
```

ip access-group from-vrf

Use this command to apply, in this VRF access context, an IPv4 access list to traffic from the specified VRF.

Syntax

ip access-group *list-name* **from-vrf** *vrf-name*

no ip access-group *list-name* **from-vrf** *vrf-name*

Parameters

list-name	Specifies access list to be applied to this VRF access group. This is an alpha-numeric text name of up to 64 characters.
vrf-name	Specifies the VRF that the traffic matching rules in the access list applied to the VRF access group will be inbound from.

Defaults

None.

Mode

VRF Configuration command, VRF access configuration**.**

Usage

The “no” form of this command removes the specified VRF access group from VRF configuration.

Example

This example shows how to apply the IPv4 **IPv4list1** ACL to any matching traffic inbound to VRF **doc** from VRF **eng**:

```
S Chassis(su-doc-config)->vrf-access
S Chassis(su-doc-config-vrf-access)->ip access-group IPv4list1 from-vrf eng
S Chassis(su-doc-config-vrf-access)->
```

ip access-group from-any-vrf

Use this command to apply, in this VRF access context, an IPv4 access list to traffic inbound from any VRF.

Syntax

ip access-group *list-name* **from-any-vrf**

no ip access-group *list-name* **from-any-vrf**

Parameters

list-name	Specifies access list to be applied to this VRF access group. This is an alpha-numeric text name of up to 64 characters.

Defaults

None.

Mode

VRF Configuration command, VRF access configuration**.**

Usage

The “no” form of this command removes the specified VRF access group from VRF configuration.

Example

This example shows how to apply the IPv4 **IPv4list1** ACL to any matching traffic inbound to VRF **doc** from any VRF:

```
S Chassis(su-doc-config)->vrf-access
S Chassis(su-doc-config-vrf-access)->ip access-group IPv4list1 from-any-vrf
S Chassis(su-doc-config-vrf-access)->
```

ip access-group to-vrf

Use this command to apply, in this VRF access context, an IPv4 access list to traffic outbound to the specified VRF.

Syntax

ip access-group *list-name* **to-vrf** *vrf-name*

no ip access-group *list-name* **to-vrf** *vrf-name*

Parameters

list-name	Specifies access list to be applied to this VRF access group. This is an alpha-numeric text name of up to 64 characters.
vrf-name	Specifies the VRF that the traffic matching rules in the access list applied to the VRF access group will be outbound to.

Defaults

None.

Mode

VRF Configuration command, VRF access configuration**.**

Usage

The “no” form of this command removes the specified VRF access group from VRF configuration.

Example

This example shows how to apply the IPv4 **Ipv4list2** ACL to any matching traffic outbound from VRF **doc** to VRF **eng**:

```
S Chassis(su-doc-config)->vrf-access
S Chassis(su-doc-config-vrf-access)->ip access-group IPv4list2 to-vrf eng
S Chassis(su-doc-config-vrf-access)->
```

ip access-group to-any-vrf

Use this command to apply, in this VRF access context, an IPv4 access list to traffic outbound to any VRF.

Syntax

ip access-group *list-name* **to-any-vrf**

no ip access-group *list-name* **to-any-vrf**

Parameters

list-name	Specifies access list to be applied to this VRF access group. This is an alpha-numeric text name of up to 64 characters.

Defaults

None.

Mode

VRF Configuration command, VRF access configuration**.**

Usage

The “no” form of this command removes the specified VRF access group from VRF configuration.

Example

This example shows how to apply the IPv4 **Ipv4list2** ACL to any matching traffic outbound from VRF **doc** to any VRF:

```
S Chassis(su-doc-config)->vrf-access
S Chassis(su-doc-config-vrf-access)->ip access-group IPv4list2 to-any-vrf
S Chassis(su-doc-config-vrf-access)->
```

ipv6 access-group from-vrf

Use this command to apply, in this VRF access context, an IPv6 access list to traffic from the specified VRF.

Syntax

ipv6 access-group *list-name* **from-vrf** *vrf-name*

no ipv6 access-group *list-name* **from-vrf** *vrf-name*

Parameters

list-name	Specifies access list to be applied to this VRF access group. This is an alpha-numeric text name of up to 64 characters.
vrf-name	Specifies the VRF that the traffic matching rules in the access list applied to the VRF access group will be inbound from.

Defaults

None.

Mode

VRF Configuration command, VRF access configuration**.**

Usage

The “no” form of this command removes the specified VRF access group from VRF configuration.

Example

This example shows how to apply the IPv6 **IPv6list1** ACL to any matching traffic inbound to VRF **doc** from VRF **eng**:

```
S Chassis(su-doc-config)->vrf-access
S Chassis(su-doc-config-vrf-access)->ipv6 access-group IPv6list1 from-vrf eng
S Chassis(su-doc-config-vrf-access)->
```

ipv6 access-group from-any-vrf

Use this command to apply, in this VRF access context, an IPv6 access list to traffic from any VRF.

Syntax

ipv6 access-group *list-name* **from-any-vrf**

no ipv6 access-group *list-name* **from-any-vrf**

Parameters

list-name	Specifies access list to be applied to this VRF access group. This is an alpha-numeric text name of up to 64 characters.

Defaults

None.

Mode

VRF Configuration command, VRF access configuration**.**

Usage

The “no” form of this command removes the specified VRF access group from VRF configuration.

Example

This example shows how to apply the IPv6 **IPv6list1** ACL to any matching traffic inbound to VRF **doc** from any VRF:

```
S Chassis(su-doc-config)->vrf-access
S Chassis(su-doc-config-vrf-access)->ipv6 access-group IPv6list1 from-any-vrf
S Chassis(su-doc-config-vrf-access)->
```

ipv6 access-group to-vrf

Use this command to apply, in this VRF access context, an IPv6 access list to traffic outbound to the specified VRF.

Syntax

ipv6 access-group *list-name* **to-vrf** *vrf-name*

no ipv6 access-group *list-name* **to-vrf** *vrf-name*

Parameters

list-name	Specifies access list to be applied to this VRF access group. This is an alpha-numeric text name of up to 64 characters.
vrf-name	Specifies the VRF that the traffic matching rules in the access list applied to the VRF access group will be outbound to.

Defaults

None.

Mode

VRF Configuration command, VRF access configuration**.**

Usage

The “no” form of this command removes the specified VRF access group from VRF configuration.

Example

This example shows how to apply the IPv6 **IPv6list2** ACL to any matching traffic outbound from VRF **doc** to VRF **eng**:

```
S Chassis(su-doc-config)->vrf-access
S Chassis(su-doc-config-vrf-access)->ipv6 access-group IPv6list2 to-vrf eng
S Chassis(su-doc-config-vrf-access)->
```

ipv6 access-group to-any-vrf

Use this command to apply, in this VRF access context, an IPv6 access list to traffic outbound to any VRF.

Syntax

ipv6 access-group *list-name* **to-any-vrf**

no ipv6 access-group *list-name* **to-any-vrf**

Parameters

list-name	Specifies access list to be applied to this VRF access group. This is an alpha-numeric text name of up to 64 characters.

Defaults

None.

Mode

VRF Configuration command, VRF access configuration**.**

Usage

The “no” form of this command removes the specified VRF access group from VRF configuration.

Example

This example shows how to apply the IPv6 **IPv6list2** ACL to any matching traffic outbound from VRF **doc** to any VRF:

```
S Chassis(su-doc-config)->vrf-access
S Chassis(su-doc-config-vrf-access)->ipv6 access-group IPv6list2 to-any-vrf
S Chassis(su-doc-config-vrf-access)->
```

85

Route-Map Manager Commands

This chapter provides detailed information for the route-map manager set of commands. For information about configuring route-map manager, refer to the "Route-Map Manager Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
General Route-Map Commands	85-1
Policy-Based Route-Map Commands	85-4
Redistribution Route-Map Commands	85-16
Filter-Based Route-Map Commands	85-24
BGP Route-Map Commands	85-31

General Route-Map Commands

General route-map commands provide for monitoring an IP interface and display of IP policy applied to the routing interface and configured route-map lists.

For information about...	Refer to page...
route-map probe	85-1
show ip policy	85-3
show route-map	85-4

route-map probe

Use this command to configure a route-map probe session to monitor the specified next hop address.

Syntax

route-map probe *ip-address* **probe-name** {*name* | **default**}

no route-map probe *ip-address* **probe-name** {*name* | **default**}

Parameters

ip-address	Specifies the next hop IPv4 or IPv6 address for this probe session to monitor.
probe-name *name* | **default**	Specifies the name of an administratively created ICMP probe to use for this session, or the **$pbr_default** default ICMP probe when the **default** keyword is specified.

Defaults

None.

Mode

Global configuration**.**

Usage

The route-map probe feature supports ICMP probes. When assigning an ICMP probe to monitor a next hop IP address, the port is auto-set to port **0** of the specified IP address. The probe is not assigned to a specific route-map. If a next hop IP address is declared down, it is removed from the next hop selection process for all route-maps specifying this address as a next hop, until it is declared up again.

The **$pbr_default** ICMP probe can not be specified directly. Use the **default** keyword to specify the **$pbr_default** ICMP probe.

Note: Next hop probes over layer 3 tunnels are not currently supported. The remote address will be declared down regardless of its state and the layer 3 tunnel will be taken down. Use “tunnel probe” on page 57-14 to monitor a layer 3 tunnel remote address.

The “no” form of this command removes the specified next hop IP address probe session.

Example

This example shows how to configure probe **ICMP-PBR** and assign it to monitor the next hop IP addresses **125.50.25.1** and **2000::1301:0:21f:45ff:fe4d:8722**:

```
S Chassis(su-config)->probe ICMP-PBR icmp
S Chassis(su-config-probe)->inservice
S Chassis(su-config-probe)->exit
S Chassis(su-config)->route-map probe 125.50.25.1 probe-name ICMP-PBR
S Chassis(su-config)->route-map probe 2000::1301:0:21f:45ff:fe4d:8722 probe-name
ICMP-PBR
S Chassis(su-config)->show probe sessions

Client Codes: P-policy based routing, S-SLB, V-VRRP, W-TWCB
              T-tracked object probe
...
Probe: ICMP-PBR, icmp
IP Address                      Port  Status    StChngs Last Change   Clients
------------------------------- ----- --------- ------- ------------- -------
125.50.25.1                     0     Up        1            0h0m30s  P
2000::1301:0:21f:45ff:fe4d:8722 0     Up        1            0h0m40s  P
```

```
Displayed 2 sessions
...
S Chassis(su-config)->
```

show ip policy

Use this command to display the policy route-map applied to all routing interfaces.

Syntax

show ip policy

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display policy route-maps applied to all routing interfaces:

```
S Chassis(rw-config)->interface vlan 5
S Chassis(rw-config-intf-vlan.0.5)->ip policy route-map rm1
S Chassis(rw-config-intf-vlan.0.5)->exit
S Chassis(rw-config)->interface vlan 25
S Chassis(rw-config-intf-vlan.0.25)->ip policy route-map rm2
S Chassis(rw-config-intf-vlan.0.25)->exit
S Chassis(rw-config)->show ip policy
Interface    route-map                        Priority  Load policy
-----------  -------------------------------  --------  -----------
vlan.0.5     rm1                              First     First Available
vlan.0.25    rm2                              First     First Available
S Chassis(rw-config)->
```

Table 85-1 show ip policy Output Details

Output...	What it displays...
Interface	Routing interface.
route-map	route-map assigned to the routing interface (using the **ip policy route-map** command as described in “ip policy route-map” on page 85-6.)
Priority	How the priority-based routing next hop selection will be prioritized. Set with the **ip policy priority** command as described in “ip policy priority” on page 85-8.

Table 85-1 show ip policy Output Details (continued)

Output...	What it displays...
Load policy	How the priority-based routing next hop will be selected. Set with the **ip policy load-policy** command as described in "ip policy priority" on page 85-8.

show route-map

Use this command to display configured route-map lists.

Syntax

show route-map [*name*] [**brief**] [**probe**]

Parameters

name	(Optional) Specifies name of the route-map to display.
brief	(Optional) Specifies that a summary line of information for each configured route-map should display.
probe	(Optional) Specifies that next hop configured probes should be displayed.

Defaults

If the *name*, **brief** or **probe** are not specified, all route-maps display.

Mode

Global Configuration.

Usage

If a next hop is no longer available based upon a route-map probe monitoring failure, an asterisk will display for that next hop in the **show route-map** command output. See "route-map probe" on page 85-1 for details on the **route-map probe** command.

Example

This example shows how to display route-map **rmP1**:

```
S Chassis(rw-config-route-map-pbr)->show route-map 101
 route-map policy rmP1 permit 10
  match ip address 101
  set next-hop 30.10.0.10* 30.10.0.20* 30.10.0.30*
 Policy matches: 0 packets
```

Policy-Based Route-Map Commands

For information about...	Refer to page...
route-map policy	85-5
ip policy route-map	85-6

For information about...	Refer to page...
ipv6 policy route-map	85-7
ip policy priority	85-8
ipv6 policy priority	85-8
ip policy load-policy	85-9
ipv6 policy load-policy	85-10
match ip address (policy)	85-11
set next-hop (policy)	85-12
set next-hop-v6 (policy)	85-12
set default-next-hop (policy)	85-13
set default-next-hop-v6 (policy)	85-14
set vrf (policy)	85-15

route-map policy

Use this command to create a named route-map entry for policy-based routing and to enable policy-based routing configuration mode.

Syntax

route-map policy *name* [**permit** | **deny**] [*sequence-number*]

no route-map policy *name* [**permit** | **deny**] [*sequence-number*]

Parameters

name	Specifies a name for this route-map.
permit	(Optional) Permits the packet to bypass route lookup and be forwarded to the next hop configured in the matching route-map.
deny	(Optional) Denies policy-based routing, forcing the packet to continue on its normal routing path.
sequence-number	(Optional) Specifies the order of this map entry in the route-map list, and the order in which this route-map entry will be checked for matching access list criteria. The packet check will exit with the first map entry in the list which matches the packet data. The default value is **10**.

Defaults

- If **permit** or **deny** is not specified, the route-map defaults to permit.
- If *sequence-number* is not specified, **10** will be applied.

Mode

Global configuration.

Usage

Route-map names can be up to 32 alphanumeric characters in length. This firmware release identifies route-map types, policy and redistribution, exclusively by the command entered and not the name identifying the route-map.

Note: Legacy route-map ID-numbers are supported (1 - 99 for redistribution; 100 - 199 for policy) but are no longer required and, in any case, no longer identify the route-map type. When upgrading from a firmware version that identified a redistribution or policy route-map solely on the basis of the number range, the upgrade process will correctly identify and configure the correct route-map type and use the legacy route-map ID-number as the route-map name.

Each named policy route-map can have one or more entries. Each policy route-map entry is identified by a unique sequence-number. Each entry can be optionally configured as a permit or deny. Route-map entries default to sequence-number 10. If you enter a route-map entry without specifying a sequence-number, and entry 10 already exists for that route-map, the new entry will replace the existing entry. Use "show route-map" on page 85-4 to display current route-map entries, by sequence-number, for a specified route-map.

Executing the **route-map policy** command enters route-map policy configuration command mode for the specified entry. Once in route-map policy configuration command mode, each entry can be configured for one or more clauses made up of **match ip-address** (see "match ip address (policy)" on page 85-11) or **set next-hop** (see "set next-hop (policy)" on page 85-12) configurations.

See the release notes that come with your product for the number of supported:

- Policy route-maps
- Set or match clauses across all configured route-maps

The "no" form of this command removes the specified route-map list, or, if the sequence number is specified, route-map entry.

Example

This example shows how to create a policy route-map named **rm1** with a sequence order of 20:

```
S Chassis(rw-config)->route-map policy rm1 permit 20
S Chassis(rw-config-route-map-pbr)->
```

ip policy route-map

Use this command to assign a route-map list to a routing interface**.**

Syntax

ip policy route-map *name*

no ip policy route-map *name*

Parameters

name	Specifies a route-map name, matching a value previously set using the **route-map policy** command ("route-map policy" on page 85-5).

Defaults

None.

Mode

Interface configuration.

Usage

Only one route-map list is allowed per interface.

The “no” form of this command removes the specified route map from the interface.

Example

This example shows how to assign route-map rm1 to VLAN 5:

```
S Chassis(rw-config)->interface vlan 5
S Chassis(rw-config-intf-vlan.0.5)->ip policy route-map rm1
```

ipv6 policy route-map

Use this command to assign a route-map to an IPv6 routing interface**.**

Syntax

ipv6 policy route-map *name*

no ipv6 policy route-map *name*

Parameters

name	Specifies the name of the route-map to assign to the IPv6 routing interface.

Defaults

None.

Mode

Interface configuration.

Usage

The **no ipv6 policy route-map** command removes the specified route-map from the IPv6 routing interface.

Example

This example shows how to assign route-map rtemap1 to VLAN 50:

```
S Chassis(su-config)->interface vlan 50
S Chassis(su-config-intf-vlan.0.50)->ipv6 policy route-map rtemap1
S Chassis(su-config-intf-vlan.0.50)->
```

ip policy priority

Use this command to prioritize priority-based routing next hop behavior.

Syntax

```
ip policy priority {[only | first | last]}
no ip policy priority
```

Parameters

only	Prioritizes use of the priority-based routing by using the priority-based routing next hop, but if it is unavailable, drops the packet.
first	Prioritizes use of the priority-based routing by using the priority-based routing next hop, but if it is unavailable, the route table is used.
last	Prioritizes use of the priority-based routing by using the route table if the route exists, but if it is unavailable, the priority-based routing next hop is used.

Defaults

None.

Mode

Interface configuration.

Usage

This command prioritizes use of the priority-based routing configured policy — as opposed to doing a lookup in the FIB (Forward Information Base) route table for a next hop.

The “no” form of this command resets the priority configuration back to the default of **first**.

Example

This example shows how to set the IP policy priority on VLAN 1 to “last”:

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip policy priority last
```

ipv6 policy priority

Use this command to prioritize priority-based routing next hop behavior on the IPv6 interface.

Syntax

```
ipv6 policy priority {only | first | last}
no ipv6 policy priority
```

Parameters

only | **first** | **last**	Prioritizes use of the priority-based routing configured policy — as opposed to doing a lookup in the FIB (Forward Information Base) route table for a next hop — as follows: • **only** - uses the priority-based routing next hop, but if it is unavailable, drops the packet. • **first** (default) - uses the priority-based routing next hop, but if it is unavailable, the route table is used. • **last** - uses the route table if route exists, but if it is unavailable, the priority-based routing next hop is used.

Defaults

None.

Mode

Interface configuration.

Usage

The **no ipv6 policy priority** command resets the priority configuration back to the default of **first**.

Example

This example shows how to set the IP policy priority on VLAN 50 to **last**:

```
S Chassis(su-config)->interface vlan 50
S Chassis(su-config-intf-vlan.0.50)->ipv6 policy priority last
S Chassis(su-config-intf-vlan.0.50)->
```

ip policy load-policy

Use this command to configure priority-based routing next hop behavior.

Syntax

ip policy load-policy {**first-available** | **round-robin** | **ip-hash** {**source** | **destination** | **both**}}

no ip policy load-policy

Parameters

first-available	Uses the first available next hop from the list of next hops. (Default).
round-robin	Uses a round robin algorithm to select from the list of next hops.
ip-hash	Selects the next hop behavior based on a random equal distribution possible next hops.
sip	Selects the next hop based upon a random equal distribution of IP source addresses.
dip	Selects the next hop based upon a random equal distribution of IP destination addresses.

both	Selects the next hop based upon a random equal distribution of both the IP source addresses and the IP destination addresses.

Defaults

None.

Mode

Interface configuration.

Usage

When more than one next hop is configured (using the **set next hop** command as described in "set next-hop (policy)" on page 85-12) the load policy specifies choosing one next hop from among the sequence of next hops in the map matching the current packet. A next hop is considered available by default unless a route-map probe is monitoring the next hop and has flagged it as unavailable.

The "no" form of this command resets the next hop behavior to **first-available**.

Example

This example shows how to set the load policy behavior on VLAN 1 to "round-robin":

```
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->ip policy load-policy round-robin
```

ipv6 policy load-policy

Use this command to configure ipv6 load balancing for multiple next hops.

Syntax

```
ipv6 policy load-policy {first-available | round-robin | ip-hash}
no ipv6 policy load-policy {first-available | round-robin | ip-hash}
```

Parameters

first-available | **round-robin** | **ip-hash**	Specifies the load balancing policy to use for this IPv6 interface: • **first-available** - Choose the first available IPv6 next hop in the list (default) • **round-robin** - Choose an IPv6 next hop by circulating through available next hops • **ip-hash** - Choose an IPv6 next hop based on a hash value

Defaults

None.

Mode

Interface configuration**.**

Usage

The **no ipv6 policy load-policy** command resets the load balancing method for the IPv6 interface to the default value of first available.

Example

This example sets the load balancing method to round robin for VLAN 50:

```
S Chassis(su-config)->interface vlan 50
S Chassis(su-config-intf-vlan.0.50)->ipv6 policy load-policy round-robin
S Chassis(su-config-intf-vlan.0.50)->
```

match ip address (policy)

Use this command to match a packet against up to five access lists.

Syntax

match ip address *access-list*

no match ip address *access-list*

Parameters

access-list	Matches a packet to up to five specified access lists delineated by a space.

Defaults

None.

Mode

Policy-based routing configuration.

Usage

This command allows the listing of up to 5 ACLs delineated by a space. Attempting to specify a sixth ACL will cause an error to display: **Error: Unknown:** "*acl-name*".

Multiple match IP address entries may be configured, but a match of at least one ACL in each match entry must occur for a successful match for this sequence.

The "no" form of this command removes the match between an access list and this route-map.

Example

This example shows how to match a packet source IP address to access lists **1**, **10**, and **extIP100**:

```
S Chassis(rw-config)->route-map policy 101
S Chassis(rw-config-route-map-pbr)->match ip address 1 10 extIP100
S Chassis(rw-config-route-map-pbr)->show route-map 101
 route-map policy 101 permit 10
  match ip address 1 10 extIP10
 Policy matches: 0 packets
```

set next-hop (policy)

Use this command to set one or more next hop IP addresses for packets matching an access list in a configured route-map.

Syntax

set next-hop {*next-hop1*}[*next-hop2....next-hop5*]

no set next-hop {*next-hop1*}[*next-hop2....next-hop5*]

Parameters

next-hop	Specifies a next hop IP address. Up to five addresses can be specified per command line.

Defaults

None.

Mode

Policy-based routing configuration.

Usage

Up to a maximum of 128 unique next hops can be configured per policy route-map, 5 per command line, using multiple command lines. The total number of next hops includes both standard next hops configured using this command and default next hops configured using the set default-next-hop (policy) command.

The "no" form of this command deletes the specified next hop IP address(es).

Example

This example shows how to set IP address 10.2.3.4 as the next hop for packets matching ACL 1:

```
S Chassis(rw-config)->route-map policy 101 permit 20
S Chassis(rw-config-route-map-pbr)->match ip address 1
S Chassis(rw-config-route-map-pbr)->set next-hop 10.2.3.4
```

set next-hop-v6 (policy)

Use this command to set one or more next hop IPv6 addresses for packets matching an access list in a configured route-map.

Syntax

set next-hop-v6 {*next-hop1*}[*next-hop2....next-hop5*]

no set next-hop-v6 {*next-hop1*}[*next-hop2....next-hop5*]

Parameters

next-hopx	Specifies a next hop IPv6 address(es). Up to five addresses can be specified per command line.

Defaults

None.

Mode

Policy-based routing configuration.

Usage

Up to a maximum of 512 unique next hops can be configured, 5 per command line, using multiple command lines. The total number of next hops includes both standard next hops configured using this command and default next hops configured using the set default-next-hop (policy) command.

The "no" form of this command deletes the specified next hop IP address(es).

Example

This example shows how to set IPv6 address 2001::11 as the next hop for packets matching ACL 101:

```
S Chassis(rw-config)->route-map policy 101 permit 20
S Chassis(rw-config-route-map-pbr)->match ip address 1
S Chassis(rw-config-route-map-pbr)->set next-hop-v6 2001::11
```

set default-next-hop (policy)

Use this command to set up to 5 default next hop IP addresses for packets matching an access list in a configured route-map.

Syntax

set default-next-hop {*next-hop1*}[*next-hop2....next-hop5*]

no set default-next-hop {*next-hop1*}[*next-hop2....next-hop5*]

Parameters

next-hop	Specifies a next hop IP address. Up to five addresses can be specified per command line.

Defaults

None.

Mode

Policy-based routing configuration.

Usage

The **set default-next-hop** command augments the **set next-hop** command. A configured default-next-hop is only used when the following criteria are both true:

- No next hops have been configured with the **set next-hop** command, or the configured next hop IP addresses are not available
- The destination IP lookup results in the default route being returned.

If both criteria are true, the next hop will be chosen from the default-next-hop IP address list, using the next hop selection setting configured with the command "ip policy load-policy" on page 85-9.

The priority configured with the command "ip policy priority" on page 85-8 does not apply when using the default-next-hop.

Up to 128 unique next hops can be configured per policy route-map, 5 per command line, using multiple command lines. The total number of next hops includes both default-next-hops configured using this command and standard next hops configured using the set next-hop (policy) command.

The "no" form of this command deletes the specified default-next hop IP address(es).

Example

This example shows how to set IP address 10.2.3.4 as the default next hop for packets matching ACL 1:

```
S Chassis(rw-config)->route-map policy 101 permit 20
S Chassis(rw-config-route-map-pbr)->match ip address 1
S Chassis(rw-config-route-map-pbr)->set default-next-hop 10.2.3.4
```

set default-next-hop-v6 (policy)

Use this command to set up to 5 default next hop IPv6 addresses for packets matching an access list in a configured route-map.

Syntax

set default-next-hop-v6 {*next-hop1*}[*next-hop2....next-hop5*]

no set default-next-hop-v6 {*next-hop1*}[*next-hop2....next-hop5*]

Parameters

next-hop	Specifies a next hop IPv6 address(es). Up to five addresses can be specified per command line.

Defaults

None.

Mode

Policy-based routing configuration.

Usage

The **set default-next-hopv6** command augments the **set next-hop-v6** command. A configured default-next-hop is only used when the following criteria are both true:

- No **set next-hop-v6** command configuration exists or the configured next-hop IP addresses are not available
- The destination IP lookup results in the default route being returned.

If both criteria are true, the next hop will be chosen from the default-next-hop-v6 IP address list, using the setting configured in the command "ip policy load-policy" on page 85-9.

The priority configured in the command "ip policy priority" on page 85-8 does not apply when using the default-next-hop.

Up to 512 unique next-hops can be configured, 5 per command line, using multiple command lines. The total number of next-hops includes both default-next-hops configured using this command and standard next-hops configured using "set next-hop-v6 (policy)" on page 85-12.

The "no" form of this command deletes the specified default-next hop IP address(es).

Example

This example shows how to set IP address 2001::12 as the default next hop for packets matching ACL 1:

```
S Chassis(rw-config)->route-map policy 1 permit 20
S Chassis(rw-config-route-map-pbr)->match ip address 1
S Chassis(rw-config-route-map-pbr)->set default-next-hop-v6 2001::12
```

set vrf (policy)

Use this command to specify the VRF that will perform the next hop lookup, when the next hop of a policy IP address match belongs to a different VRF.

Syntax

set vrf *vrf-name*

no set vrf *vrf-name*

Parameters

vrf-name	Specifies the VRF instance that will determine the next hop based upon its route lookup.

Defaults

None.

Mode

Policy-based routing configuration.

Usage

If the next hop of a policy IP address match, specified in the **set next-hop** command, belongs to a different VRF, use this command to configure the next hop VRF to perform the route lookup.

The "no" form of this command deletes the specified set VRF router configuration for this route map.

Example

This example shows how to set VRF vr2 to determine the next hop based upon its route table lookup:

```
S Chassis(rw-vr1-config)->route-map policy 101 permit 20
S Chassis(rw-vr1-config-route-map-pbr)->match ip address 1
S Chassis(rw-vr1-config-route-map-pbr)->set vrf vr2
```

Redistribution Route-Map Commands

For information about...	Refer to page...
route-map redistribution	85-16
match interface (redistribution)	85-18
match ip address (redistribution)	85-18
match ipv6 address (redistribution)	85-19
match metric (redistribution)	85-19
match tag (redistribution)	85-20
set tag (redistribution)	85-21
set metric (redistribution)	85-22
set metric decrement (redistribution)	85-22
set metric increment (redistribution)	85-23
set metric-type (redistribution)	85-24

route-map redistribution

Use this command to create a named route-map entry for redistribution and to enable route-map redistribution configuration mode.

Syntax

route-map redistribution *name* [**permit** | **deny**] [*sequence-number*]

no route-map *name* [**permit** | **deny**] [*sequence-number*]

Parameters

name	Specifies a name for this route-map of up to 32 alphanumeric characters.
permit	(Optional) Permits the packet to be redistributed based upon the matching route-map.
deny	(Optional) Denies redistribution of a packet based upon the matching route-map.
sequence-number	(Optional) Specifies the order of this map entry in the route-map list, and the order in which this route-map entry will be checked for matching access list criteria. The packet check will exit with the first map entry in the list which matches the packet data. The default value is **10**.

Defaults

- If **permit** or **deny** is not specified, this command will enable route-map redistribution configuration mode.
- If *sequence-number* is not specified, **10** will be applied.

Mode

Global configuration.

Usage

Route-map names can be up to 32 alphanumeric characters in length. This firmware release identifies route-map types policy, redistribution, and filter, exclusively by the command entered and not the name identifying the route-map.

Note: Legacy route-map ID-numbers are supported (1 - 99 for redistribution; 100 - 199 for policy) but no longer required and, in any case, no longer identify the route-map type. When upgrading from a firmware version that identified a redistribution or policy route-map solely on the basis of the number range, the upgrade process will correctly identify and configure the correct route-map type and use the legacy route-map ID-number as the route-map name.

Each named redistribution route-map list can have one or more entries. Each redistribution route-map entry is identified by a unique sequence-number. Each entry can be optionally configured as a permit or deny. Route-map entries default to sequence-number 10. If you enter a route-map entry without specifying a sequence-number, and entry 10 already exists for that route-map, the new entry will replace the existing entry. Use "show route-map" on page 85-4 to display current route-map entries, by sequence-number, for a specified route-map.

In a redistribution context, a deny entry specifies that no action will take place, which is the default behavior if permit is not specified.

Executing the **route-map redistribution** command enters route-map configuration command mode for the specified entry. Once in route-map configuration command mode, each entry can be configured for one or more clauses made up of:

- **match ip-address** (see "match ip address (redistribution)" on page 85-18)
- **match interface** (see "match interface (redistribution)" on page 85-18)
- **match metric** (see "match metric (redistribution)" on page 85-19)
- **match tag** (see "match tag (redistribution)" on page 85-20)
- **set tag** (see "set tag (redistribution)" on page 85-21)
- **set metric** (see "set metric (redistribution)" on page 85-22)
- **set metric decrement** (see "set metric decrement (redistribution)" on page 85-22)
- **set metric increment** (see "set metric increment (redistribution)" on page 85-23)
- **set metric-type** (see "set metric-type (redistribution)" on page 85-24)

See the release notes that come with your product for the number of supported:

- Redistribution route-maps
- Set or match clauses across all configured route-maps

The "no" form of this command removes the specified route-map, or, if the sequence number is specified, route-map entry.

Example

This example shows how to create a redistribution route-map named rm2 with a sequence order of 5:

```
S Chassis(rw-config)->route-map redistribution rm2 permit 5
S Chassis(rw-config-route-map)->
```

match interface (redistribution)

Use this command to match a packet source IP address against the specified VLAN interface.

Syntax

match interface {**vlan** *vlan* | *string*}

no match interface {**vlan** *vlan* | *string*}

Parameters

vlan *vlan* | *string*	Specifies a VLAN in either number (vlan 1) or string (vlan.0.1) format.

Defaults

None.

Mode

Route-map configuration.

Usage

The "no" form of this command removes the match between a VLAN and this route-map.

Example

This example shows how to match a packet source IP address to VLAN 100 on route-map rm5:

```
S Chassis(rw-config)->route-map redistribution rm5
S Chassis(rw-config-route-map)->match interface vlan.0.100
```

match ip address (redistribution)

Use this command to match a packet source IP address against up to 5 access lists.

Syntax

match ip address {*access-list-number*}

no match ip address {*access-list-number*}

Parameters

access-list-number	Matches packet source IP addresses to up to five specified access lists delineated by a space.

Defaults

None.

Mode

Route-map configuration.

Usage

This command allows the listing of up to 5 ACLs delineated by a space. Attempting to specify a sixth ACL will cause an error to display: **Error: Unknown: "acl-name"**.

Multiple match IP address entries may be configured, but a match of at least one ACL in each match entry must occur for a successful match for this sequence.

The “no” form of this command removes the match between an access list and this route-map.

Example

This example shows how to match a packet source IP address to access-lists **2 5 10 12 13**:

```
S Chassis(rw-config)->route-map redistribution rm5
S Chassis(rw--config-route-map)->match ip address 2 5 10 12 13
S Chassis(rw--config-route-map)->
```

match ipv6 address (redistribution)

Use this command to match a packet source IPv6 address against up to 5 access lists.

Syntax

match ipv6 address {*access-list-name*}

no match ipv6 address {*access-list-name*}

Parameters

access-list-name	Matches packet source IPv6 addresses to up to five specified access lists.

Defaults

None.

Mode

Route-map configuration.

Usage

The “no” form of this command removes the match between an access list and this route-map.

Example

This example shows how to match a packet source IP address to IPv6 access-lists 3 6 11 14 15:

```
S Chassis(rw-config)->route-map redistribution rm5
S Chassis(rw-config-route-map)->match ipv6 address 3 6 11 14 15
S Chassis(rw-config-route-map)->
```

match metric (redistribution)

Use this command to match a route metric or range of route metrics.

Syntax

match metric {*cost* | **range** *min-cost max-cost*}

no match metric {*cost* | **range** *min-cost max-cost*}

Parameters

cost	Specifies a metric cost to be matched for this route-map. Valid values: **1** - **4294967295**. Default Value: None.
range *min-cost max-cost*	Specifies a range of metric costs to be matched for this route-map: • *min-cost* - Specifies the low end cost of the range. • *max-cost* - Specifies the high end cost of the range. Valid values: **1** - **4294967295**. Default Value: None.

Defaults

None.

Mode

Route-map configuration.

Usage

The "no" form of this command removes the match for the specified cost or range of costs.

Example

This example shows how to match a range of costs starting at 100 and ending at 200 for redistribution route-map rm5:

```
S Chassis(rw-config)->route-map redistribution rm5
S Chassis(rw--config-route-map)->match metric range 100 200
S Chassis(rw--config-route-map)->
```

match tag (redistribution)

Use this command to match an OSPF route tag ID or range of route tag IDs.

Syntax

match tag {*tag-id* | **range** *min-tag-id max-tag-id*}

no match tag {*tag-id* | **range** *min-tag-id max-tag-id*}

Parameters

tag-id	Specifies an OSPF tag ID to be matched for this route-map. Valid values: **0** - **4294967295**. Default Value: None.
range *min-tag-id max-tag-id*	Specifies a range of OSPF tag IDs to be matched for this route-map: • *min-tag-id* - Specifies the low end tag ID of the range. • *max-tag-id* - Specifies the high end tag ID of the range. Valid values: **0** - **4294967295**. Default Value: None.

Defaults

None.

Mode

Route-map configuration.

Usage

The “no” form of this command removes the match for the specified tag ID or range of tag IDs.

Example

This example shows how to match a range of OSPF tag IDs starting at 10000 and ending at 20000 for redistribution route-map rm5:

```
S Chassis(rw-config)->route-map redistribution rm5
S Chassis(rw--config-route-map)->match tag range 10000 20000
S Chassis(rw--config-route-map)->
```

set tag (redistribution)

Use this command to set a route tag to be used for redistribution by the source packet matched in this route-map.

Syntax

set tag *tag*

no set tag *tag*

Parameters

tag	Specifies a route tag to be used for redistribution by the source packet matched in this route-map. Valid values: 0 - 4294967295.

Defaults

None.

Mode

Route-map configuration.

Usage

OSPF route tags are displayed in the **show ip ospf database external** command (see “show ip ospf database” on page 73-44.

An OSPF route tag is a 32-bit numeric value that is attached to redistributed routes into OSPF. The route tag is not used by OSPF, but can be used by other routers for making policy decisions.

The “no” form of this command deletes this route tag set clause.

Example

This example shows how to set route tag 555 as the route to be used by a match for sequence 1 of the rm5 route-map:

```
S Chassis(rw-config)->route-map redistribution rm5 permit 1
S Chassis(rw-config-route-map)->match ip address 1
S Chassis(rw-config-route-map)->set tag 555
```

set metric (redistribution)

Use this command to set a route metric to be used for redistribution by the source packet matched in this route-map.

Syntax

set metric *cost*

no set metric *cost*

Parameters

cost	Specifies a route cost to be used for redistribution by the source packet matched in this route-map. Valid values: **1** - **4294967295**. Default Value: None.

Defaults

None.

Mode

Route-map configuration.

Usage

The "no" form of this command deletes this route metric set clause.

Example

This example shows how to set the route cost to 200 for redistribution by the source packet matched in the rm5 route-map:

```
S Chassis(rw-config)->route-map redistribution rm5
S Chassis(rw-config-route-map)->set metric 200
S Chassis(rw-config-route-map)->
```

set metric decrement (redistribution)

Use this command to decrement the existing cost when redistributing a source packet matched by this route-map.

Syntax

set metric decrement *cost*

no set metric decrement *cost*

Parameters

cost	Specifies the amount to decrement the existing cost when redistributing a source packet matched by this route-map. Valid values: **1** - **4294967295**. Default Value: None.

Defaults

None.

Mode

Route-map configuration.

Usage

The “no” form of this command deletes this metric decrement set clause.

Example

This example shows how to decrement the route cost by 50 when redistributing source packets matched in the rm5 route-map:

```
S Chassis(rw-config)->route-map redistribution rm5
S Chassis(rw-config-route-map)->set metric decrement 50
S Chassis(rw-config-route-map)->
```

set metric increment (redistribution)

Use this command to increment the existing cost when redistributing a source packet matched by this route-map.

Syntax

set metric increment *cost*

no set metric increment *cost*

Parameters

cost	Specifies the amount to increment the existing cost when redistributing a source packet matched by this route-map. Valid values: **1** - **4294967295**. Default Value: None.

Defaults

None.

Mode

Route-map configuration.

Usage

The “no” form of this command deletes this metric increment set clause.

Example

This example shows how to increment the route cost by 50 when redistributing source packets matched in the rm5 route-map:

```
S Chassis(rw-config)->route-map redistribution rm5
S Chassis(rw-config-route-map)->set metric increment 50
S Chassis(rw-config-route-map)->
```

set metric-type (redistribution)

Use this command to specify the OSPF metric type when redistributing a source packet matched by this route-map.

Syntax

```
set metric-type {type-1 | type-2}
no set metric-type {type-1 | type-2}
```

Parameters

type-1 | **type-2**	Specifies the OSPF metric type when redistributing a source packet by this route-map. Valid values: **type-1** or **type-2**. Default Value: None.

Defaults

None.

Mode

Route-map configuration.

Usage

The “no” form of this command deletes this metric type set clause.

Example

This example shows how to set the OSPF metric type to type-2 when redistributing source packets matched in the rm5 route-map:

```
S Chassis(rw-config)->route-map redistribution rm5
S Chassis(rw-config-route-map)->set metric-type type-2
S Chassis(rw-config-route-map)->
```

Filter-Based Route-Map Commands

For information about...	Refer to page...
route-map filter	85-25
match interface (filter)	85-26
match ip (filter)	85-26
match ipv6 (filter)	85-27
match tag (filter)	85-28
match metric (filter)	85-29
match route-type (filter)	85-30

route-map filter

Use this command to create a route-map for OSPF filtering.

Syntax

route-map filter *name* [**permit** | **deny**] [*sequence-number*]

no route-map *name* [**permit** | **deny**] [*sequence-number*]

Parameters

name	Specifies a name for this route-map of up to 32 alphanumeric characters.
permit	(Optional) Permits the packet to be filtered based upon the matching route-map.
deny	(Optional) Denies filtering of a packet based upon the matching route-map.
sequence-number	(Optional) Specifies the order of this map entry in the route-map list, and the order in which this route-map entry will be checked for matching access list criteria. The packet check will exit with the first map entry in the list which matches the packet data. The default value is **10**.

Defaults

- If **permit** or **deny** is not specified, this command will enable route-map filtering configuration mode.
- If *sequence-number* is not specified, **10** will be applied.

Mode

Global configuration.

Usage

Route-map names can be up to 32 alphanumeric characters in length.

Each named OSPF filter route-map can have one or more entries. Each OSPF filter route-map entry is identified by a unique sequence-number. Each entry can be optionally configured as permit or deny.

Entering the **route-map filter** command enters route-map configuration command mode for the specified entry. Once in route-map configuration command mode, each entry can be configured for one or more clauses made up of:

- **match interface** (see "match interface (filter)" on page 85-26)
- **match ip** (see "match ip (filter)" on page 85-26)
- **match tag** (see "match tag (filter)" on page 85-28)
- **match metric** (see "match metric (filter)" on page 85-29)
- **match metric** (see "match route-type (filter)" on page 85-30)

See the release notes that come with your product for the number of supported:

- Filter route-maps
- Match clauses across all configured route-maps

The “no” form of this command removes the specified route-map, or, if the sequence-number is specified, route-map entry.

Example

This example shows how to create a filter route-map named ospf1 with a sequence order of 5:

```
S Chassis(rw-config)->route-map filter ospf1 permit 5
S Chassis(rw-config-fltr)->
```

match interface (filter)

Use this command to match the outgoing interface of the route to be installed in the OSPF routing table.

Syntax

match interface {*interface-name* | *alias*}

no match interface {*interface-name* | *alias*}

Parameters

interface-name | *alias*	Specifies an interface name or alias to match for this OSPF filter.

Defaults

None.

Mode

Route-map filter configuration.

Usage

The specified interface represents the outgoing interface for the route being installed into the routing table by OSPF.

Apply the filter route-map using the **distribute-list route-map in** command in OSPF router configuration command mode to prevent route matches from entering the OSPF routing table.

The “no” form of this command removes the match between an interface and this route-map.

Example

This example shows how to match a packet source IP address to VLAN 100 on route-map **ospf1**:

```
S Chassis(rw-config)->route-map filter ospf1
S Chassis(rw-config-fltr)->match interface vlan.0.100
```

match ip (filter)

Use this command to match a route network address, next hop, or source router ID.

Syntax

match ip {**address** | **next-hop** | **route-source**} *access-list*

no match ip {**address** | **next-hop** | **route-source**} *access-list*

Parameters

address	Specifies that network addresses should be matched against the contents of the specified ACL(s).
next-hop	Specifies that next-hop addresses should be matched against the contents of the specified ACL(s).
route-source	Specifies that source route IDs should be matched against the contents of the specified ACL(s).
access-list	Specifies the ACL for which the specified command option will be matched against.

Defaults

None.

Mode

Route-map filter configuration.

Usage

Allows for up to **5** access lists in a single command line to be associated with each address, next-hop, or route-source entry. Multiple access list entries are delineated by a space.

Apply the filter route-map using the **distribute-list route-map in** command in OSPF router configuration command mode to prevent route matches from entering the OSPF routing table.

The "no" form of this command removes the IP match for this route-map.

Example

This example shows how to match a packets next hop IP address to the contents of the **acl1** and **acl2** access lists:

```
S Chassis(rw-config)->route-map filter ospf1
S Chassis(rw--config-fltr)->match ip next-hop acl1 acl2
```

match ipv6 (filter)

Use this command to match a route network address, next hop or source router ID to an IPv6 ACL.

Syntax

match ipv6 {**address** | **next-hop** | **route-source**} *access-list*

no match ipv6 {**address** | **next-hop** | **route-source**} *access-list*

Parameters

address	Specifies a network address to be matched against the contents of the specified IPv6 ACL(s).
next-hop	Specifies a next-hop address to be matched against the contents of the specified IPv6 ACL(s).
route-source	Specifies the source route ID to be matched against the contents of the specified IPv6 ACL(s).

access-list	Specifies the IPv6 ACL for which the specified command option will be matched against.

Defaults

None.

Mode

Route-map filter configuration.

Usage

Allows for up to **5** IPv6 access-lists to be associated with each address, next-hop or route-source entry.

Multiple match IPv6 entries may be configured, but a match of at least one ACL in each match entry must occur for a successful match for this sequence.

Apply the filter route-map using the **distribute-list route-map in** command in OSPF router configuration command mode to prevent route matches from entering the OSPF routing table.

The "no" form of this command removes the IP match for this route-map.

Example

This example shows how to match a packets next hop IP address to the contents of the acl1 access-list:

```
S Chassis(rw-config)->route-map filter ospf1
S Chassis(rw-config-fltr)->match ipv6 next-hop acl
```

match tag (filter)

Use this command to match a packet's OSPF tag or a range of OSPF tags.

Syntax

match tag {*tag* | **range** *min-tag max-tag*}

no match tag {*tag* | **range** *min-tag max-tag*}

Parameters

tag	Specifies the tag ID to match against the packet OSPF tag. Valid values are **1** - **4294967295**.
range *min-tag max-tag*	Specifies an OSPF tag ID range: • *min-tag* - Specifies the start of the OSPF tag range. • *max-tag* - Specifies the end of the OSPF tag range.

Defaults

None.

Mode

Route-map filter configuration.

Usage

OSPF tags can be assigned to external routes that are redistributed to OSPF. The permit or deny option can be assigned and matched against the packet OSPF tag using this command.

Apply the filter route-map using the **distribute-list route-map in** command in OSPF router configuration command mode to prevent route matches from entering the OSPF routing table.

The "no" form of this command removes the match between an OSPF tag and this route-map.

Examples

This example shows how to match a packet OSPF tag against tag ID **13456**:

```
S Chassis(rw-config)->route-map filter ospf1
S Chassis(rw-config-fltr)->match tag 13456
```

This example shows how to match a packet OSPF tag against tag ID range **13000** to **14000**:

```
S Chassis(rw-config)->route-map filter ospf1
S Chassis(rw-config-fltr)->match tag range 13000 14000
```

match metric (filter)

Use this command to match a route's metric cost value or a range of metric cost values.

Syntax

match metric {*cost* | **range** *min-cost max-cost*}

no match metric {*cost* | **range** *min-cost max-cost*}

Parameters

cost	Specifies a metric cost value to match against the metric cost value of the packet for this route filter. Valid values: **1** - **4294967295**.
range *min-cost max-cost*	Specifies a range of metric cost values to match against the metric cost value of the packet for this route filter: • *min-cost* - Specifies the start of the metric range. • *max-cost* - Specifies the end of the metric range. Valid values: **1** - **4294967295**.

Defaults

None.

Mode

Route-map filter configuration.

Usage

Apply the filter route-map using the **distribute-list route-map in** command in OSPF router configuration command mode to prevent route matches from entering the OSPF routing table.

The "no" form of this command removes the match between a metric cost and this route-map.

Examples

This example shows how to match a packet cost metric against the specified value of **100**:

```
S Chassis(rw-config)->route-map filter ospf1
S Chassis(rw--config-fltr)->match metric 100
```

This example shows how to match a packet cost metric against the range of metric values from **100** to **200**:

```
S Chassis(rw-config)->route-map filter ospf1
S Chassis(rw--config-fltr)->match metric range 100 200
```

match route-type (filter)

Use this command to match a route type.

Syntax

match route-type {**internal** | **external-t1** | **external-t2** | **nssa-external**}

no match interface {**internal** | **external-t1** | **external-t2** | **nssa-external**}

Parameters

internal	Specifies that the internal route type will be matched.
external-t1	Specifies that the external route type 1 will be matched.
external-t2	Specifies that the external route type 2 will be matched.
naas-external	Specifies that the external NSSA route type will be matched.

Defaults

None.

Mode

Route-map filter configuration.

Usage

OSPF route types can be internal routes, external Type 1 or Type 2 routes, or external NSSA routes. The route type specified is matched against the packet route type.

Apply the filter route-map using the **distribute-list route-map in** command in OSPF router configuration command mode to prevent route matches from entering the OSPF routing table.

The “no” form of this command removes the match between a VLAN and this route-map.

Example

This example shows how to match a packet internal route type:

```
S Chassis(rw-config)->route-map filter ospf1
S Chassis(rw--config-fltr)->match route-type internal
```

BGP Route-Map Commands

For information about...	Refer to page...
route-map bgp	85-31
match afi	85-32
match safi	85-33
match as-path	85-34
match community	85-35
match extended-community	85-36
match prefix-list	85-37
match med	85-38
set as	85-38
set as-path-limit	85-39
set community	85-40
set extended-community ip-route-target	85-41
set extended-community as-route-target	85-42
set extended-community ip-site-of-origin	85-43
set extended-community as-site-of-origin	85-44
set extended-community as4-route-target	85-45
set extended-community as4-site-of-origin	85-46
set extended-community ospf-domain-id	85-47
set extended-community ospf-router-id	85-48
set extended-community ospf-route-type	85-49
set local-preference	85-50
set med	85-51
set ip next-hop	85-51
set origin	85-52
set orf-association local	85-53
set weight	85-54
set flap-table	85-54

route-map bgp

Use this command to create a BGP route map and enter configuration mode for this route map.

Syntax

route-map bgp *name* [**permit** | **deny**] [*sequence-number*]

no route-map bgp *name* [**permit** | **deny**] [*sequence-number*]

Parameters

name	Specifies a name for this route-map.
permit	(Optional) Specifies that set command configurations will be applied on packets matching all match clauses.
deny	(Optional) Specifies that set command configurations should be skipped on packets matching all match clauses.
sequence-number	(Optional) Specifies the sequence for this route map in the route map list.

Defaults

- If **permit** or **deny** is not specified, the route-map defaults to permit.
- If *sequence-number* is not specified, **10** will be applied.

Mode

Global configuration.

Usage

Route-map names support up to 32 alphanumeric characters.

Each named named route-map can have one or more entries. Each BGP route-map entry is identified by a unique sequence-number. Each entry can be optionally configured as a permit or deny.

Executing the **route-map bgp** command enters BGP route map configuration command mode for the specified entry. Once in BGP route map configuration command mode, each entry can be configured for one or more clauses made up of **match** or **set** configurations.

The system supports 100 BGP route maps.

The system supports 1000 set or match clauses across all configured route-maps.

The **no route-map bgp** command removes the specified route-map list.

Example

This example shows how to create a BGP permit route map named **bgprm1** with a sequence value of 20:

```
S Chassis(su-config)->route-map bgp bgprm1 permit 20
S Chassis(su-config-route-map-bgp)->show route-map bgprm1
 route-map bgp bgprm1 permit 20
S Chassis(su-config-route-map-bgp)->
```

match afi

Use this command to match a packet against its Address Family Indicator (AFI) attribute.

Syntax

match afi {**ipv4** | **ipv6**}

no match afi {**ipv4** | **ipv6**}

Parameters

ipv4 | **ipv6**	Specifies the AFI attribute to match a packet against: • **ipv4** - The IPv4 AFI attribute • **ipv6** - The IPv6 AFI attribute

Defaults

None.

Mode

BGP route map configuration.

Usage

The **no match afi** command removes the specified AFI match clause from this route map.

Example

This example shows how to match a packet IPv6 AFI attribute for route map **bgprm1**:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->match afi ipv6
S Chassis(su-config-route-map-bgp)->show route-map bgprm1
 route-map bgp bgprm1 permit 10
  match afi ipv6
S Chassis(su-config-route-map-bgp)->
```

match safi

Use this command to match a packet against its Subsequent Address Family Indicator (SAFI) attribute.

Syntax

match safi {**unicast** | **multicast**}

no match safi {**unicast** | **multicast**}

Parameters

unicast | **multicast**	Specifies the SAFI attribute to match a packet against: • **unicast** - The unicast SAFI attribute • **multicast** - The multicast SAFI attribute

Defaults

None.

Mode

BGP route map configuration.

Usage

The **no match safi** command removes the specified SAFI match clause from this route map.

Example

This example shows how to match a packet unicast SAFI attribute for route map **bgprm1**:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->match safi unicast
S Chassis(su-config-route-map-bgp)->show route-map bgprm1
 route-map bgp bgprm1 permit 10
  match afi ipv6
  match safi unicast
S Chassis(su-config-route-map-bgp)->
```

match as-path

Use this command to match a packet against its AS path attribute.

Syntax

match as-path *as-path-string*

no match as-path *as-path-string*

Parameters

as-path-string	Specifies a string value to match against this packets AS path attribute.

Defaults

None.

Mode

BGP route map configuration.

Usage

The **match as-path** command supports the following regular expressions:

- **^** - start of string (eg ^200 matches any string starting with 200)
- **$** - end of string (eg 200$ matches any string ending with 200)
- **.** - matches any character (eg 2.0 match 200, 210, 220, etc)
- ***** - matches preceding element zero or more times (eg 22* matches 2, 22, 222, etc)
- **.*** - matches any character any number of times (i.e. this is a match all)
- **[]** - match a single character inside the brackets
- **[-]** - denotes a range (eg [0-9] matches any number from 0 to 9)
- **()** - a subexpression (eg (200:500) is treated as a single entity).
- **[^]** - match any single character not in brackets.

- **?** - match preceding element zero or one time.
- **+** - match preceding element one or more times.
- **|** - choice operator matches either expression before or after operator.

The **no match as-path** command removes the match clause from this route map.

Example

This example shows how to match a packet AS path attribute that starts with AS number **20313** and with the next AS number ending with **13**:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->match as-path ^20313.*13$
S Chassis(su-config-route-map-bgp)->show route-map bgprm1
 route-map bgp bgprm1 permit 10
  match afi ipv6
  match safi unicast
  match as-path "^20313_$13"
S Chassis(su-config-route-map-bgp)->
```

match community

Use this command to match a packet against the specified community name.

Syntax

match community *name*

no match community *name*

Parameters

name	Specifies the name of the community to match a packet against.

Defaults

None.

Mode

BGP route map configuration.

Usage

Regular expressions can be used to match routes with multiple community attributes. See the usage section of “match as-path” on page 85-34 for a listing of supported regular expressions.

The **no match community** command removes the match clause for the specified community.

Example

This example shows how to match a packet community to community 100 in AS 121:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
```

```
S Chassis(su-config-route-map-bgp)->match community 121:100
S Chassis(su-config-route-map-bgp)->show route-map bgprm1
 route-map bgp bgprm1 permit 10
  match afi ipv6
  match safi unicast
  match as-path "^20313_$13"
  match community "100"
```

match extended-community

Use this command to match a packet against the specified extended community.

Syntax

match extended-community *name*

no match extended-community *name*

Parameters

name	Specifies the extended community to match this packet against.

Defaults

None.

Mode

BGP route map configuration.

Usage

The **no match extended-community** command removes the match clause for the specified extended community.

Example

This example shows how to match a packet against the extended community route target attribute **000203E9000186A0**:

```
S Chassis(su)->show ip bgp 1.0.0.0/8 detail
Route status codes: > - active

    Network                Next Hop             Rib MED Local-Pref Origin AS Path
>   1.0.0.0/8              192.168.121.112       U   0      100    IGP     121 2013

Community attributes in route:
121:100

Extended Community attributes in route:
Route Target: 1001:100000 (0x000203E9000186A0)
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
```

```
S Chassis(su-config-route-map-bgp)->match extended-community 000203E9000186A0
S Chassis(su-config-route-map-bgp)->show route-map bgprm1
 route-map bgp bgprm1 permit 10
  match safi unicast
  match as-path "^20313_$13"
  match extended-community "000203E9000186A0"
S Chassis(su-config-route-map-bgp)->
```

match prefix-list

Use this command to match a packet against the specified prefix list.

Syntax

match prefix-list *prefix-list*

no match prefix-list *prefix-list*

Parameters

prefix-list	Specifies a prefix list to match this packet against.

Defaults

None.

Mode

BGP route map configuration.

Usage

Multiple prefix-list entries may be entered. At least one prefix-list entry must match for set clauses to be performed. This is an exception to the general route-map rule that all match clauses within a sequence must match for set clauses to be performed.

The no match prefix-list command removes the match clause for the specified prefix list.

Example

This example shows how to match a packet against the **permit100** prefix list:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->match prefix-list permit100
S Chassis(su-config-route-map-bgp)->show route-map bgprm1
 route-map bgp bgprm1 permit 10
  match prefix-list permit100
  match afi ipv6
  match safi unicast
  match as-path "^20313_$13"
  match community "100"
S Chassis(su-config-route-map-bgp)->
```

match med

Use this command to match a packet against the specified MED value.

Syntax

match med *value*

no match med *value*

Parameters

value	Specifies a MED value to match this packet against.

Defaults

None.

Mode

BGP route map configuration.

Usage

The **no match med** command removes the match clause for the specified MED value.

Example

This example shows how to match a packet against the MED value **50**:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->match med 50
S Chassis(su-config-route-map-bgp)->show route-map bgprm1
 route-map bgp bgprm1 permit 10
  match prefix-list permit100
  match afi ipv6
  match safi unicast
  match as-path "^20313_$13"
  match community "100"
  match med 50
S Chassis(su-config-route-map-bgp)->
```

set as

Use this command to specify the number of times to prepend the AS number of this router to the AS path for this route map context.

Syntax

set as *num*

no set as *num*

Parameters

num	Specifies the number of times to prepend the AS number of this router to the AS path.

Defaults

None.

Mode

BGP route map configuration.

Usage

The default value for the **set as** command is **0**. The AS path is a mandatory attribute in the route update. A single entry will be present if the **set as** command is set for either **0** or **1**.

Route selection takes into account the length of the AS path. Prepending additional AS numbers is a way of affecting route selection by lengthening the AS path.

The **no set as** command resets the number of times to prepend the AS number of this router to the AS path to the default value of **0** (a single entry is present in the route update).

Example

This example shows how to set the number of times to prepend this router's AS number to the AS path to 2, if all match clauses in the **bgprm1** route map match:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->set as 2
S Chassis(su-config-route-map-bgp)->
```

set as-path-limit

Use this command to sets a maximum length of the AS path attribute allowed when all match clauses match for this route map.

Syntax

set as-path-limit *limit*

no set as-path-limit *limit*

Parameters

limit	Specifies the maximum length of the AS path attribute that will be allowed. Valid values are **0** - **255**. Default Value is **0** (not set).

Defaults

None.

Mode

BGP route map configuration.

Usage

BGP allows attributes such as the AS path to be attached to every advertised IP prefix. The total length of BGP attributes attached to a single IP prefix can be very large. IP prefixes with an excessive amount of attribute data residing in the BGP table can result in significant memory utilization. The **set as-path-limit** command sets the maximum AS path length allowed when all match clauses match for this route map.

The default value for the **set as-path-limit** command is no AS path limit is set.

The **no set as-path-limit** command resets the allowed length of the AS path attribute when all match clauses match for this route map to the default value of no AS path length is set.

Example

This example shows how to set the maximum length of the AS path attribute when all match clauses in the **bgprm1** route map match to **20**:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->set as-path-limit 20
S Chassis(su-config-route-map-bgp)->
```

set community

Use this command to set the community when all match clauses match for this route map.

Syntax

set community {*as*:*community* | *defined-community*} {**remove-all** | **remove-specific** | **set-specific** | **remove-all-and-set**}

no set community {*as*:*community* | *defined-community*} {**remove-all** | **remove-specific** | **set-specific** | **remove-all-and-set**}

Parameters

as:*community*	Specifies the AS number, followed by a colon (**:**), followed by the community number to set if all match clauses match for this route map.
defined-community	There are predefined community values defined in RFC 1997 and RFC 3765 that are supported by the community field such as: • **NO_EXPORT** - Routes must not be advertised outside a BGP confederation boundary • **NO_ADVERTISE** - Routes must not be advertised to other BGP peers • **NO_EXPORT_SUBCONFED** - Routes must not be advertised to external BGP peers • **NO_PEER** - Routes must not be advertised across bilateral peer connections
remove-all	Specifies that the action is to remove all communities from the route.
remove-specific	Specifies that the action is to remove all matching communities from the route.
set-specific	Specifies that the action is to append the specified community to the route.

remove-all-and-set	Specifies that the action is to replace any existing communities in the route with the specified community

Defaults

None.

Mode

BGP route map configuration.

Usage

The default value for the **set community** command is no community is set.

The **no set community** command resets the community to no community is set when all match clauses match for this route map.

Examples

:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->match prefix-list permit100
S Chassis(su-config-route-map-bgp)->set community 100:100 set-specific
S Chassis(su-config-route-map-bgp)->
```

:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->match prefix-list permit200
S Chassis(su-config-route-map-bgp)->set community NO_PEER set-specific
S Chassis(su-config-route-map-bgp)->
```

set extended-community ip-route-target

Use this command to specify an action for an extended community IP route target when all match clauses match for this route map.

Syntax

set extended-community ip-route-target *set-value* {**remove-all** | **remove-specific** | **set-specific** | **remove-all-and-set**}

no set extended-community ip-route-target *set-value* {**remove-all** | **remove-specific** | **set-specific** | **remove-all-and-set**}

Parameters

set-value	Specifies that an IPv4 specific route-target extended community with a set value in the format: valid IPv4 address followed by a colon (:) followed by a number in the range **0** - **65535** as defined in RFC 4360.
remove-all	Specifies that the action is to remove all extended communities from the route.

remove-specific	Specifies that the action is to remove all matching extended communities from the route.
set-specific	Specifies that the action is to append the specified extended community to the route.
remove-all-and-set	Specifies that the action is to replace any existing extended communities in the route with the specified extended community

Defaults

None.

Mode

BGP route map configuration.

Usage

The route target community is an extended community that identifies one or more routers that may receive a set of routes carried by BGP. This is transitive across the AS boundary.

The **no set extended-community ip-route-target** command removes the specified IP route target set clause from the route map.

Example

This example shows how remove all matching extended communities from the IP route target **1.1.1.1:150** when all match clauses match for route map **bgprm1**:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->set extended-community ip-route-target
1.1.1.1:150 remove-specific
S Chassis(su-config-route-map-bgp)->
```

set extended-community as-route-target

Use this command to specify an action for an extended community AS route target when all match clauses match for this route map.

Syntax

set extended-community as-route-target *set-value* {**remove-all** | **remove-specific** | **set-specific** | **remove-all-and-set**}

no set extended-community as-route-target *set-value* {**remove-all** | **remove-specific** | **set-specific** | **remove-all-and-set**}

Parameters

as-route-target *set-value*	Specifies an AS route-target extended community with a set value in the format: valid AS number followed by a colon (:) followed by a number in the range **0** - **4294967295** as defined in RFC 4360.
remove-all	Specifies that the action is to remove all extended communities from the route for this match
remove-specific	Remove all matching extended communities from the route

set-specific	Append the specified extended community to the route
remove-all-and-set	Replace any existing extended communities in the route with the specified extended community

Defaults

None.

Mode

BGP route map configuration.

Usage

The default value for the **set extended-community as-route-target** command is no AS route target specified.

The **no set extended-community as-route-target** command removes the specified AS route target clause from the route map.

Example

This example shows how remove all matching extended communities from the AS route target **100:100** when all match clauses match for route map **bgprm1**:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->set extended-community as-route-target
100:100 remove-specific
S Chassis(su-config-route-map-bgp)->
```

set extended-community ip-site-of-origin

Use this command to specify an action for an extended community IP site of origin when all match clauses match for this route map.

Syntax

set extended-community ip-site-of-origin *set-value* {**remove-all** | **remove-specific** | **set-specific** | **remove-all-and-set**}

no set extended-community ip-site-of-origin *set-value* {**remove-all** | **remove-specific** | **set-specific** | **remove-all-and-set**}

Parameters

ip-site-of-origin *set-value*	Specifies that an IPv4 specific site-of-origin extended community with a set value in the format: valid IPv4 address followed by a colon (:) followed by a number in the range **0** - **65535** as defined in RFC 4360.
remove-all	Specifies that the action is to remove all extended communities from the route for this match
remove-specific	Remove all matching extended communities from the route
set-specific	Append the specified extended community to the route
remove-all-and-set	Replace any existing extended communities in the route with the specified extended community

Defaults

None.

Mode

BGP route map configuration.

Usage

The default value for the **set extended-community ip-site-of-origin** command is no IP site of origin specified.

The **no set extended-community ip-site-of-origin** command removes the specified IP site of origin clause from the route map.

Example

This example shows how remove all matching extended communities from the IP site of origin **1.1.1.1:150** when all match clauses match for route map **bgprm1**:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->set extended-community ip-site-of-origin
1.1.1.1:150 remove-specific
S Chassis(su-config-route-map-bgp)->
```

set extended-community as-site-of-origin

Use this command to specify an action for an extended community AS site of origin when all match clauses match for this route map.

Syntax

set extended-community as-site-of-origin *set-value* {**remove-all** | **remove-specific** | **set-specific** | **remove-all-and-set**}

no set extended-community as-site-of-origin *set-value* {**remove-all** | **remove-specific** | **set-specific** | **remove-all-and-set**}

Parameters

as-site-of-origin *set-value*	Specifies that a 2-octet AS site-of-origin extended community with a set value in the format: valid AS number followed by a colon (:) followed by a number in the range **0** - **4294967295** as defined in RFC 4360.
remove-all	Specifies that the action is to remove all extended communities from the route for this match
remove-specific	Remove all matching extended communities from the route
set-specific	Append the specified extended community to the route
remove-all-and-set	Replace any existing extended communities in the route with the specified extended community

Defaults

None.

Mode

BGP route map configuration.

Usage

The default value for the **set extended-community as-site-of-origin** command is no AS site of origin specified.

The **no set extended-community as-site-of-origin** command removes the specified AS site of origin clause from the route map.

Example

This example shows how remove all matching extended communities from the AS site of origin **100:150** when all match clauses match for route map **bgprm1**:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->set extended-community as-site-of-origin
100:150 remove-specific
S Chassis(su-config-route-map-bgp)->
```

set extended-community as4-route-target

Use this command to specify an action for an extended community AS4 route target when all match clauses match for this route map.

Syntax

set extended-community as4-route-target *set-value* {**remove-all** | **remove-specific** | **set-specific** | **remove-all-and-set**}

no set extended-community as4-route-target *set-value* {**remove-all** | **remove-specific** | **set-specific** | **remove-all-and-set**}

Parameters

as4-route-target *set-value*	Specifies that a 4-octet AS route-target extended community as defined in draft http://www.iana.org/assignments/bgp-extended-communities with a set value in the format: valid AS number followed by a colon (:) followed by a number in the range **0** - **65535**.
remove-all	Specifies that the action is to remove all extended communities from the route for this match
remove-specific	Remove all matching extended communities from the route
set-specific	Append the specified extended community to the route
remove-all-and-set	Replace any existing extended communities in the route with the specified extended community

Defaults

None.

Mode

BGP route map configuration.

Usage

The default value for the **set extended-community as4-route-target** command is no AS4 route target specified.

The **no set extended-community as4-route-target** command removes the specified AS4 route target clause from the route map.

Example

This example shows how remove all matching extended communities from the AS4 route target **100:150** when all match clauses match for route map **bgprm1**:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->set extended-community as4-route-target
100:150 remove-specific
S Chassis(su-config-route-map-bgp)->
```

set extended-community as4-site-of-origin

Use this command to specify an action for an extended community AS4 site of origin when all match clauses match for this route map.

Syntax

set extended-community as4-site-of-origin *set-value* {**remove-all** | **remove-specific** | **set-specific** | **remove-all-and-set**}

no set extended-community as4-site-of-origin *set-value* {**remove-all** | **remove-specific** | **set-specific** | **remove-all-and-set**}

Parameters

as4-site-of-origin *set-value*	Specifies that a 4-octet AS site-of-origin extended community with a set value in the format: valid AS number followed by a colon (:) followed by a number in the range **0** - **65535** as defined in RFC 4360.
remove-all	Specifies that the action is to remove all extended communities from the route for this match
remove-specific	Remove all matching extended communities from the route
set-specific	Append the specified extended community to the route
remove-all-and-set	Replace any existing extended communities in the route with the specified extended community

Defaults

None.

Mode

BGP route map configuration.

Usage

The default value for the **set extended-community as4-site-of-origin** command is no AS4 site of origin specified.

The **no set extended-community as4-site-of-origin** command removes the specified AS4 site of origin clause from the route map.

Example

This example shows how remove all matching extended communities from the AS4 site of origin **100:150** when all match clauses match for route map **bgprm1**:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->set extended-community as4 site-of-origin
100:150 remove-specific
S Chassis(su-config-route-map-bgp)->
```

set extended-community ospf-domain-id

Use this command to specify an action for an extended community OSPF domain ID when all match clauses match for this route map.

Syntax

set extended-community ospf-domain-id *set-value* {**remove-all** | **remove-specific** | **set-specific** | **remove-all-and-set**}

no set extended-community ospf-domain-id *set-value* {**remove-all** | **remove-specific** | **set-specific** | **remove-all-and-set**}

Parameters

ospf-domain-id *set-value*	Specifies that an OSPF domain identifier with a set value in the format: 4 byte dotted decimal as defined in RFC 4577.
remove-all	Specifies that the action is to remove all extended communities from the route for this match
remove-specific	Remove all matching extended communities from the route
set-specific	Append the specified extended community to the route
remove-all-and-set	Replace any existing extended communities in the route with the specified extended community

Defaults

None.

Mode

BGP route map configuration.

Usage

The default value for the **set extended-community ospf-domain-id** command is no OSPF domain ID specified.

The **no set extended-community ospf-domain-id** command removes the specified OSPF domain ID clause from the route map.

Example

This example shows how remove all matching extended communities from the route for OSPF Domain ID **1.1.1.1** when all match clauses match for route map **bgprm1**:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->set extended-community ospf-domain-id 1.1.1.1
remove-specific
S Chassis(su-config-route-map-bgp)->
```

set extended-community ospf-router-id

Use this command to specify an action for an extended community OSPF router ID when all match clauses match for this route map.

Syntax

set extended-community ospf-router-id *set-value* {**remove-all** | **remove-specific** | **set-specific** | **remove-all-and-set**}

no set extended-community ospf-router-id *set-value* {**remove-all** | **remove-specific** | **set-specific** | **remove-all-and-set**}

Parameters

ospf-router-id *set-value*	Specifies that an OSPF router ID with a set value in the format: 4 byte dotted decimal as defined in RFC 4577.
remove-all	Specifies that the action is to remove all extended communities from the route for this match
remove-specific	Remove all matching extended communities from the route
set-specific	Append the specified extended community to the route
remove-all-and-set	Replace any existing extended communities in the route with the specified extended community

Defaults

None.

Mode

BGP route map configuration.

Usage

The default value for the **set extended-community ospf-router-id** command is no OSPF router ID specified.

The **no set extended-community ospf-router-id** command removes the specified OSPF router ID clause from the route map.

Example

This example shows how remove all matching extended communities from the route for OSPF router ID **1.1.1.1** when all match clauses match for route map **bgprm1**:

```
S Chassis(su)->configure
```

```
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->set extended-community ospf-router-id 1.1.1.1
remove-specific
S Chassis(su-config-route-map-bgp)->
```

set extended-community ospf-route-type

Use this command to specify an action for an extended community OSPF route type when all match clauses match for this route map.

Syntax

set extended-community ospf-route-type *area* **route-type** *type* [**type2-metric**] {**remove-all** | **remove-specific** | **set-specific** | **remove-all-and-set**}

no set extended-community ospf-route-type *area* **route-type** *type* [**type2-metric**] {**remove-all** | **remove-specific** | **set-specific** | **remove-all-and-set**}

Parameters

area	Specifies an OSPF area.
route-type *type*	Specifies that an OSPF route-type extended community as defined in RFC 4577 will be set with one of the following values: • **1** or **2** - intra-area routes (depending on whether the route came from a type 1 or a type 2 LSA • **3** - inter-area routes • **5** - external routes (area number must be 0) • **7** - NSSA routes
type2-metric	(Optional) Specifies that the OSPF metric is a type-2 metric
remove-all	Specifies that the action is to remove all extended communities from the route for this match
remove-specific	Remove all matching extended communities from the route
set-specific	Append the specified extended community to the route
remove-all-and-set	Replace any existing extended communities in the route with the specified extended community

Defaults

If the **type2-metric** option is not specified, a type 1 metric is used.

Mode

BGP route map configuration.

Usage

The default value for the **set extended-community ospf-router-type** command is no OSPF router type specified.

The **no set extended-community ospf-router-type** command removes the specified OSPF router type clause from the route map.

Example

This example shows how remove all matching extended communities from the route for area **100** external OSPF routes when all match clauses match for route map **bgprm1**:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->set extended-community ospf-router-type 100
router-type 5 remove-specific
S Chassis(su-config-route-map-bgp)->
```

set local-preference

Use this command to specify the local preference to be set when all match clauses in the route map match.

Syntax

set local-preference *value*

no set local-preference *value*

Parameters

value	Specifies the local preference value for advertised routes to be set when all match clauses in the route map match. Valid values are **1** - **4294967295**.

Defaults

None.

Mode

BGP route map configuration.

Usage

The **no set local-preference** command removes the specified local preference set clause from the route map.

Example

This example shows how to set the local preference to 100, if all match clauses in the **bgprm1** route map match:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->set local-preference 100
S Chassis(su-config-route-map-bgp)->
```

set med

Use this command to specify the MED to be set when all match clauses in the route map match.

Syntax

set med *value*

no set med *value*

Parameters

value	Specifies the MED value to set if all match clauses for this route map match. Valid values are **0** - **4294967295**

Defaults

None.

Mode

BGP route map configuration.

Usage

The **no set med** command removes the specified MED clause from the route map.

Example

This example shows how to set the MED value to 50, if all match clauses in the **bgprm1** route map match:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->set med 50
S Chassis(su-config-route-map-bgp)->
```

set ip next-hop

Use this command to specify the next hop IP address to be set when all match clauses in the route map match.

Syntax

set ip next-hop *ip-address*

no set ip next-hop *ip-address*

Parameters

ip-address	Specifies the IP address to set for the next-hop if all match clauses match for this route map.

Defaults

None.

Mode

BGP route map configuration.

Usage

Entering match AFI and match SAFI entries are required before setting the next-hop behavior.

The **no set ip next-hop** command removes the set clause for the specified next-hop for this route map.

Example

This example shows how to set the next-hop to 10.10.10.10, if all match clauses in the **bgprm1** route map match:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->set ip next-hop 10.10.10.10
S Chassis(su-config-route-map-bgp)->
```

set origin

Use this command to specify the origin code to be set when all match clauses in the route map match.

Syntax

set origin *code*

no set origin *code*

Parameters

code	Specifies the origin attribute value to set if all match clauses in this route map match. Valid values are: **0** - IGP **1** - EGP **2** - Incomplete

Defaults

None.

Mode

BGP route map configuration.

Usage

The **no set origin** command removes the specified origin clause from the route map.

Example

This example shows how to set the origin attribute code to EGP, if all match clauses in the **bgprm1** route map match:

```
S Chassis(su)->configure
```

```
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->set origin 1
S Chassis(su-config-route-map-bgp)->
```

set orf-association local

Use this command to set local ORF association when all match clauses in the route map match.

Syntax

set orf-association local

no set orf-association local

Parameters

None.

Defaults

None.

Mode

BGP route map configuration.

Usage

The local ORF association advertises filtering information contained within this route map to peers that advertise the appropriate ORF support.

Local ORF association is specified on an inbound route map. Match clauses supported for local ORF association are prefix-list, community string, or extended community string.

The ORF capability is configured using the “bgp orf comm-filter” on page 72-12, “bgp orf extcomm-filter” on page 72-13, or “bgp orf prefix-filter” on page 72-14 commands. The ORF protocol is defined in RFC 5291.

Use the **set orf-association local** command to set local association as the behavior when all match clauses in the route map match.

The **no set orf-association** command removes the specified ORF association clause from the route map.

Example

This example shows how to set the ORF association to advertise matching routes to neighbors that support ORF, if all match clauses in the **bgprm1** route map match:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->set orf-association local
S Chassis(su-config-route-map-bgp)->
```

set weight

Use this command to specify the weight to be set when all match clauses in the route map match.

Syntax

set weight *value*

no set weight *value*

Parameters

value	Specifies the weight to set when all match clauses in the route map match. Valid values are from **1** - **2147483647**.

Defaults

None.

Mode

BGP route map configuration.

Usage

The **no set weight** command removes the specified weight clause from this route map.

Example

This example shows how to set the weight to 50, if all match clauses in the **bgprm1** route map match:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->set weight 50
S Chassis(su-config-route-map-bgp)->
```

set flap-table

Use this command to specify the flap table to be set when all match clauses in the inbound route map match.

Syntax

set flap-table *name*

no set flap-table *name*

Parameters

name	Specifies the name of the route flap table to set for matching routes when all match clauses in the route map match.

Defaults

None.

Mode

BGP route map configuration.

Usage

Setting the flap table is supported on inbound route maps.

The **no set flap-table** command removes the specified flap table clause from the route map.

Example

This example shows how to set the flap table to **flaptbl1**, if all match clauses in the **bgprm1** route map match:

```
S Chassis(su)->configure
S Chassis(su-config)->route-map bgp bgprm1 permit
S Chassis(su-config-route-map-bgp)->set flap-table flaptbl1
S Chassis(su-config-route-map-bgp)->
```

86

RADIUS Commands

This chapter describes the RADIUS set of commands and how to use them. For information about configuring RADIUS, refer to the "Authentication Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show radius	86-1
set radius	86-3
set radius mgmt attribute	86-4
set radius retries	86-5
set radius timeout	86-5
set radius server	86-6
set radius realm	86-6
clear radius	86-7
show radius accounting	86-7
set radius accounting	86-9
clear radius accounting	86-10

show radius

Use this command to display the current RADIUS client/server configuration.

Syntax

show radius [**state** | **retries** | **timeout** | **server** [*index* | **all** | **verbose**]]

Parameters

state	(Optional) Displays the RADIUS client's enable status.
retries	(Optional) Displays the number of retry attempts before the RADIUS server times out.
timeout	(Optional) Displays the maximum amount of time (in seconds) to establish contact with the RADIUS server before retry attempts begin.
server	(Optional) Displays RADIUS server configuration information.
index | **all**	(Optional) Displays configuration information for a specified server or all RADIUS servers.

verbose	(Optional) Displays detailed server information.

Defaults

If **verbose** is not specified, a standard level of configuration information will be displayed. If no other parameter is specified, all RADIUS configuration information will be displayed.

Mode

All command modes.

Example

This example shows how to display RADIUS configuration information:

```
S Chassis(rw)->show radius
 RADIUS state:    Enabled
 RADIUS retries:  2
 RADIUS timeout:  10 seconds
 RADIUS Attribute mgmt password type:  standard
 RADIUS Retransmission Algorithm:  standard
 RADIUS Server    IP Address                              Auth-Port  Realm-Type          Max-Sessions Status
 ---------------  --------------------------------------  ---------  ------------------  ------------ --------
 1                172.10.10.2                             1812       management-access   9216         Active
 2                172.10.3.50                             1812       any                 9216         Active
 3                172.10.3.100                            1812       management-access   9216         Active
 4                172.10.3.75                             1812       management-access   9216         Active
 5                172.10.3.51                             1812       management-access   9216         Active
```

Table 86-1 provides an explanation of the command output.

Table 86-1 show radius Output Details

Output...	What it displays...
RADIUS state	Whether the RADIUS client is **enabled** or **disabled**.
RADIUS retries	Number of retry attempts before the RADIUS server times out. The default value of **3** can be reset using the **set radius** command as described in “set radius” on page 86-3.
RADIUS timeout	Maximum amount of time (in seconds) to establish contact with the RADIUS server before retry attempts begin. The default value of **20** can be reset using the **set radius** command as described in “set radius” on page 86-3.
RADIUS Attribute mgmt password type	Specifies the RADIUS password management attribute sent to the server. Valid values are standard or MS-CHAPv2.
RADIUS Retransmission Algorithm	Specifies the RADIUS retransmission algorithm. Valid values are: standard, round-robin, or sticky-round-robin.
RADIUS Server	IP address, UDP authentication port, authentication realm type (**management**, **network** or **any**), and status (whether or not the RADIUS server has been configured).
IP Address	Specifies the server IP address.
Auth-Port	Specifies the port the server is authenticated on.
Realm-Type	Specifies whether the RADIUS server realm will be restricted to management or network access authentication, or whether it is allowed to perform all authentications.
Max-Sessions	Specifies the maximum number of server sessions supported.

Table 86-1 show radius Output Details (continued)

Output...	What it displays...
Status	Specifies server status.

This example shows how to display the verbose version of the show radius server command:

```
S Chassis(rw)->show radius server 1 verbose
 RADIUS Server    IP Address                              Auth-Port  Realm-Type          Max-Sessions Status
 ---------------  --------------------------------------  ---------  ------------------  ------------ --------
 1                172.10.3.50                             1812       any                 9216         Active

Current sticky sessions: 0

TRANSMISSIONS (0)
Requests:            0               Retransmissions:     0

RESPONSES (0)
Accepts:             0               Rejects:             0
Challenges:          0

TIMING TRANSACTIONS (0)
Pending Requests:    0               Client Timeouts:     0
Round Trip Time:     0           cs

ERRORS (0)
Malformed Responses: 0               Bad Authenticators:  0
Unknown Frame Types: 0               Frames Dropped:      0
```

Table 86-2 provides an explanation of the show radius server verbose command output.

Table 86-2 show radius server verbose Output Details

Output...	What it displays...
RADIUS Server	RADIUS server IP address, UDP authentication port, authentication realm type (**management**, **network** or **any**), and status (whether or not the RADIUS server has been configured).
Transmissions	Total transmissions requests and retransmissions.
Responses	Total response accepts, rejects, and challenges.
Timing Transactions	Total timing transaction pending requests, client timeouts, and round trip time.
Errors	Total malformed responses, bad authenticators, unknown frame types, and frames dropped.

set radius

Use this command to globally enable or disable RADIUS authentication on the device.

Syntax

set radius {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables the RADIUS client.

Defaults

None.

Mode

All command modes.

Usage

The RADIUS client can only be enabled on the switch once a RADIUS server is online, and its IP address(es) has been configured with the same password the RADIUS client will use.

Example

This example shows how to enable the RADIUS client on the switch:

```
S Chassis(rw)->set radius enable
```

set radius mgmt attribute

Use this command to configure RADIUS management attributes sent to the server.

Syntax

set radius mgmt attribute password {**standard** | **mschapv2**}

Parameters

password	Specifies the way the password attribute is sent to the server.
standard	Specifies that the standard user password attribute will be sent to the server. Standard is the default password attribute.
mschapv2	Specifies that the MS-CHAPv2 user password attribute will be sent to the server.

Defaults

None.

Mode

All command modes.

Usage

The MS-CHAPv2 password attribute must be set for IPsec to work. MS-CHAPv2 is the Microsoft Version 2 of the Challenge-Handshake Authentication Protocol (CHAP). MS-CHAPv2 provides mutual authentication between peers by piggybacking a peer challenge on the Response packet and an authenticator response on the Success packet.

Example

This example shows how to configure the switch to send the MS-CHAPv2 RADIUS password attribute to the server:

```
S Chassis(rw)->set radius mgmt attribute password mschapv2
```

set radius retries

Use this command to set the number of retry attempts before the RADIUS server times out.

Syntax

set radius retries *number-of-retries*

Parameters

number-of-retries	Specifies the number of retry attempts before the RADIUS server times out. Valid values are from **1** to **10**. Default is **3**.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set RADIUS retries to 10:

```
S Chassis(rw)->set radius retries 10
```

set radius timeout

Use this command to set the maximum amount of time allowed to establish contact with the RADIUS server before retry attempts begin.

Syntax

set radius timeout *timeout*

Parameters

timeout	Specifies the maximum amount of time (in seconds) to establish contact with the RADIUS server before retry attempts begin. Valid values are from **1** to **30**. Default is **20** seconds.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the RADIUS timeout to 5 seconds:

```
S Chassis(rw)->set radius timeout 5
```

set radius server

Use this command to configure a RADIUS authentication server.

Syntax

set radius server *index ip-address port* [*secret-value*]

Parameters

index ip-address port	Specifies the index number, IP address and the UDP authentication port for the RADIUS server.
secret-value	(Optional) Specifies an encryption key to be used for authentication between the RADIUS client and server.

Defaults

The S-Series supports up to 8 RADIUS servers.

If *secret-value* is not specified, none will be applied.

Mode

All command modes.

Examples

This example shows how to enable the RADIUS client for authenticating with RADIUS server 1 at IP address 10.1.6.203, UDP authentication port 1812, and an authentication password of "pwsecret." As previously noted, the "server secret" password entered here must match that already configured as the Read-Write (rw) password on the RADIUS server:

```
S Chassis(rw)->set radius server 1 10.1.6.203 1812 pwsecret
```

set radius realm

Use this command to configure a RADIUS realm.

Syntax

set radius realm {**management-access** | **network-access** | **any**} {*index* | **all**}

Parameters

management-access | **network-access** | **any**	(Optional) Restricts the RADIUS server realm to management or network access authentication, or allows it to perform all authentications.
index | **all**	Applies the server realm setting to a specific server or to all servers.

Defaults

If **realm** is not specified, **any** authentication will be allowed.

Mode

All command modes.

Examples

This example shows how to restrict all RADIUS servers to authenticate management access only

```
S Chassis(rw)->set radius realm management-access all
```

clear radius

Use this command to clear RADIUS server settings.

Syntax

clear radius [**state**] [**retries**] [**timeout**] [**server** [*index* | **all**] [**realm** {*index* | **all**}]

Parameters

state	(Optional) Resets the RADIUS client state to the default setting of disabled.
retries	(Optional) Resets the maximum number of attempts a user can contact the RADIUS server before timing out to **3**.
timeout	(Optional) Resets the maximum amount of time to establish contact with the RADIUS server before timing out to **20** seconds.
server	(Optional) Deletes server settings.
realm	(Optional) Resets the realm setting to allowing any authentication.
index | **all**	Resets settings for a specified server or all RADIUS servers.

Defaults

- If *index* or **all** is not specified for clearing RADIUS server, all RADIUS server settings will be deleted.
- If no other optional parameters are specified, all RADIUS settings will be cleared.

Mode

All command modes.

Examples

This example shows how to clear all settings on all RADIUS servers:

```
S Chassis(rw)->clear radius server all
```

This example shows how to reset the RADIUS timeout to the default value of 20 seconds:

```
S Chassis(rw)->clear radius timeout
```

show radius accounting

Use this command to display the RADIUS accounting configuration.

Syntax

show radius accounting [**updateinterval**] | [**intervalminimum**] | [**state**] | [**server** {*index* | **all** | **verbose**}]

Parameters

updateinterval	(Optional) Displays the number of seconds between each RADIUS accounting interim update (when accumulated accounting data is sent to the server for a session.)
intervalminimum	(Optional) Displays the minimum update interval setting. This controls the frequency of RADIUS accounting updates.
state	(Optional) Displays the RADIUS accounting enable state.
server *index* | **all**	(Optional) Displays one or all RADIUS accounting server configurations.
verbose	Displays detailed server information.

Defaults

If no parameters are specified, all RADIUS accounting configuration information will be displayed.

Mode

All command modes.

Usage

RADIUS accounting transmits accounting information between a network access server and a shared accounting server.

Example

This example shows how to display RADIUS accounting configuration information. In this case, RADIUS accounting is enabled and global default settings have not been changed. One server has been configured. The Extreme Networks S-Series device allows for up to 10 RADIUS accounting servers to be configured, with up to 2 active at any given time.

For details on enabling and configuring RADIUS accounting, refer to “set radius accounting” on page 86-9:

```
S Chassis(rw)->show radius accounting
Accounting state:              Enabled
Accounting update interval:    1800 secs
Accounting interval minimum:   600 secs

Server        Server          Acct
Index           IP            Port  Retries  Timeout     Status
-------------------------------------------------------------------
1           1.1.1.1           1236     2        5        Primary
```

set radius accounting

Use this command to configure RADIUS accounting.

Syntax

set radius accounting {[**enable**] [**disable**] [**intervalminimum** *value*] [**updateinterval** *value*] [**retries** *retries*] [**timeout** *timeout*] [**server** {*index* | **all**} *ip_address port server-secret*

Parameters

enable | **disable**	Enables or disables the RADIUS accounting client.
intervalminimum *value*	Sets the minimum interval at which RADIUS accounting will send interim updates. Valid values are **60** - **2147483647**.
updateinterval *value*	Sets the number of seconds between each RADIUS accounting interim update (when accumulated accounting data is sent to the server for a session.) Valid values are **0** - **2147483647**.
retries *retries*	Sets the maximum number of attempts to contact a specified RADIUS accounting server before timing out. Valid retry values are **0** - **20**.
timeout *timeout*	Sets the maximum amount of time (in seconds) to establish contact with a specified RADIUS accounting server before timing out. Valid timeout values are **2** - **10**.
index | **all**	Applies the settings to a specific RADIUS accounting server or to all. Valid index values: **1** - **2147483647**
server *ip_address port server-secret*	Specifies the accounting server's: • IP address • UDP authentication port (**0** - **65535)** • *server-secret* (Read-Write password to access this accounting server. If not specified, the device will prompt for this entry upon creating a server instance, as shown in the example below.)

Defaults

None.

Mode

All command modes.

Examples

This example shows how to enable the RADIUS accounting client for authenticating with the accounting server 1 at IP address 10.2.4.12, UDP authentication port 1800. As previously noted, the "server secret" password entered here must match that already configured as the Read-Write (rw) password on the RADIUS accounting server.

```
S Chassis(rw)->set radius accounting server 1 10.2.4.12 1800
 Server Secret:******
 Retype Server Secret:******
 Make This Entry Active (y/n)? y
 Warning: rfc2138 recommends secret minimum length of 16
```

This example shows how to set the RADIUS accounting timeout to 10 seconds on server 6:

```
S Chassis(rw)->set radius accounting timeout 10 6
```

This example shows how to set RADIUS accounting retries to 10 on server 6:

```
S Chassis(rw)->set radius accounting retries 10 6
```

clear radius accounting

Use this command to clear RADIUS accounting configuration settings.

Syntax

clear radius accounting {[**server**{*index* | **all**}] [**retries** {*index* | **all**}] [**timeout** {*index* | **all**}] [**intervalminimum**] [**updateinterval**]}

Parameters

server *index* | **all**	Clears the configuration on one or more accounting servers.
retries *index* | **all**	Resets the retries to the default value of 2 on one or more accounting servers.
timeout *index* | **all**	Resets the timeout to 5 seconds on one or more accounting servers.
intervalminimum	Resets the minimum interval to 600 seconds.
updateinterval	Resets the update interval to 1800 seconds.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the RADIUS accounting timeout to 5 seconds on all servers:

```
S Chassis(rw)->clear radius accounting timeout all
```

87

RFC 3580 Commands

This chapter describes the RFC 3580 set of commands and how to use them. For information about configuring RFC 3580, refer to the "Authentication Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show vlanauthorization	87-1
set vlanauthorization	87-2
clear vlanauthorization	87-2
set vlanauthorization port	87-3

show vlanauthorization

Use this command to display the VLAN Authorization settings.

Syntax

show vlanauthorization [*port-list*] | [**all**]

Parameters

port-list	(Optional) Displays the port(s) VLAN Authorization settings.
all	(Optional) Displays all port(s) VLAN Authorization settings.

Defaults

If no parameters are specified, all VLAN Authorization configuration information will be displayed.

Mode

All command modes.

Example

This example shows how to display VLAN Authorization configuration information for ports ge.1.1-3:

```
S Chassis(su)->show vlanauthorization ge.1.1-3
 VLAN Authorization Global Status:  enabled
```

```
 VLAN Authorization Table   :

 Port       Status       Admin Egress   Oper Egress    VLAN ID
-----------------------------------------------------------------
 ge.1.1     enabled      untagged       untagged       4094
 ge.1.2     disabled     untagged       untagged       none
 ge.1.3     enabled      untagged       untagged       unknown
```

set vlanauthorization

Use this command to set the VLAN Authorization state.

Syntax

set vlanauthorization {**enable** | **disable**}

Parameters

enable | **disable**	Enable or disable VLAN Authorization.

Defaults

None.

Mode

All command modes.

Example

This example shows how to enable VLAN Authorization:

```
S Chassis(su)->set vlanauthorization enable
```

clear vlanauthorization

Use this command to clear the VLAN Authorization attributes to the defaults.

Syntax

clear vlanauthorization {*port-list* | **all**}

Parameters

port-list	Clear port(s) attributes for VLAN Authorization.
all	Clear all VLAN Authorization to the defaults.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear VLAN Authorization for all ports:

```
S Chassis(su)->clear vlanauthorization all
```

This example shows how to clear VLAN Authorization for ports ge.1.1-4:

```
S Chassis(su)->clear vlanauthorization ge.1.1-4
```

set vlanauthorization port

Use this command to set the VLAN Authorization attributes.

Syntax

set vlanauthorization port *port-list* {**enable** | **disable** | **none** | **tagged** | **untagged** | **dynamic**}

Parameters

port *port-list*	Set port(s) attributes for VLAN Authorization.
enable | **disable**	Enable or disable port VLAN Authorization.
none | **tagged** | **untagged** | **dynamic**	**none** - No egress change will be made. **tagged** - Port added to egress. **untagged** - Port added to untagged egress. **dynamic** - Use information in authentication response.

Defaults

None.

Mode

All command modes.

Example

This example shows how to enable VLAN Authorization for port ge.1.1 for tagged packets:

```
S Chassis(su)->set vlanauthorization port ge.1.1 enable tagged
```

88

Quarantine Agent Authentication Commands

This chapter describes the quarantine agent authentication set of commands and how to use them. For information about configuring quarantine agent, refer to the "Authentication Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show quarantine-agent	88-1
set quarantine-agent	88-2
set quarantine-agent port	88-4
clear quarantine-agent	88-4
set quarantine accounting	88-5
set quarantine-agent port authallocated	88-5
set quarantine-agent port idle-timeout	88-6
set quarantine-agent port session-timeout	88-7

show quarantine-agent

Use this command to display all ports enabled for quarantine agent authentication and global quarantine agent authentication state or state and configuration information for the specified port.

Syntax

show quarantine-agent [**port** *port-string*]

Parameters

port *port-string*	(Optional) Specifies the port to display.

Defaults

If no port is specified, a list of all ports enabled for the quarantine agent displays.

Mode

All command modes.

Examples

This example shows how to display the global quarantine agent state on the device and all ports enabled for quarantine agent authentication:

```
S Chassis(rw)->show quarantine-agent
Quarantine Agent:                       enabled
Quarantine Agent Accounting:            disabled


Enabled Ports:
lag.0.4,6;ge.1.1-46;ge.2.1-47,101-112;tg.3.4-5,8;tg.5.1-15;ge.6.2-46;tg.6.101-10
4;ge.7.1-47
```

This example shows how to display quarantine agent state and configuration information for LAG **6**:

```
show quarantine-agent port lag.0.6
Quarantine Agent:                       enabled

Port            Port State      Session TO Idle TO    Allowed    Allocated
--------------- --------------- ---------- ---------- ---------- ----------
lag.0.6         enabled         0          0          9216       9216
S Chassis(rw)->
```

Table 88-1 provides an explanation of the command output.

Table 88-1 show quarantine-agent Output Display

Output...	What it displays...
Quarantine Agent	Quarantine agent state: enabled or disabled.
Enabled Ports	Displays all ports enabled for the quarantine agent.
Port State	Quarantine agent port state.
Session TO	Session time out value in seconds. If **0**, the quarantine agent session timeout value defaults to the MultiAuth global session time out value as configured by “set multiauth session-timeout” on page 96-14.
Idle TO	Idle time out value in seconds. If **0**, the quarantine agent session timeout value defaults to the MultiAuth global idle time out value as configured by “set multiauth idle-timeout” on page 96-11.
Allowed	Number of quarantine users allowed on the port.
Allocated	Number of quarantine users actually allocated on the port.

set quarantine-agent

Use this command to enable or disable the quarantine agent on the switch.

Syntax

set quarantine-agent {**enable** | **disable**}

Parameters

enable	Enables quarantine agent on the switch.
disable	Disables quarantine agent on the switch.

Defaults

Quarantine agent is disabled by default.

Mode

All command modes.

Usage

The quarantine agent must be enabled globally on the switch and locally on the port to be operational on the port. See "set quarantine-agent port" on page 88-4 for information on configuring quarantine agent authentication on the port.

The quarantine agent is a form of authentication that depends upon the existence of one or more configured quarantine policy rules, with each rule associated with a policy profile. To configure a policy rule as a quarantine profile, configure the policy rule with the desired traffic filtering specifications and specify the quarantine-profile rule option, indicating the associated policy profile. See "set policy rule" on page 43-23 for quarantine policy rule configuration details. See "set policy profile" on page 43-4 for policy profile configuration details.

Once one or more quarantine policy rules are configured and associated with a policy profile, the quarantine authentication agent behaves as any other MultiAuth authentication agent. By default, the quarantine agent has the highest configurable MultiAuth precedence. Static rules have the highest multiauth precedence. Static rule MultiAuth precedence is not configurable.

There are two circumstance for which actions specified in a quarantine policy are used:

- A quarantine policy rule is hit. In this case, the quarantine agent becomes one of the authentication agents from which the authentication provisioning result will be chosen based upon MultiAuth precedence. So long as the default precedence is not changed, if a quarantine policy rule hit occurs, quarantine agent authentication is selected and any actions configured in the policy profile taken.
- An anti-spoofing class threshold has been met for which a quarantine action has been configured (see "set antispoof class threshold-index" on page 95-9).

Should you configure quarantine agent authentication for a lower MultiAuth precedence using "set multiauth precedence" on page 96-5, if a non-quarantine authentication agent both returns a result and has the highest MultiAuth precedence, quarantine agent authentication will not be used in that context. If you change the quarantine agent MultiAuth precedence level to a lower precedence, make sure this is the behavior you want.

Examples

This example shows how to enable quarantine agent globally on the switch:

```
S Chassis(rw)->set quarantine-agent enable
```

set quarantine-agent port

Use this command to enable or disable the quarantine agent on the specified port.

Syntax

set quarantine-agent port {**enable** | **disable**} *port-string*

Parameters

enable	Enables quarantine agent on the specified port.
disable	Disables quarantine agent on the specified port.
port-string	Specifies the port to configure.

Defaults

Quarantine agent is disabled by default on all ports.

Mode

All command modes.

Usage

The quarantine agent must be enabled globally on the switch and locally on the port to be operational on the port. See "set quarantine-agent" on page 88-2 for information on global quarantine agent configuration. See the usage section of "set quarantine-agent" on page 88-2 for a description of quarantine agent dependencies.

Examples

This example shows how to enable quarantine agent on port **tg.1.1**:

```
S Chassis(rw)->set quarantine-agent port enable tg.1.1
```

clear quarantine-agent

Use this command to disable the quarantine agent globally or on the specified port.

Syntax

clear quarantine-agent {**all** | **port** *port-string*}

Parameters

all	Resets quarantine agent state globally on the switch to the default value of disabled.
port *port-string*	Specifies the port to reset quarantine agent configuration to default value of disabled.

Defaults

The MultiAuth quarantine agent is disabled by default both globally and on all ports.

Mode

All command modes.

Examples

This example shows how to disable the quarantine agent globally on the switch:

```
S Chassis(rw)->clear quarantine-agent all
```

This example shows how to disable the quarantine agent on port tg.1.1:

```
S Chassis(rw)->clear quarantine-agent port tg.1.1
```

set quarantine accounting

Use this command to enable or disable quarantine agent accounting.

Syntax

set quarantine accounting {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables quarantine agent accounting. Quarantine agent accounting is globally disabled by default.

Defaults

Quarantine accounting is disabled by default.

Mode

All command modes.

Usage

RADIUS accounting must be enabled using "set radius accounting" on page 86-9 for quarantine accounting to take place. RADIUS accounting is disabled by default. If RADIUS accounting is enabled, 802.1X accounting remains disabled by default.

Examples

This example shows how to enable quarantine accounting:

```
S Chassis(rw)->set quarantine accounting enable
```

set quarantine-agent port authallocated

Use this command to configure the maximum number of quarantine agent sessions allowed on the specified port.

Syntax

set quarantine-agent port authallocated *num-users port-string*

Parameters

num-users	Specifies the maximum number of quarantine agent sessions for the specified port. Valid values are **0** - maximum allowed users. The default value is the number of MultiAuth users per port set by "set multiauth port" on page 96-7.
port-string	Specifies the port to configure.

Defaults

The maximum number of quarantine agent sessions on a port defaults to the number of MultiAuth users per port set by "set multiauth port" on page 96-7. The number of MultiAuth users per port defaults to 8.

Mode

All command modes.

Usage

The maximum number of quarantine agent sessions supported on a port is device dependent. See the release notes for your device for the supported maximum number of authenticated users per port.

Use "clear quarantine-agent" on page 88-4, specifying the **port** option, to reset the maximum number of quarantine agent sessions on the port to the default value.

Examples

This example shows how to set the maximum number of quarantine agent authenticated sessions on port **tg.1.1** to **50**:

```
S Chassis(rw)->set quarantine port authallocated 50 tg.1.1
```

set quarantine-agent port idle-timeout

Use this command to configure the quarantine agent port idle timeout value in seconds.

Syntax

set quarantine-agent port idle-timeout *idle-timeout port-string*

Parameters

idle-timeout	Specifies the quarantine agent idle timeout in seconds for the specified port. Valid values are **0** - **65535**. Default value is **0** (specifies that the global MultiAuth idle timeout value as set by "set multiauth idle-timeout" on page 96-11 is used.
port-string	The port to configure.

Defaults

The quarantine agent port idle timeout defaults to **0**. A value of 0 specifies that the global MultiAuth idle timeout value as set by "set multiauth idle-timeout" on page 96-11 is used. The global MultiAuth idle timeout defaults to 300 seconds.

Mode

All command modes.

Usage

Use "clear quarantine-agent" on page 88-4, specifying the **port** option, to reset the port auto-tracking idle timeout to the default value.

Examples

This example shows how to set the quarantine agent idle timeout value for **port tg.1.1** to **350** seconds:

```
S Chassis(rw)->set quarantine-agent port idle-timeout 350 tg.1.1
```

set quarantine-agent port session-timeout

Use this command to configure the quarantine agent port session timeout value in seconds.

Syntax

set quarantine-agent port session-timeout *session-timeout port-string*

Parameters

session-timeout	Specifies the quarantine agent session timeout in seconds for the specified port. Valid values are **0** - **65535**. Default value is **0** (specifies that the global MultiAuth session timeout value as set by "set multiauth session-timeout" on page 96-14 is used.
port-string	The port to configure.

Defaults

The quarantine agent port session timeout defaults to **0**. A value of 0 specifies that the global MultiAuth session timeout value as set by "set multiauth session-timeout" on page 96-14 is used. The global MultiAuth session timeout defaults to **0** and specifies that no session timeout is applied to the port.

Mode

All command modes.

Usage

Use "clear quarantine-agent" on page 88-4, specifying the **port** option, to reset the quarantine agent session timeout on the port to the default value.

Examples

This example shows how to set the quarantine agent session timeout value for **port tg.1.1** to **600** seconds:

```
S Chassis(rw)->set quarantine port session-timeout 600 tg.1.1
```

89

802.1X Authentication Commands

This chapter describes the 802.1x authentication set of commands and how to use them. For information about configuring 802.1x, refer to the "Authentication Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show dot1x	89-1
show dot1x auth-config	89-3
set dot1x	89-5
set dot1x auth-config	89-6
clear dot1x auth-config	89-7

show dot1x

Use this command to display 802.1X status, diagnostics, statistics, and reauthentication or initialization control information for one or more ports.

Syntax

```
show dot1x [access-entity | auth-diag | auth-session-stats | auth-stats [all] |
[mac {all | mac}] | [port [init | reauth] [port-string]] | user {name | all}]]
[port-string] [index index-list]
```

Parameters

access-entity	(Optional) Displays access entity information.
auth-diag	(Optional) Displays authentication diagnostics information.
auth-session-stats	(Optional) Displays authentication session statistics.
auth-stats	(Optional) Displays authentication statistics.
all	(Optional) Displays inactive and active authentication entries.
mac all *mac*	(Optional) Displays information for one or all MAC addresses.
index *index-list*	(Optional) Displays information for one or more access entities. Valid values are 0 - 2047.
port init | **reauth**	(Optional) Displays the status of port initialization and reauthentication control.
port-string	(Optional) Displays information for specific port(s).

user *name* | **all**	(Optional) Displays information for a specific user or all users. Valid values are a full or partial user name. The first 8 characters are compared.

Defaults

- If no parameters are specified, 802.1X status will be displayed.
- If **all** is not specified, only active entries will be displayed.
- If *index* is not specified, information for all access entities will be displayed.
- If *port-string* is not specified, information for all ports will be displayed.

Mode

All command modes.

Examples

This example shows how to display 802.1X status:

```
S Chassis(rw)->show dot1x
DOT1X is disabled.
S Chassis(rw)->
```

This example shows how to display authentication diagnostics information for ge.1.1:

```
S Chassis(rw)->show dot1x auth-diag ge.1.1

 Port: 1     Auth-Diag:
 Enter Connecting:                    0
 EAP Logoffs While Connecting:        0
 Enter Authenticating:                0
 Success While Authenticating:        0
 Timeouts While Authenticating:       0
 Fail While Authenticating:           0
 ReAuths While Authenticating:        0
 EAP Starts While Authenticating:     0
 EAP Logoff While Authenticating:     0
 ReAuths While Authenticated:         0
 EAP Starts While Authenticated:      0
 EAP Logoff While Authenticated:      0
 Backend Responses:                   0
 Backend Access Challenges:           0
 Backend Other Requests To Supp:      0
 Backend NonNak Responses From Supp:  0
 Backend Auth Successes:              0
 Backend Auth Fails:                  0
```

This example shows how to display authentication session statistics for ge.1.1:

```
S Chassis(rw)->show dot1x auth-session-stats ge.1.1
```

```
Port: 1     Auth-Session-Stats:
Session Octets Rx:        0
Session Octets Tx:        0
Session Frames Rx:        0
Session Frames Tx:        0
Session Id:               (1, 00-00-00-00-00-00)
Session Authentic Method: Remote Auth Server
Session Time:             0 secs
Session Terminate Cause:  Port Failure
Session UserName:
```

This example shows how to display authentication statistics for ge.1.1:

```
S Chassis(rw)->show dot1x auth-stats ge.1.1

Port: 1     Auth-Stats:
EAPOL Frames Rx:            0
EAPOL Frames Tx:            0
EAPOL Start Frames Rx:      0
EAPOL Logoff Frames Rx:     0
EAPOL RespId Frames Rx:     0
EAPOL Resp Frames Rx:       0
EAPOL ReqId Frames Tx:      0
EAPOL Req Frames Tx:        0
Invalid EAPOL Frames Rx:    0
EAP Length Error Frames Rx: 0
Last EAPOL Frame Version:   0
Last EAPOL Frame Source:    0:0:0:0:0:0
```

show dot1x auth-config

Use this command to display 802.1X authentication configuration settings for one or more ports.

Syntax

show dot1x auth-config [**authcontrolled-portcontrol**] [**keytxenabled**] [**maxreq**] [**quietperiod**] [**reauthenabled**] [**reauthperiod**] [**servertimeout**] [**supptimeout**] [**txperiod**] [*port-string*]

Parameters

authcontrolled-portcontrol	(Optional) Displays the current value of the controlled Port control parameter for the Port.
keytxenabled	(Optional) Displays the state of 802.1X key transmission currently in use by the authenticator PAE state machine.
maxreq	(Optional) Displays the value set for maximum requests currently in use by the backend authentication state machine.
quietperiod	(Optional) Displays the value set for quiet period currently in use by the authenticator PAE state machine.

reauthenabled	(Optional) Displays the state of reauthentication control used by the Reauthentication Timer state machine.
reauthperiod	(Optional) Displays the value, in seconds, set for the reauthentication period used by the reauthentication timer state machine.
servertimeout	(Optional) Displays the server timeout value, in seconds, currently in use by the backend authentication state machine.
supptimeout	(Optional) Displays the authentication supplicant timeout value, in seconds, currently in use by the backend authentication state machine.
txperiod	(Optional) Displays the transmission period value, in seconds, currently in use by the authenticator PAE state machine.
port-string	(Optional) Limits the display of desired information information to specific port(s).

Defaults

- If no parameters are specified, all 802.1X settings will be displayed.
- If *port-string* is not specified, information for all ports will be displayed.

Mode

All command modes.

Examples

This example shows how to display the EAPOL port control mode for ge.1.1:

```
S Chassis(rw)->show dot1x auth-config authcontrolled-portcontrol ge.1.1
Port: ge.1.1     Auth controlled port control          : Auto
```

This example shows how to display the 802.1X auth-config settings for ge.1.1:

```
S Chassis(rw)->show dot1x auth-config ge.1.1

Port: ge.1.1     Auth-Config:
PAE state                             : Initialize
Backend auth State                    : Initialize
Admin controlled directions           : Both
Oper controlled directions            : Both
Auth controlled port status           : Unauthorized
Auth controlled port control          : Auto
Quiet period                          : 60 seconds
Tx period                             : 30 seconds
Supp Timeout                          : 30 seconds
Server Timeout                        : 30 seconds
Max requests                          : 2
Reauthentication period               : 3600 seconds
Reauthentication enabled              : FALSE
Key tx enabled                        : FALSE
```

This example shows how to display the 802.1X auth-config quietperiod setting for ge.1.1

```
S Chassis(su)->show dot1x auth-config quietperiod ge.1.1
```

```
Port: ge.1.1     Quiet period                          : 60 seconds
```

set dot1x

Use this command to enable or disable 802.1X authentication, to reauthenticate one or more access entities, or to reinitialize one or more supplicants.

Syntax

set dot1x {[**enable** | **disable**] | [{**init** | **reauth**} [*port-string*] [**index** *index-list*]]}

Parameters

enable | **disable**	Enables or disables 802.1X authentication. 802.1X authentication is globally disabled by default and enabled on all ports by default.
init | **reauth**	Reinitializes one or more access entities or reauthenticates one or more supplicants.
port-string	(Optional) Specifies the port(s) to reinitialize or reauthenticate.
index *index-list*	(Optional) Specifies one or more access entities on which to enable initialization or reauthentication control. Valid values are **0** - **2047**.

Defaults

If *port-string* not specified, the reinitialization or reauthentication setting will be applied to all ports.

If *index* is not specified, all access entities will be affected.

Mode

All command modes.

Examples

This example shows how to enable 802.1X globally:

```
S Chassis(rw)->set dot1x enable
```

This example shows how to disable 802.1X on VLAN 1:

```
S Chassis(rw)->configure terminal
S Chassis(rw)->configure terminal
S Chassis(rw-config)->interface vlan 1
S Chassis(rw-config-intf-vlan.0.1)->set dot1x disable
```

This example shows how to reinitialize ge.2.24:

```
S Chassis(rw)->set dot1x init ge.2.24
```

set dot1x auth-config

Use this command to configure 802.1X authentication.

Syntax

```
set dot1x auth-config {[authcontrolled-portcontrol {auto | forced-auth |
forced-unauth}] [keytxenabled{false | true}] [maxreq value] [quietperiod value]
[reauthenabled {false | true}] [reauthperiod value] [servertimeout timeout]
[supptimeout timeout] [txperiod value]} [port-string]
```

Parameters

authcontrolled-portcontrol auto | **forced-auth** | **forced-unauth**	Specifies the EAPOL port control mode as: • **auto** - Auto authorization mode (default). The Extreme Networks system will only forward frames received on a port which are considered authenticated according to the state of the corresponding access entity. • **forced-auth** - Forced authorized mode, which effectively disables 802.1X authentication on the port, and allows all frames received on the port to be forwarded. • **forced-unauth** - Forced unauthorized mode, which effectively disables 802.1X authentication on the port. When 802.1X is the only active authentication agent on a given port, this setting means all frames received will be dropped.
keytxenabled false | **true**	Enables (**true**) or disables (**false**) 802.1X key transmission by the authenticator PAE state machine. Default value is **false**.
maxreq *value*	Specifies the maximum number of authentication requests allowed by the backend authentication state machine. Valid values are **1** - **10**. The default value is **2**.
quietperiod *value*	Specifies the time (in seconds) following a failed authentication before another attempt can be made by the authenticator PAE state machine. Valid values are **0** - **65535** seconds. The default value is **60** seconds.
reauthenabled false | **true**	Enables (**true**) or disables (**false**) reauthentication control of the reauthentication timer state machine. The default value is **false**.
reauthperiod *value*	Specifies the time lapse (in seconds) between attempts by the reauthentication timer state machine to reauthenticate a port. Valid values are **0** - **65535**. The default value is **3600**.
servertimeout *timeout*	Specifies a timeout period (in seconds) for the authentication server, used by the backend authentication state machine. Valid values are **1** - **300**. The default Value is **30** seconds.
supptimeout *timeout*	Specifies a timeout period (in seconds) for the authentication supplicant used by the backend authentication state machine. Valid values are **1** - **300**. The default value is **30** seconds.
txperiod *value*	Specifies the period (in seconds) which passes between authenticator PAE state machine EAP transmissions. Valid values are **1** - **65535**. The default value is **30** seconds.
port-string	(Optional) Limits the configuration of desired settings to specified port(s).

Defaults

If *port-string* is not specified, authentication parameters will be set on all ports

Mode

All command modes.

Examples

This example shows how to set EAPOL port control to forced authorized mode on ports ge.1.1-5, which disables authentication on these ports:

```
S Chassis(rw)->set dot1x auth-config authcontrolled-portcontrol forced-auth
ge.1.1-5
```

This example shows how to enable reauthentication control on ports ge.1.1-3:

```
S Chassis(rw)->set dot1x auth-config reathenabled true ge.1.1-3
```

This example shows how to set the 802.1X quiet period to 120 seconds on ports ge.1.1-3:

```
S Chassis(rw)->set dot1x auth-config quietperiod 120 ge.1.1-3
```

clear dot1x auth-config

Use this command to reset 802.1X authentication parameters to default values on one or more ports.

Syntax

clear dot1x auth-config [**authcontrolled-portcontrol**] [**keytxenabled**] [**maxreq**] [**quietperiod**] [**reauthenabled**] [**reauthperiod**] [**servertimeout**] [**supptimeout**] [**txperiod**] [*port-string*]

Parameters

authcontrolled-portcontrol	(Optional) Resets the 802.1X port control mode to **auto**.
keytxenabled	(Optional) Resets the 802.1X key transmission state to disabled (**false**).
maxreq	(Optional) Resets the maximum requests value to **2**.
quietperiod	(Optional) Resets the quiet period value to **60** seconds.
reauthenabled	(Optional) Resets the reauthentication control state to disabled (**false**).
reauthperiod	(Optional) Resets the reauthentication period value to 3**600** seconds.
servertimeout	(Optional) Resets the server timeout value to **30** seconds.
supptimeout	(Optional) Resets the authentication supplicant timeout value to **30** seconds.
txperiod	(Optional) Resets the transmission period value to **30** seconds.
port-string	(Optional) Resets settings on specific port(s).

Defaults

- If no parameters are specified, all authentication parameters will be reset.
- If *port-string* is not specified, parameters will be set on all ports.

Mode

All command modes.

Examples

This example shows how to reset the 802.1X port control mode to auto on all ports:

```
S Chassis(rw)->clear dot1x auth-config authcontrolled-portcontrol
```

This example shows how to reset reauthentication control to disabled on ports ge.1.1-3:

```
S Chassis(rw)->clear dot1x auth-config reauthenabled ge.1.1-3
```

This example shows how to reset the 802.1X quiet period to 60 seconds on ports ge.1.1-3:

```
S Chassis(rw)->clear dot1x auth-config quietperiod ge.1.1-3
```

90

Port Web Authentication (PWA) Commands

This chapter describes the Port Web Authentication (PWA) set of commands and how to use them. For information about configuring PWA, refer to the "Authentication Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show pwa	90-2
set pwa	90-4
set pwa hostname	90-4
clear pwa hostname	90-5
show pwa banner	90-5
set pwa banner	90-6
clear pwa banner	90-6
set pwa displaylogo	90-7
set pwa redirecttime	90-7
clear pwa redirecttime	90-8
set pwa ipaddress	90-8
clear pwa ipaddress	90-9
set pwa protocol	90-9
clear pwa protocol	90-10
set pwa enhancedmode	90-10
set pwa guestname	90-11
clear pwa guestname	90-11
set pwa guestpassword	90-12
set pwa gueststatus	90-12
set pwa initialize	90-13
set pwa quietperiod	90-14
clear pwa quietperiod	90-14
set pwa maxrequest	90-15
clear pwa maxrequest	90-15
set pwa portcontrol	90-16

For information about...	Refer to page...
show pwa session	90-17
show pwa summary	90-17

show pwa

Use this command to display port web authentication information for one or more ports.

Syntax

show pwa [*port-string*]

Parameters

port-string	(Optional) Displays PWA information for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, PWA information will be displayed for all ports.

Mode

All command modes.

Examples

This example shows how to display PWA information for port ge.1.1:

```
S Chassis(su)->show pwa ge.1.1
PWA Status                   - disabled
PWA Hostname                 -
PWA IP Address               - 0.0.0.0
PWA Protocol                 - PAP
PWA Enhanced Mode            - disabled
PWA Logo                     - enabled
PWA Guest Networking Status - disabled
PWA Guest Name               - guest
PWA Redirect Time            - 5

Port     Mode              AuthStatus      QuietPeriod  MaxReq
-------- ----------------  --------------  -----------  -----------
ge.1.1   disabled           disconnected    60           16
```

Table 90-1 provides an explanation of the command output.

Table 90-1 show pwa Output Details

Output...	What it displays...
PWA Status	Whether or not port web authentication is enabled or disabled. Default state of disabled can be changed using the **set pwa** command as described in "set pwa" on page 90-4.
PWA Hostname	Hostname of the authenticating host for this PWA session. Set using the **set pwa hostname** command as described in "set pwa hostname" on page 90-4.
PWA IP Address	IP address of the end station from which PWA will prevent network access until the user is authenticated. Set using the **set pwa ipaddress** command as described in "set pwa ipaddress" on page 90-8.
PWA Protocol	Whether PWA protocol is CHAP or PAP. Default setting of PAP can be changed using the set pwa protocol command as described in "set pwa protocol" on page 90-9.
PWA Enhanced Mode	Whether PWA enhanced mode is enabled or disabled. Default state of disabled can be changed using the **set pwa enhancedmode** command as described in "set pwa enhancedmode" on page 90-10.
PWA Logo	Whether the Extreme Networks logo will be displayed or hidden at user login. Default state of enabled (displayed) can be changed using the **set pwa displaylogo** command as described in "set pwa displaylogo" on page 90-7.
PWA Guest Networking Status	Whether PWA guest user status is disabled or enabled with RADIUS or no authentication. Default state of disabled can be changed using the **set pwa gueststatus** command as described in "set pwa gueststatus" on page 90-12.
PWA Guest Name	Guest user name for PWA enhanced mode networking. Default value of "guest" can be changed using the **set pwa guestname** command as described in "set pwa guestname" on page 90-11.
PWA Guest Password	Guest user's password. Default value of an empty string can be changed using the **set pwa guestpassword** command as described in "set pwa guestpassword" on page 90-12.
PWA Redirect Time	Time in seconds after login success before the user is redirected to the PWA home page. Default of 5 can be reset using the **set pwa redirecttime** command as described in "set pwa redirecttime" on page 90-7.
Port	PWA port designation.
Mode	PWA port control mode.
Auth Status	Whether or not the port state is disconnected, authenticating authenticated, or held (authentication has failed).
Quiet Period	Amount of time a port will be in the held state after a user unsuccessfully attempts to log on to the network. Default value of 60 can be changed using the **set pwa quietperiod** command as described in "set pwa quietperiod" on page 90-14.
MaxReq	Maximum number of log on attempts allowed before transitioning the port to a held state. Default value of 2 can be changed using the **set pwa maxrequests** command as described in "set pwa maxrequest" on page 90-15.

set pwa

Use this command to enable or disable port web authentication.

Syntax

set pwa {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables port web authentication.

Defaults

None.

Mode

All command modes.

Example

This example shows how to enable port web authentication:

```
S Chassis(rw)->set pwa enable
```

set pwa hostname

Use this command to set a port web authentication host name.

Syntax

set pwa hostname *name*

Parameters

name	Specifies a name for accessing the PWA login page.

Defaults

None.

Mode

All command modes.

Usage

This is a URL for accessing the PWA login page.

Example

This example shows how to set the PWA host name to “pwahost”:

```
S Chassis(rw)->set pwa hostname pwahost
```

clear pwa hostname

Use this command to clear the port web authentication host name.

Syntax

clear pwa hostname

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear the PWA host name:

```
S Chassis(rw)->clear pwa hostname
```

show pwa banner

Use this command to display the port web authentication login banner string.

Syntax

show pwa banner

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display the PWA login banner:

```
S Chassis(rw)->show pwa banner
Welcome to Enterprise Services Homepage
```

set pwa banner

Use this command to configure a string to be displayed as the PWA login banner.

Syntax

set pwa banner *string*

Parameters

string	Specifies the PWA login banner.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the PWA login banner to “Welcome to Extreme Networks”:

```
S Chassis(rw)->set pwa banner Welcome to Enterprise Services Homepage
```

clear pwa banner

Use this command to reset the PWA login banner to a blank string.

Syntax

clear pwa banner

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the PWA login banner to a blank string

```
S Chassis(rw)->clear pwa banner
S Chassis(rw)->show pwa banner
S Chassis(rw)->
```

set pwa displaylogo

Use this command to set the display options for the Extreme Networks logo.

Syntax

set pwa displaylogo {**display** | **hide**}

Parameters

display | **hide**	Displays or hides the Extreme Networks logo when the PWA website displays.

Defaults

None.

Mode

All command modes.

Example

This example shows how to hide the Extreme Networks logo:

```
S Chassis(rw)->set pwa displaylogo hide
```

set pwa redirecttime

Use this command to set the PWA login success page redirect time.

Syntax

set pwa redirecttime *time*

Parameters

time	Specifies the number of seconds before the user will be redirected to the PWA home page after successful login. Valid values are **0** - **120**.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the PWA redirect time to 10 seconds:

```
S Chassis(rw)->set pwa redirecttime 10
```

clear pwa redirecttime

Use this command to reset the PWA login success page redirect time to the default value.

Syntax

clear pwa redirecttime

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to reset the PWA redirect time to the default value:

```
S Chassis(rw)->clear pwa redirecttime
S Chassis(rw)->show pwa ge.1.1
PWA Status                  - disabled
.
.
.

PWA Redirect Time           - 5
```

set pwa ipaddress

Use this command to set the PWA IP address.

Syntax

set pwa ipaddress *ip-address*

Parameters

ip-address	Specifies a globally unique IP address. This same value must be configured into every authenticating switch in the domain.

Defaults

None.

Mode

All command modes.

Usage

This is the IP address of the end station from which PWA will prevent network access until the user is authenticated.

Example

This example shows how to set a PWA IP address of 1.2.3.4:

```
S Chassis(rw)->set pwa ipaddress 1.2.3.4
```

clear pwa ipaddress

Use this command to clear the port web authentication IP address.

Syntax

clear pwa ipaddress

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear the PWA host name:

```
S Chassis(rw)->clear pwa ipaddress
```

set pwa protocol

Use this command to set the port web authentication protocol.

Syntax

set pwa protocol {**chap** | **pap**}

Parameters

chap | **pap**	Sets the PWA protocol to: • CHAP (PPP Challenge Handshake Protocol) - encrypts the username and password between the end-station and the switch port. • PAP (Password Authentication Protocol) - does not provide any encryption between the end-station the switch port. (default)

Defaults

None.

Mode

All command modes.

Example

This example shows how to set a the PWA protocol to CHAP:

```
S Chassis(rw)->set pwa protocol chap
```

clear pwa protocol

Use this command to reset the PWA protocol to the default value.

Syntax

clear pwa protocol

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear the PWA protocol:

```
S Chassis(rw)->clear pwa protocol
S Chassis(rw)->
```

set pwa enhancedmode

Use this command to enable or disable PWA enhanced mode.

Syntax

set pwa enhancedmode {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables PWA enhanced mode.

Defaults

None.

Mode

All command modes.

Usage

When enabled, users on unauthenticated PWA ports can type any URL into a browser and be presented the PWA login page on their initial web access. They will also be granted guest networking privileges.

Example

This example shows how to enable PWA enhanced mode:

```
S Chassis(rw)->set pwa enhancedmode enable
```

set pwa guestname

Use this command to set a guest user name for PWA enhanced mode networking.

Syntax

set pwa guestname *name*

Parameters

name	Specifies a guest user name. Default value is “guest”.

Defaults

None.

Mode

All command modes.

Usage

When enhanced mode is enabled (as described in “set pwa enhancedmode” on page 90-10), PWA will use this name to grant network access to guests without established login names and passwords.

Example

This example shows how to set the PWA guest user name to “guestuser”:

```
S Chassis(rw)->set pwa guestname guestuser
```

clear pwa guestname

Use this command to clear the PWA guest user name.

Syntax

clear pwa guestname

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear the PWA guest user name

```
S Chassis(rw)->clear pwa guestname
```

set pwa guestpassword

Use this command to set the guest user password for PWA networking.

Syntax

set pwa guestpassword *password*

Parameters

password	Specifies a guest password. Default value is <return>.

Defaults

None.

Mode

All command modes.

Usage

When enhanced mode is enabled, (as described in "set pwa enhancedmode" on page 90-10) PWA will use this password and the guest user name to grant network access to guests without established login names and passwords.

Example

This example shows how to set the PWA guest user password name:

```
S Chassis(rw)->set pwa guestpassword
Guest Password: *********
Retype Guest Password: *********
```

set pwa gueststatus

Use this command to enable or disable guest networking for port web authentication.

Syntax

set pwa gueststatus {**authnone** | **authradius** | **disable**}

Parameters

authnone	Enables guest networking with no authentication method.
authradius	Enables guest networking with RADIUS authentication. Upon successful authentication from RADIUS, PWA will apply the policy returned from RADIUS to the PWA port.
disable	Disables guest networking.

Defaults

None.

Mode

All command modes.

Usage

When enhanced mode is enabled (as described in "set pwa enhancedmode" on page 90-10), PWA will use a guest password and guest user name to grant network access with default policy privileges to users without established login names and passwords.

Example

This example shows how to enable PWA guest networking with RADIUS authentication:

```
S Chassis(rw)->set pwa guestnetworking authradius
```

set pwa initialize

Use this command to initialize a PWA port to its default unauthenticated state.

Syntax

set pwa initialize [*port-string*]

Parameters

port-string	(Optional) Initializes specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, all ports will be initialized.

Mode

All command modes.

Example

This example shows how to initialize ports ge.1.5-7:

```
S Chassis(rw)->set pwa initialize ge.1.5-7
```

set pwa quietperiod

Use this command to set the amount of time a port will remain in the held state after a user unsuccessfully attempts to log on to the network.

Syntax

set pwa quietperiod *time* [*port-string*]

Parameters

time	Specifies quiet time in seconds. Valid values are **0** - **2147483647**. Default: 60 seconds
port-string	(Optional) Sets the quiet period for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, quiet period will be set for all ports.

Mode

All command modes.

Example

This example shows how to set the PWA quiet period to 30 seconds for ports ge.1.5-7:

```
S Chassis(rw)->set pwa quietperiod 30 ge.1.5-7
```

clear pwa quietperiod

Use this command to reset the quiet period for one or all ports.

Syntax

clear pwa maxrequest [*port-string*]

Parameters

port-string	(Optional) Resets the quiet period for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, the quiet period value is reset on all ports.

Mode

All command modes.

Example

This example shows how to clear the PWA quiet period for port ge.1.1:

```
S Chassis(rw)->clear pwa quietperiod ge.1.1
S Chassis(rw)->show pwa ge.1.1
PWA Status                  - disabled
.
.
.
Port     Mode              AuthStatus      QuietPeriod  MaxReq
-------- ----------------  --------------  -----------  -----------
ge.1.1   disabled           disconnected    60           16
S Chassis(rw)->
```

set pwa maxrequest

Use this command to set the maximum number of log on attempts allowed before transitioning the PWA port to a held state.

Syntax

set pwa maxrequest max*requests* [*port-string*]

Parameters

maxrequests	Specifies the maximum number of log on attempts. Valid Values: **0** - **2147483647**. Default **16**.
port-string	(Optional) Sets the maximum requests for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, maximum requests will be set for all ports.

Mode

All command modes.

Example

This example shows how to set the PWA maximum requests to 3 for all ports:

```
S Chassis(rw)->set pwa maxrequests 3
```

clear pwa maxrequest

Use this command to reset the allowed maximum request failed to the default value.

Syntax

clear pwa maxrequest [*port-string*]

Parameters

port-string	(Optional) Resets the maximum requests for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, the maximum requests value is reset on all ports.

Mode

All command modes.

Example

This example shows how to clear the PWA maximum requests for port ge.1.1:

```
S Chassis(rw)->clear pwa maxrequest ge.1.1
S Chassis(rw)->show pwa ge.1.1
PWA Status                   - disabled
.
.
.
Port     Mode              AuthStatus      QuietPeriod  MaxReq
-------- ----------------  --------------  -----------  -----------
ge.1.1   disabled           disconnected    60           16
S Chassis(rw)->
```

set pwa portcontrol

Use this command to set the PWA port control mode.

Syntax

set pwa portcontrol {**enable** | **disable**} [*port-string*]

Parameters

enable | **disable**	Enables or disables PWA on the specified port.
port-string	(Optionally) Enables or disables a specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

Enables or disables all ports if no port is specified.

Mode

All command modes.

Example

This example shows how to enable PWA on all ports:

```
S Chassis(rw)->set pwa portcontrol enable
```

show pwa session

Use this command to display information about current PWA sessions.

Syntax

show pwa session [*port-string*]

Parameters

port-string	(Optional) Displays PWA session information for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, session information for all ports will be displayed.

Mode

All command modes.

Example

This example shows how to display PWA session information:

```
S Chassis(rw)->show pwa session
Port     MAC               IP              User          Duration     Status
-------- ----------------- --------------- ------------- ------------ ---------
ge.2.19  00-c0-4f-20-05-4b 172.50.15.121   pwachap10     0,14:46:55   active
ge.2.19  00-c0-4f-24-51-70 172.50.15.120   pwachap1      0,15:43:30   active
ge.2.19  00-00-f8-78-9c-a7 172.50.15.61    pwachap11     0,14:47:58   active
```

show pwa summary

Use this command to display information about current PWA sessions.

Syntax

show pwa summary

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display PWA summary information:

```
S Chassis(rw)->show pwa summary
PWA Status                  - disabled
PWA Hostname                -
PWA IP Address              - 0.0.0.0
PWA Protocol                - PAP
PWA Enhanced Mode           - disabled
PWA Logo                    - enabled
PWA Guest Networking Status - disabled
PWA Guest Name              - guest
PWA Redirect Time           - 5
S Chassis(rw)->
```

91

MAC Authentication Commands

This chapter describes the MAC Authentication set of commands and how to use them. For information about configuring MAC authentication, refer to the "Authentication Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show macauthentication	91-1
show macauthentication session	91-3
set macauthentication	91-4
set macauthentication password	91-5
clear macauthentication password	91-5
set macauthentication significant-bits	91-6
clear macauthentication significant-bits	91-6
set macauthentication port	91-7
set macauthentication authallocated	91-7
clear macauthentication authallocated	91-8
set macauthentication portinitialize	91-8
set macauthentication macinitialize	91-9
set macauthentication reauthentication	91-9
set macauthentication portreauthenticate	91-10
set macauthentication macreauthenticate	91-10
set macauthentication reauthperiod	91-11
clear macauthentication reauthperiod	91-11
set macauthentication quietperiod	91-12
clear macauthentication quietperiod	91-12

show macauthentication

Use this command to display MAC authentication information for one or more ports.

Syntax

show macauthentication [*port-string*]

Parameters

port-string	(Optional) Displays MAC authentication information for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified, MAC authentication information will be displayed for all ports.

Mode

All command modes.

Example

This example shows how to display MAC authentication information:

```
S Chassis(rw)->show macauthentication
MAC authentication:           - enabled
MAC user password:            - MCKINLEY
Port username significant bits  - 48

 Port      Port     Quiet      Reauth     Reauth   MultiAuth MAC Auth  Current
           State    Period     Period     Enabled  Limit     Limit     Sessions
 --------  -------- ---------- ---------- -------- --------- --------- ---------
 ge.5.1    disabled 0          0          disabled 8         2048      0
 ge.5.2    disabled 0          0          disabled 8         2048      0
 ge.5.3    disabled 0          11         disabled 8         2048      0
 ge.5.4    disabled 0          11         disabled 8         2048      0
 ge.5.5    enabled  0          3600       disabled 2         2048      2
 ge.5.6    disabled 0          3600       disabled 8         2048      0
 ge.5.7    disabled 0          3600       disabled 8         2048      0
 ge.5.8    disabled 0          3600       disabled 8         2048      0
 ge.5.9    disabled 0          3600       disabled 8         2048      0
```

Table 91-1 provides an explanation of the command output.

Table 91-1 show macauthentication Output Details

Output...	What it displays...
MAC authentication	Whether MAC authentication is globally enabled or disabled. Set using the **set macauthentication** command as described in "set macauthentication" on page 91-4.
MAC user password	User password associated with MAC authentication on the device. Set using the **set macauthentication password** command as described in "set macauthentication password" on page 91-5.

Table 91-1 show macauthentication Output Details (continued)

Output...	What it displays...
Port username significant bits	Number of significant bits in the MAC addresses to be used starting with the left-most bit of the vendor portion of the MAC address. The significant portion of the MAC address is sent as a user-name credential when the primary attempt to authenticate the full MAC address fails. Any other failure to authenticate the full address, (i.e., authentication server timeout) causes the next attempt to start once again with a full MAC authentication. Default is 48 and cannot be reset.
Port	Port designation.
Port State	Whether or not MAC authentication is enabled or disabled on this port.
Quiet Period	Enables a reauthentication attempt for failed entries at the period specified in seconds. Default value is 0 (never).
Reauth Period	Reauthentication period for this port. Default value of **30** can be changed using the **set macauthentication reauthperiod** command described in “set macauthentication reauthperiod” on page 91-11.
Reauth enabled	Whether or not reauthentication is enabled or disabled on this port. Set using the **set macauthentication reauthentication** command described in “set macauthentication reauthentication” on page 91-9.
Multiauth limit	Number of concurrent authentications supported on this port.
MacAuth limit	Maximum theoretical limit for the number of MAC authentications permitted for all ports, if all chassis slots are filled and licenses are applied.
Current Sessions	Specifies the number of currently active MacAuthentication sessions for this port.

show macauthentication session

Use this command to display the active MAC authenticated sessions.

Syntax

```
show macauthentication session [port port-string] [mac mac-address]
```

Parameters

port *port-string*	(Optional) Specifies the port of the MAC authentication session to display. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
mac *mac-address*	(Optional) Specifies the MAC address of the MAC authentication session to display

Defaults

If no optional parameter is specified, MAC session information will be displayed for all MAC authentication sessions.

Mode

All command modes.

Example

This example shows how to display MAC session information:

```
S Chassis(rw)->show macauthentication session
Port       MAC Address       Duration   Reauth Period   Reauthentications
-----    -----------------  ----------  -------------   -----------------
ge.1.2   00:60:97:b5:4c:07  0,00:52:31  3600            disabled
```

Table 91-2 provides an explanation of the command output.

Table 91-2 show macauthentication session Output Details

Output...	What it displays...
Port	Port designation.
MAC Address	MAC address associated with the session.
Duration	Time this session has been active.
Reauth Period	Reauthentication period for this port, set using the **set macauthentication reauthperiod** command described in “set macauthentication reauthperiod” on page 91-11.
Reauthentications	Whether or not reauthentication is enabled or disabled on this port. Set using the **set macauthentication reauthentication** command described in “set macauthentication reauthentication” on page 91-9.

set macauthentication

Use this command to globally enable or disable MAC authentication.

Syntax

set macauthentication {**enable** | **disable**}

Parameters

enable | **disable**	Globally enables or disables MAC authentication.

Defaults

Disabled.

Mode

All command modes.

Examples

This example shows how to globally enable MAC authentication:

```
S Chassis(rw)->set macauthentication enable
```

set macauthentication password

Use this command to set a MAC authentication password.

Syntax

set macauthentication password *password*

Parameters

password	Specifies a text string MAC authentication password.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to set the MAC authentication password to "macauth":

```
S Chassis(rw)->set macauthentication password macauth
```

clear macauthentication password

Use this command to clear the MAC authentication password.

Syntax

clear macauthentication password

Parameters

None.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to clear the MAC authentication password:

```
S Chassis(rw)->clear macauthentication password
```

set macauthentication significant-bits

Use this command to set the number of significant bits of the MAC address to use for authentication.

Syntax

set macauthentication significant-bits *number*

Parameters

number	Specifies a number of significant bits.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to set the MAC authentication significant bits to 24:

```
S Chassis(rw)->set macauthentication significant-bits 24
```

clear macauthentication significant-bits

Use this command to clear the MAC authentication significant bits setting.

Syntax

clear macauthentication significant-bits

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear the MAC authentication significant bits setting:

```
S Chassis(rw)->clear macauthentication significant-bits
```

set macauthentication port

Use this command to enable or disable one or more ports for MAC authentication.

Syntax

set macauthentication port {**enable** | **disable**} *port-string*

Parameters

enable | **disable**	Enables or disables MAC authentication.
port-string	Specifies port(s) on which to enable or disable MAC authentication. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Usage

Enabling port(s) for MAC authentication requires globally enabling MAC authentication on the device as described in "set macauthentication" on page 91-4, and then enabling it on a port-by-port basis. By default, MAC authentication is globally disabled and disabled on all ports.

Example

This example shows how to enable MAC authentication on ge.2.1 though 5:

```
S Chassis(rw)->set macauthentication port enable ge.2.1-5
```

set macauthentication authallocated

Use this command to set the number of MAC authentication sessions allowed for one or more ports.

Syntax

set macauthentication authallocated *number port-string*

Parameters

number	Specifies the number of authentication sessions allowed.
port-string	Specifies port(s) on which to set the number of authentication sessions. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Example

This example shows how to set the number of allowed MAC authentication sessions to 4 on ge.2.1:

```
S Chassis(rw)->set macauthentication authallocated 4 ge.2.1
```

clear macauthentication authallocated

Use this command to clear the number of MAC authentication sessions allowed for one or more ports.

Syntax

clear macauthentication authallocated [*port-string*]

Parameters

port-string	(Optional) Clears the number of authentication sessions allowed for specific port(s). For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

If *port-string* is not specified the number of allowed authentication sessions will be cleared on all ports.

Mode

All command modes.

Example

This example shows how to clear the number of allowed MAC authentication sessions on ge.2.1:

```
S Chassis(rw)->clear macauthentication authallocated ge.2.1
```

set macauthentication portinitialize

Use this command to force one or more MAC authentication ports to re-initialize and remove any currently active sessions on those ports.

Syntax

set macauthentication portinitialize *port-string*

Parameters

port-string	Specifies the MAC authentication port(s) to re-initialize. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Example

This example shows how to force ge.2.1 through 5 to initialize:

```
S Chassis(rw)->set macauthentication portinitialize ge.2.1-5
```

set macauthentication macinitialize

Use this command to force a current MAC authentication session to re-initialize and remove the session.

Syntax

set macauthentication macinitialize *mac_addr*

Parameters

mac_addr	Specifies the MAC address of the session to re-initialize.

Defaults

None.

Mode

All command modes.

Example

This example shows how to force the MAC authentication session for address 00-60-97-b5-4c-07 to re-initialize:

```
S Chassis(rw)->set macauthentication macinitialize 00-60-97-b5-4c-07
```

set macauthentication reauthentication

Use this command to enable or disable reauthentication of all currently authenticated MAC addresses on one or more ports.

Syntax

set macauthentication reauthentication {**enable** | **disable**} *port-string*

Parameters

enable | **disable**	Enables or disables MAC reauthentication.
port-string	Specifies port(s) on which to enable or disable MAC reauthentication. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Example

This example shows how to enable MAC reauthentication on ge.4.1 though 5:

```
S Chassis(rw)->set macauthentication reauthentication enable ge.4.1-5
```

set macauthentication portreauthenticate

Use this command to force an immediate reauthentication of the currently active sessions on one or more MAC authentication ports.

Syntax

set macauthentication portreauthenticate *port-string*

Parameters

port-string	Specifies MAC authentication port(s) to be reauthenticated. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Example

This example shows how to force ge.2.1 though 5 to reauthenticate:

```
S Chassis(rw)->set macauthentication portreauthentication ge.2.1-5
```

set macauthentication macreauthenticate

Use this command to force an immediate reauthentication of a MAC address.

Syntax

set macauthentication macreauthenticate *mac_addr*

Parameters

mac_addr	Specifies the MAC address of the session to reauthenticate.

Defaults

None.

Mode

All command modes.

Example

This example shows how to force the MAC authentication session for address 00-60-97-b5-4c-07 to reauthenticate:

```
S Chassis(rw)->set macauthentication macreauthenticate 00-60-97-b5-4c-07
```

set macauthentication reauthperiod

Use this command to set the MAC reauthentication period (in seconds).

Syntax

set macauthentication reauthperiod *time port-string*

Parameters

time	Specifies the number of seconds between reauthentication attempts. Valid values are **0** - **4294967295**.
port-string	Specifies the port(s) on which to set the MAC reauthentication period. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None.

Mode

All command modes.

Usage

This is the time lapse between attempts to reauthenticate any current MAC address authenticated to a port. A value of **0** specifies never.

Example

This example shows how to set the MAC reauthentication period to 7200 seconds (2 hours) on ge.2.1 through 5:

```
S Chassis(rw)->set macauthentication reauthperiod 7200 ge.2.1-5
```

clear macauthentication reauthperiod

Use this command to clear the MAC reauthentication period on one or more ports.

Syntax

clear macauthentication reauthperiod [*port-string*]

Parameters

port-string	(Optional) Clears the MAC reauthentication period on specific port(s).

Defaults

If port-string is not specified, the reauthentication period will be cleared on all ports.

Mode

All command modes.

Example

This example shows how to globally clear the MAC reauthentication period:

```
S Chassis(rw)->clear macauthentication reauthperiod
```

set macauthentication quietperiod

Use this command to enable a reauthentication attempt for failed entries at the period specified in seconds.

Syntax

set macauthentication quietperiod *time port-string*

Parameters

time	Specifies the number of seconds between reauthentication attempts. Valid values are **0** - **4294967295**.
port-string	Specifies the port(s) on which to set the macauthentication quiet period.

Defaults

None.

Mode

All command modes.

Usage

Default value is 0 (never).

Example

This example shows how to set the macauthentication quiet period to 120 seconds (2 minutes) on ge.2.1 through 5:

```
S Chassis(rw)->set macauthentication quiet period 120 ge.2.1-5
```

clear macauthentication quietperiod

Use this command to clear the macauthentication quiet period on one or more ports to the default value.

Syntax

clear macauthentication quietperiod [*port-string*]

Parameters

port-string	(Optional) Clears the macauthentication quiet period on specific port(s).

Defaults

None.

Mode

All command modes.

Usage

The default value is 0 (never).

Example

This example shows how to clear the macauthentication quietperiod for port ge.1.1

```
S Chassis(rw)->clear macauthentication quietperiod ge.1.1
```

92

Convergence End Points (CEP) Phone Detection Commands

This chapter describes the set of commands for Convergence End Points (CEP) command information. For information about configuring CEP, refer to the "Authentication Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show cep connections	92-1
show cep detection	92-2
show cep policy	92-3
show cep port	92-4
set cep	92-4
set cep accounting	92-5
set cep port	92-5
set cep policy	92-6
set cep detection-id	92-6
set cep detection-id type	92-7
set cep detection-id address	92-8
set cep detection-id protocol	92-9
set cep detection-id porthigh | portlow	92-9
set cep initialize	92-10
clear cep	92-11

show cep connections

Use this command to display all learned CEPs.

Syntax

show cep connections *port-string*

Parameters

port-string	Displays CEP status for one or more ports. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None

Mode

All command modes.

Example

This example shows how to display CEP connections for port ge.1.21:

```
S Chassis(rw)->show cep connections ge.1.21
Connection Info for ge.1.21
Endpoint Type      h323
Policy Index       3
Discovery Time     MON FEB 06 02:31:42 2008
Firmware Version
Address Type       unknown
Endpoint IP        unavailable
Endpoint MAC       00:04:0d:01:f8:35
```

show cep detection

Use this command to display CEP phone detection parameters.

Syntax

show cep detection [*detection-id*]

Parameters

detection-id	(Optional) Show CEP detection parameters, based on the CEP configuration group id.

Defaults

If no *detection-id* is specified, global CEP detection parameters are displayed.

Mode

All command modes.

Examples

This example shows how to display CEP detection information:

```
S Chassis(rw)->show cep detection
Global CEP state enabled
```

```
Global CEP RADIUS accounting state disabled
Detection Rules for Index 1:
Endpoint Phone Type h323
Protocol tcp & udp
Port Low 1718
Port High 1720
Address Type unknown
Address
Mask Type unknown
Mask
Row Status enabled
```

show cep policy

Use this command to display the global policies of all supported CEP types.

Syntax

show cep policy

Parameters

None.

Defaults

None

Mode

All command modes.

Examples

This example shows how to display CEP policy information:

```
S Chassis(rw)->show cep policy
CEP default policies
CEP Type  Policy Index  Policy Name
--------  ------------  ------------
cisco     13            Cisco IP Phone
siemens   9             IP Phone Siemens
h323      3             IP Phone Avaya
sip       0
lldp-med  0
S Chassis(rw)->
```

show cep port

Use this command to display enable status of all supported CEP types.

Syntax

show cep port *port-string*

Parameters

port-string	Displays CEP status for one or more ports. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.

Defaults

None

Mode

All command modes.

Examples

This example shows how to display CEP status information for port ge.1.1:

```
S Chassis(rw)->show cep port ge.1.1
Port          H323     Siemens    Cisco     SIP     LLDP-MED
----------  --------  --------  --------  --------  --------
ge.1.1      enabled   enabled   disabled  disabled  disabled
```

set cep

Use this command to globally enable or disable CEP detection.

Syntax

set cep {**enable** | **disable**}

Parameters

enable | **disable**	Globally enables or disables CEP detection.

Defaults

Disabled.

Mode

All command modes.

Example

This example shows how to globally enable CEP detection:

```
S Chassis(rw)->set cep enable
```

set cep accounting

Use this command to enable or disable CEP accounting.

Syntax

set cep accounting {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables CEP accounting. CEP accounting is globally disabled by default.

Defaults

CEP accounting is disabled by default.

Mode

All command modes.

Usage

This example shows how to enable CEP accounting:

```
S Chassis(rw)->set cep accounting enable
```

set cep port

Use this command to enable or disable a CEP detection type on one or more ports.

Syntax

set cep port *port-string* {**cisco** | **h323** | **lldp-med** | **siemens** | **sip**} {**enable** | **disable**}

Parameters

port-string	Specifies the port(s) to enable or disable. For a detailed description of possible *port-string* values, refer to the *Extreme Networks S-Series Configuration Guide*.
cisco	Set the Cisco detection status on the specified ports.
h323	Set the H323 detection status on the specified ports.
lldp-med	Set the LLDP-MED detection status on the specified ports.
siemens	Set the Siemens detection status on the specified ports.
sip	Set the SIP detection status on the specified ports.
enable | **disable**	Enables or disables CEP detection as specified.

Defaults

None.

Mode

All command modes.

Example

This example shows how to enable Cisco phone detection on port ge. 3. 1:

```
S Chassis(rw)->set cep port ge.3.1 cisco enable
```

set cep policy

Use this command to set a global default policy for a CEP detection type.

Syntax

set cep policy {**cisco** | **h323** | **lldp-med** | **siemens** | **sip**} *index*

Parameters

cisco	Set the Cisco global default policy index.
h323	Set the H323 global default policy index.
lldp-med	Set the LLDP-MED global default policy index.
siemens	Set the Siemens global default policy index.
sip	Set the SIP global default policy index.
index	Set the policy index value. This must be configured using the policy management commands described in Chapter 43, **Policy Profile Commands**. Valid values are **0** - **1023**.

Defaults

None.

Mode

All command modes.

Usage

This is the policy that will be applied when a phone of the specified type is detected on a port. It must be configured using the policy management commands described in Chapter 43, **Policy Profile Commands**.

Example

This example shows how to assign policy index 1 to all H.323 phones detected:

```
S Chassis(rw)->set cep policy h323 1
```

set cep detection-id

Use this command to create a new H.323, Siemens, or SIP phone detection configuration group, or enable, disable or remove an existing group.

Syntax

set cep detection-id *id* {**create** | **delete** | **disable** | **enable**}

Parameters

id	Specifies a CEP configuration group value. Valid values are **1**-**2147483647**.
create | **delete** | **disable** | **enable**	Creates a new convergence end points detection configuration group, or removes, disables or enables an existing group. A group must first be created then enabled to become operational.

Defaults

None.

Mode

All command modes.

Usage

This command applies only to Siemens, H.323, and SIP phone detection. Cisco detection uses CiscoDP as its discovery method.

The S-Series supports the configuration of up to 16 CEP configuration groups on a device.

Example

This example shows how to create CEP detection group 1:

```
S Chassis(rw)->set cep detection-id 1 create
```

set cep detection-id type

Use this command to specify whether a phone detection group will use H.323, Siemens or SIP as its phone discovery type.

Syntax

set cep detection-id *id* **type** {**h323** | **siemens** | **sip**}

Parameters

id	Specifies a CEP configuration group ID. This group must be created and enabled using the **set cep detection-id** command as described in "set cep detection-id" on page 92-6. Valid values are **1** - **2147483647**.
h323 | **siemens** | **sip**	Specifies the phone type to detect as H.323, Siemens, or SIP.

Defaults

None.

Mode

All command modes.

Usage

This command applies only to Siemens, H.323, and SIP phone detection. Cisco detection uses CiscoDP as its discovery method.

There are currently 3 manual detection types (Siemens, H323, SIP). Under manual detection configuration, for each of the types, the "Endpoint Phone Type" will be listed correctly. However, the high and low ports will not reflect default ports for the "Endpoint Phone Types". The user will have to configure the port low and high options to match their needs for the Endpoint Phone Type being configured, as described in "set cep detection-id porthigh | portlow" on page 92-9.

Example

This example shows how to set the phone detection type to type H.323 for CEP group 1:

```
S Chassis(rw)->set cep detection-id 1 h323
```

set cep detection-id address

Use this command to set an H.323, Siemens, or SIP phone detection group's IP address or mask.

Syntax

set cep detection-id *id* **address** {*ip-address* | **unknown**} **mask** {*mask* | **unknown**}

Parameters

id	Specifies a CEP configuration group ID. This group must be created and enabled using the **set cep detection-id** command as described in "set cep detection-id" on page 92-6. Valid values are **1** - **2147483647**.
address *ip-address* | **unknown**	Sets the IP address for CEP detection, or sets the address to **unknown**.
mask *mask* | **unknown**	Set the IP mask for CEP detection, or sets the mask to **unknown**.

Defaults

None.

Mode

All command modes.

Usage

This command applies only to Siemens, H.323, and SIP phone detection. Cisco detection uses CiscoDP as its discovery method.

By default, H.323 will use 224.0.1.41 as its IP address and Siemens will have no IP address configured.

Example

This example shows how to set an IP address of 10.1.1.3 and mask for detection group 1:

```
S Chassis(rw)->set cep detection-id 1 address 10.1.1.3 mask 255.255.0.0
```

set cep detection-id protocol

Use this command to specify an IP protocol type for H.323, Siemens, or SIP convergence end points detection.

Syntax

set cep detection-id *id* **protocol** {**tcp** | **udp** | **both** | **none**}

Parameters

id	Specifies a CEP configuration group ID. This group must be created and enabled using the **set cep detection-id** command as described in "set cep detection-id" on page 92-6. Valid values are **1** - **2147483647**.
tcp | **udp** | **both** | **none**	Sets the CEP IP protocol type to be used for detection as: • TCP • UDP • Both UDP and TCP • None

Defaults

None.

Mode

All command modes.

Usage

This command applies only to Siemens, H.323, and SIP phone detection. Cisco detection uses CiscoDP as its discovery method.

If an IP address is not set for a phone detection group as described in "set cep detection-id address" on page 92-8, this will configure detection on UDP and/or TCP ports using a port range defined with the **set cep detection-id porthigh** | **portlow** command as described in "set cep detection-id porthigh | portlow" on page 92-9.

Example

This example shows how to enable both TCP and UDP convergence end points detection for CEP detection group 1:

```
S Chassis(rw)->set cep detection-id 1 protocol both
```

set cep detection-id porthigh | portlow

Use this command to set the maximum and minimum ports used for TCP or UDP convergence end points detection.

Syntax

set cep detection-id *id* {**porthigh** | **portlow}** *port*

Parameters

id	Specifies a CEP configuration group ID. This group must be created and enabled using the **set cep detection-id** command as described in "set cep detection-id" on page 92-6. Valid values are **1** - **2147483647**.
porthigh | **portlow** *port*	Specifies a maximum or minimum UDP or TCP port for CEP detection.Valid values are **1** - **65535**.

Defaults

None.

Mode

All command modes.

Usage

This command applies only to Siemens, H.323, and SIP phone detection. Cisco detection uses CiscoDP as its discovery method.

Once UDP and/or TCP phone detection has been specified using the **set cep detection-id protocol** command as described in "set cep detection-id protocol" on page 92-9, the protocols will use this port range for detection matching.

Example

This example shows how to set port 65 as the minimum port to be used for convergence end points detection for CEP group 1:

```
S Chassis(rw)->set cep detection-id 1 portlow 65
```

set cep initialize

Use this command to clear all existing CEP connections for one or more CEP-enabled ports.

Syntax

set cep initialize [*port-string*]

Parameters

port-string	(Optional) Specifies the CEP-enabled port(s) to clear existing CEP connections. This must be a *port-string* enabled for CEP using the **set cep port** command as described in "set cep port" on page 92-5.

Defaults

If no *port-string* is specified, all existing CEP connections on all ports are cleared.

Mode

All command modes.

Usage

This command is similar to the **clear cep users** command.

Example

This example shows how to re-initialize CEP ports ge.1.3-5:

```
S Chassis(rw)->set cep initialize ge.1.3-5
```

clear cep

Use this command to clear convergence end points parameters.

Syntax

clear cep {**all** | **policy** | **detection** [*detection-id*] | **users** [*port-string*] | **port** *port-string* {**all** | **cisco** | **lldp-med** | **h323** | **siemens** |**sip**}}

Parameters

all	Restores factory defaults to all CEP configuration information.
policy	Restore factory defaults to CEP policy configuration.
detection [*detection-id*]	Restore factory defaults to CEP detection group configuration. Optionally, specify a particular CEP configuration group to clear with *detection-id*. Valid values are **1** - **2147483647**.
users [*port-string*]	Clear discovered Convergence Endpoints. Optionally, specify one or more port(s) on which to clear discovered CEPs.
port [*port-string* {**all** | **cisco** |**lldp-med** | **h323** | **siemens** | **sip**}]	Resets the CEP enabled state to the default of disabled. Specify one or more port(s) to disable and specify all detection types or individual detection types to disable.

Defaults

If no *detection-id* is specified, all CEP detection groups are returned to the default configuration.

If no *port-string* is specified with the **users** parameter, all discovered Convergence Endpoints are cleared.

If no *port-string* is specified with the port parameter, all ports are cleared.

Mode

All command modes.

Examples

This example shows how to clear all CEP policy parameters

```
S Chassis(rw)->clear cep policy
```

This example shows how to clear detection id 4 parameters

```
S Chassis(rw)->clear cep detection-id 4
```

This example shows how to clears ports ge.1.1-5 of Cisco phone detection parameters

```
S Chassis(rw)->clear cep port ge.1.1-5 cisco
```

93

RADIUS Snooping Commands

This chapter describes the RADIUS Snooping set of commands and how to use them. For information about configuring RADIUS Snooping, refer to the "RADIUS Snooping Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
set radius-snooping	93-1
set radius-snooping accounting	93-2
set radius-snooping timeout	93-2
set radius-snooping port	93-3
set radius-snooping flow	93-4
set radius-snooping initialize	93-5
clear radius-snooping all	93-5
clear radius-snooping flow	93-6
clear radius-snooping port	93-6
show radius-snooping	93-7
show radius-snooping port	93-8
show radius-snooping flow	93-9
show radius-snooping session	93-10

set radius-snooping

Use this command to globally enable or disable RS for this device.

Syntax

```
set radius-snooping {enable | disable}
```

Parameters

enable	Globally enables RS on this device.
disable	Globally disables RS on this device.

Defaults

None.

Mode

All command modes.

Usage

This command does not enable RS on the ports for this device. To enable ports for RS see the command "set radius-snooping port" on page 93-3.

Example

This example shows how to enable RS globally on this device:

```
S Chassis(rw)->set radius-snooping enable
```

set radius-snooping accounting

Use this command to enable or disable RS accounting.

Syntax

set radius-snooping accounting {**enable** | **disable**}

Parameters

enable | **disable**	Enables or disables RS accounting. RS accounting is globally disabled by default.

Defaults

RS accounting is disabled by default.

Mode

All command modes.

Usage

RADIUS accounting must be enabled using "set radius accounting" on page 86-9 for RS accounting to take place. RADIUS accounting is disabled by default. If RADIUS accounting is enabled, RS accounting remains disabled by default.

Examples

This example shows how to enable RS accounting:

```
S Chassis(rw)->set radius-snooping accounting enable
```

set radius-snooping timeout

Use this command to set the number of seconds that the firmware waits for a RADIUS response frame to be returned from the RADIUS server, after successfully snooping a RADIUS request frame from the client.

Syntax

set radius-snooping timeout *seconds*

Parameters

seconds	Specifies the number of seconds that the firmware waits from the time it successfully snoops a RADIUS request frame, for a RADIUS response frame to be returned from the RADIUS server. Default: **20**

Defaults

None.

Mode

All command modes.

Usage

If no response is seen before the timeout expires, the session is terminated.

Example

This example shows how to set the RS timeout to **30** seconds:

```
S Chassis(rw)->set radius-snooping timeout 30
```

set radius-snooping port

Use this command to enable RS on all or the specified port(s).

Syntax

set radius-snooping port [**enable** | **disable**] [**timeout** *seconds*] [**drop** {**enable** | **disable**}] [**authallocated** *number*] [*port-string*]

Parameters

enable | **disable**	(Optional) Enables or disables RS functionality on the specified port(s). Disabled by default.
timeout *seconds*	(Optional) Specifies the number of seconds the firmware waits for a RADIUS response frame after it successfully snoops a RADIUS request frame. The timeout timer defaults to 0 seconds (unset). When 0 seconds is configured, the firmware uses the system level timeout value.
drop {**enable** | **disable**}	(Optional) Sets the RADIUS traffic drop behavior for this port. Disabled by default.
authallocated *number*	(Optional) Sets the number of RS sessions allowed on a per port basis. Default value is 8, 128, or 256 depending upon the system license for this device.
port-string	(Optional) Enables RS for the specified port(s).

Defaults

If no timeout value is specified, the global timeout value specified in the **set radius-snooping timeout** command is used.

If no parameters are specified, RADIUS snooping is enabled on all ports.

Mode

All command modes.

Usage

If the timeout timer expires, the affected session is terminated. If timeout is set to **0**, the global timeout is used.

Set the authallocated value equal to or less than the configured value for **set multiauth port numusers**. This value is the maximum number of users per port for all authentication clients.

In some cases it may be necessary to drop RADIUS traffic in order to maintain session consistency between the distribution tier device and the edge switches. Packets are always dropped for a resource issue situation. With drop enabled, frames with an invalid calling station ID are also dropped.

Example

This example enables RS on ports **ge.1.10** through **ge.1.15**, sets the timeout to **15** seconds and enables drop:

```
S Chassis(rw)->set radius-snooping enable timeout 15 drop enable ge.1.10-15
```

set radius-snooping flow

Use this command to provide for the entering of RADIUS client and server session flow entries into the RS flow table.

Syntax

set radius-snooping flow *index client-IP-address server-IP-address server-port* [*secret*]

Parameters

index	Specifies a numeric index ID for this flow table entry.
client-IP-address	Specifies the client IP address for this RS flow table entry.
server-IP-address	Specifies the server IP address for this RS flow table entry.
server-port	Specifies the RADIUS UDP port to use for this RS flow table entry.
secret	(Optional) Specifies the RADIUS secret for this RS flow table entry.

Defaults

If no **secret** is specified, no secret is used for this flow entry.

Mode

All command modes.

Usage

RADIUS flows defined in the RS flow table are snooped if RS is enabled for both the system and this port.

Flow entries are added to the flow table based upon the entry index value. The first matching entry in the table is the entry used for the continuation of the authentication process.

The standard server UDP port is **1812**.

If a secret is configured on the authentication server and not configured here, no validation will occur.

Example

This example creates an index 1 entry in the RADIUS flow table for client **192.10.5.10** and server **192.10.20.1** for the standard UPD port 1812 with a secret **mysecret**:

```
S Chassis(rw)->set radius-snooping flow 1 192.10.5.10 192.10.20.1 1812 mysecret
```

set radius-snooping initialize

Use this command to terminate all RS sessions on the system for the specified port or MAC address.

Syntax

set radius-snooping initialize {**port** *port-string* | *mac-address*}

Parameters

port *port-string*	Specifies the port(s) to initialize. Use *.*.* for all ports.
mac-address	Specifies the MAC address to initialize.

Defaults

None.

Mode

All command modes.

Example

This example terminates all RS sessions associated with port **ge.1.1** by initializing the port:

```
S Chassis(rw)->set radius-snooping initialize port ge.1.1
```

clear radius-snooping all

Use this command to reset all RS configuration to the default values for this system.

Syntax

clear radius-snooping all

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example resets all RS configuration to the default setting for this system:

```
S Chassis(rw)->clear radius-snooping all
```

clear radius-snooping flow

Use this command to clear all entries or the specified index entry from the RS flow table.

Syntax

clear radius-snooping flow {**all** | *index*}

Parameters

all	Specifies that all flow table entries are to be cleared.
index	Specifies a specific flow table index entry to be cleared.

Defaults

None.

Mode

All command modes.

Usage

Use the *index* value to clear flows for a particular port.

Examples

This example clears all flow table entries:

```
S Chassis(rw)->clear radius-snooping flow all
```

This example clears the flow table entry for index 5:

```
S Chassis(rw)->clear radius-snooping flow 5
```

clear radius-snooping port

Use this command to clear RADIUS-snooping configuration for all or the specified ports.

Syntax

clear radius-snooping port [*port-string*]

Parameters

port-string	(Optional) Specifies a specific port to clear.

Defaults

If no port is specified, configuration is cleared on all ports.

Mode

All command modes.

Examples

This example clears RADIUS-snooping configuration on all ports:

```
S Chassis(rw)->clear radius-snooping port all
```

This example clears RADIUS-snooping configuration on port ge.1.1:

```
S Chassis(rw)->clear radius-snooping port ge.1.1
```

show radius-snooping

Use this command to display a general overview of the global RS status.

Syntax

show radius-snooping

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display RADIUS configuration information:

```
S Chassis(rw)->show radius-snooping
RADIUS Snooping:                        enabled
RADIUS Snooping Accounting:             enabled
Timeout:                                20
Number of Configured Flows:             12
Active Sessions:                        0
Enabled ports:
ge.1.5
Enabled ports: ge.1.1-ge.1.8; ge.1.22
```

Table 93-1 Radius-Snooping Settings

Output...	What it displays...
RADIUS Snooping	Specifies whether RS is globally enabled or disabled.
RADIUS Snooping Accounting	Specifies whether RS accounting is enabled or disabled.
Timeout	Specifies the number of seconds that the firmware waits for a RADIUS response frame to be returned from the RADIUS server, after successfully snooping a RADIUS request frame from the client.

Table 93-1 Radius-Snooping Settings

Output...	What it displays...
Number of configured flows	Specifies the number of globally configured flows for this system.
Active sessions	Specifies the number of active sessions for this system.
Enabled ports	Specifies the ports RS is currently enabled on.

show radius-snooping port

Use this command to display both a general overview of the global RS status as well as the per port RS status for the port(s) specified.

Syntax

show radius-snooping port *port-string*

Parameters

port-string	Specifies the port for status to be displayed.

Defaults

None.

Mode

All command modes.

Example

This example displays the RS status for port **ge.1.5**:

```
S Chassis(rw)->show radius-snooping port ge.1.5
RADIUS Snooping:                          enabled

Port            Port State      Timeout    Drop State      Allowed    Allocated
--------------- --------------- ---------- --------------- ---------- ----------
ge.1.5          disabled        0          enabled         128        128
```

Table 93-2 Radius-Snooping Port Settings

Output...	What it displays...
Port	Specifies the port(s) currently enabled for RS.
Port State	Specifies the actual port state.
Timeout	Specifies the amount of time in seconds before the session will be terminated if no response is seen from the RADIUS server once a request is seen from the client.
Drop State	Specifies whether Drop State is enabled or disabled for sessions on this port.
Allowed	Specifies the maximum number of sessions allowed by license for this port.
Allocated	Specifies the number of allocated sessions as set in the command “set radius-snooping port” on page 93-3.

show radius-snooping flow

Use this command to display information for all flows or the specified index entry in the flow table.

Syntax

show radius-snooping flow {*index* | **all**}

Parameters

index	Specifies a specific flow table index entry to be displayed.
all	Specifies that all flow table entries are to be displayed.

Defaults

None.

All command modes.

Usage

Use the *index* to specify a particular flow to display, otherwise use **all**.

Example

This example displays the flow information for index **1**:

```
S Chassis(rw)->show radius-snooping flow 1
Flow ID         Client IP       Server IP       UDP Port        Validation
--------------- --------------- --------------- --------------- ---------------
1               192.10.20.5     192.10.10.10    1812            Enabled

Number of current sessions     : 17
Number pending                 : 4

Total Sessions:                : 85
Total RADIUS Access Requests   : 242
Total RADIUS Access Accepts    : 212
Total RADIUS Access Rejects    : 26
Invalid RADIUS Request packets : 0
Invalid RADIUS Response packets: 0
Total Dropped Packets          : 0
```

Table 93-3 Radius-Snooping Flow Settings

Output...	What it displays...
FlowID	Specifies the index ID for this flow.
Client IP	Specifies the client IP address for this flow.
Server IP	Specifies the server IP address for this flow.
UDP Port	Specifies the authentication server UDP port for this flow.

Table 93-3 Radius-Snooping Flow Settings

Output...	What it displays...
Validation	Specifies enabled if there is a secret configured, otherwise specifies disabled. For security reasons the secret does not display.
Number of current sessions	Specifies the number of active sessions for this flow.
Number pending	Specifies the number of valid RADIUS request frames pending, but no matching RADIUS response frame has been seen. These sessions are currently inactive.
Total Sessions	Specifies the total number of sessions on this system.
Total RADIUS Access Requests	Specifies the total number of RADIUS access requests seen by RS on this system.
Total RADIUS Access Accepts	Specifies the total number of RADIUS access accepts seen by RS on this system.
Total RADIUS Access Rejects	Specifies the total number of RADIUS response reject frames seen by RS on this system.
Invalid RADIUS Request Packets	Specifies the total number of RADIUS request frames seen by the RS on this system.
Invalid RADIUS Response Packets	Specifies the total number of Invalid RADIUS response frames seen by RS on this system. An invalid frame is generated when request frames do not contain the necessary attributes with the required values for successful processing.
Total Dropped Packets	Specifies the total number of frames dropped by RS on this system.

show radius-snooping session

Use this command to display an RS summary for all sessions or the specified port or MAC address criteria.

Syntax

show radius-snooping session {**port** *port-string* | **mac** *mac-address*}

Parameters

port *port-string*	Specifies the port(s) session to display. Enter *.*.* for all ports.
mac *mac-address*	Specifies the MAC address session to display

Defaults

None.

Mode

All command modes.

Examples

This example displays RADIUS configuration information for port **ge.1.1**:

```
S Chassis(rw)->show radius-snooping session port ge.1.1
MAC Address          Port       Duration
-------------------- ---------- --------------------
00-0E-0C-12-13-14    ge.1.1     00:02:36
```

Table 93-4 Radius-Snooping Session Port Settings

Output...	What it displays...
MAC Address	Specifies the MAC address associated with the session information in this display.
Port	Specifies the port ID associated with the session information in this display.
Duration	Specifies the length of time this session has been active.

This example displays RADIUS configuration information for MAC address 00-00-44-44-00-04:

```
S Chassis(rw)->show radius-snooping session 00-00-44-44-00-04
          MAC Address:    00-00-44-44-00-04
          Port:                      ge.2.8
          Duration:              0, 00:01:47

          Downstream Device IP:  10.21.64.70
          RADIUS Server IP:      10.21.1.150
```

Table 93-5 Radius-Snooping Session MAC Settings

Output...	What it displays...
Port	Specifies the port associated with this MAC address.
MAC Address	Specifies the MAC Address for this session.
Duration	Specifies the length of time that this session has been active.
Downstream device IP	Specifies the IP address of the client associated with this session.
Radius Server IP	Specifies the IP address of the RADIUS server for this session.

94

Auto-Tracking Authentication Commands

This chapter describes the auto-tracking authentication set of commands and how to use them. For information about configuring auto-tracking, refer to the "Authentication Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show auto-tracking	94-1
set auto-tracking	94-2
set auto-tracking accounting	94-4
set auto-tracking port	94-4
clear auto-tracking	94-5
set auto-tracking port authallocated	94-5
set auto-tracking port idle-timeout	94-6
set auto-tracking port radius-timeout-profile	94-7
set auto-tracking port radius-reject-profile	94-7
set auto-tracking port session-timeout	94-8

show auto-tracking

Use this command to display auto-tracking agent state and all ports enabled for the auto-tracking agent or auto-tracking agent state and configuration information for the specified port.

Syntax

show auto-tracking [**port** *port-string*]

Parameters

port *port-string*	(Optional) Specifies the port to display.

Defaults

If no port is specified, a list of all ports enabled for auto-tracking displays.

Mode

All command modes.

Examples

This example shows how to display auto-tracking state on the device and all ports enabled for auto-tracking authentication:

```
S Chassis(rw)->show auto-tracking
Auto Tracking:                          enabled
Auto Tracking Accounting:               disabled
Enabled Ports:
lag.0.6;ge.1.1-46;ge.2.1-47,101-112;tg.3.4-5,8;tg.5.1-15;ge.6.2-46;tg.6.101-104;
ge.7.1-47
```

This example shows how to display auto-tracking agent state and configuration information for LAG **6**:

```
S Chassis(rw)->show auto-tracking port lag.0.6

Auto Tracking:                          enabled

Port            Port State      Session TO Idle TO    Allowed    Allocated
--------------- --------------- ---------- ---------- ---------- ----------
lag.0.6         enabled         0          0          9216       9216
S Chassis(rw)->
```

Table 94-1 provides an explanation of the command output.

Table 94-1 show auto-tracking Output Display

Output...	What it displays...
Auto Tracking	Auto-tracking state: enabled or disabled.
Auto Tracking Accounting	Auto-tracking accounting state: enabled or disabled.
Enabled Ports	Displays all ports enabled for auto-tracking.
Port State	Auto-tracking port state.
Session TO	Auto-tracking session time out value in seconds. If **0**, the auto-tracking session timeout value defaults to the MultiAuth global session time out value as configured by “set multiauth session-timeout” on page 96-14.
Idle TO	Auto-tracking idle time out value in seconds. If **0**, the auto-tracking session timeout value defaults to the MultiAuth global idle time out value as configured by “set multiauth idle-timeout” on page 96-11.
Allowed	The number of auto-tracking sessions allowed on a port.
Allocated	The number of auto-tracking session allocated using “set auto-tracking port authallocated” on page 94-5. Defaults to the number of sessions supported on the port.

set auto-tracking

Use this command to enable or disable auto-tracking on the switch.

Syntax

set auto-tracking {**enable** | **disable**}

Parameters

enable	Enables auto-tracking on the switch.
disable	Disables auto-tracking on the switch.

Defaults

Auto-tracking is disabled by default.

Mode

All command modes.

Usage

The auto-tracking authentication agent must be enabled globally on the switch and locally on the port to be operational on the port. See "set auto-tracking port" on page 94-4 for information on configuring auto-tracking on the port.

The auto-tracking agent is a form of authentication that authenticates those sessions that are not captured by the other supported MultiAuth authentication agents (quarantine, 802.1x, PWA, MAC, CEP, and RADIUS snooping). If auto-tracking is disabled, these sessions are never entered into the session table. Many policy driven switch features depend on the session being in the session table for the feature to interact with the session. It is important that a network administrator have the ability to determine which station addresses on which ports are not being authenticated through traditional MultiAuth methods. Auto-tracking provides the administrator with the ability to assign these session a provisioning result based upon the contents of the admin-policy. Because these sessions can now be tracked, an administrator can determine whether and how to provision them in the future, allowing for increased security and control.

The auto-tracking authentication agent behaves the same as any other authentication agent, with the exception that it always returns an authentication result. By default, the auto-tracking agent has the lowest MultiAuth precedence. The auto-tracking agent is one of the authentication agents from which the authentication provisioning result will be chosen based upon MultiAuth precedence. Each authentication agent attempts to authenticate the user. All authentication agents that return a result are grouped. The authentication agent with the highest MultiAuth precedence is selected to authorize the user. For the default MultiAuth precedence ordering, all other authentication agents must fail to return an authentication result for auto-tracking to be selected. If auto-tracking is the selected authentication method, the admin-policy provisions the user session.

It is recommended that you do not configure auto-tracking authentication for a higher MultiAuth precedence than its default setting of lowest. If a non-auto-tracking authentication agent both returns a result and has a lower MultiAuth precedence, that authentication method will never be used, because auto-tracking always returns a result and has been configured with a higher MultiAuth precedence. The MultiAuth precedence ordering is configured using "set multiauth precedence" on page 96-5.

Examples

This example shows how to enable auto-tracking globally on the switch:

```
S Chassis(rw)->set auto-tracking enable
```

set auto-tracking accounting

Use this command to enable or disable auto-tracking accounting.

Syntax

```
set auto-tracking accounting {enable | disable}
```

Parameters

enable | **disable**	Enables or disables auto-tracking accounting. Auto-tracking accounting is globally disabled by default.

Defaults

Auto-tracking accounting is disabled by default.

Mode

All command modes.

Usage

RADIUS accounting must be enabled using "set radius accounting" on page 86-9 for auto-tracking accounting to take place. RADIUS accounting is disabled by default. If RADIUS accounting is enabled, auto-tracking accounting remains disabled by default.

Examples

This example shows how to enable auto-tracking accounting:

```
S Chassis(rw)->set auto-tracking accounting enable
```

set auto-tracking port

Use this command to configure auto-tracking state on the specified port.

Syntax

```
set auto-tracking port {enable | disable} port-string
```

Parameters

enable	Enables auto-tracking on the specified port.
disable	Disables auto-tracking on the specified port.
port-string	Specifies the port to configure.

Defaults

Auto-tracking is disabled by default on all ports.

Mode

All command modes.

Usage

The auto-tracking agent must be enabled globally on the switch and locally on the port to be operational. See "set auto-tracking" on page 94-2 for information on globally configuring the auto-tracking agent on the switch.

Examples

This example shows how to enable auto-tracking on port **tg.1.1**:

```
S Chassis(rw)->set auto-tracking port enable tg.1.1
```

clear auto-tracking

Use this command to reset auto-tracking state to the default value globally or on the specified port.

Syntax

clear auto-tracking {**all** | **port** *port-string*}

Parameters

all	Resets auto-tracking state globally on the switch to the default value of disabled.
port *port-string*	Specifies the port to reset auto-tracking configuration to the default value of disabled.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to disable auto-tracking globally on the switch:

```
S Chassis(rw)->clear auto-tracking all
```

This example shows how to disable auto-tracking on port tg.1.1:

```
S Chassis(rw)->clear auto-tracking port tg.1.1
```

set auto-tracking port authallocated

Use this command to configure the port maximum number of auto-tracking sessions allowed.

Syntax

set auto-tracking port authallocated *num-users port-string*

Parameters

num-users	Specifies the maximum number of auto-tracking sessions for the specified port. Valid values are **0** - maximum sessions supported. The default value is the number of MultiAuth users per port set by "set multiauth port" on page 96-7.
port-string	Specifies the port to configure.

Defaults

The maximum number of auto-tracking sessions on a port defaults to the number of MultiAuth users per port set by "set multiauth port" on page 96-7. The number of MultiAuth users per port is device dependent. See the release notes that come with your device for the maximum number of supported authenticated sessions.

Mode

All command modes.

Usage

The maximum number of sessions supported on the device is device-dependent. See the release notes that come with your device for the maximum number of authenticated sessions supported on your device.

Use "clear auto-tracking" on page 94-5, specifying the **port** option, to reset the maximum number of users on the port to the default value of 8.

Examples

This example shows how to set the maximum number of auto-tracking authenticated users on port **tg.1.1** to **50**:

```
S Chassis(rw)->set auto-tracking port authallocated 50 tg.1.1
```

set auto-tracking port idle-timeout

Use this command to configure the auto-tracking agent port idle timeout value in seconds.

Syntax

set auto-tracking port idle-timeout *idle-timeout port-string*

Parameters

idle-timeout	Specifies the auto-tracking agent idle timeout in seconds for the specified port. Valid values are **0** - **65535**. Default value is **0** (specifies that the global MultiAuth idle timeout value as set by "set multiauth idle-timeout" on page 96-11 is used.
port-string	The port to configure.

Defaults

The auto-tracking agent port idle timeout defaults to **0**. A value of 0 specifies that the global MultiAuth idle timeout value as set by "set multiauth idle-timeout" on page 96-11 is used. The global MultiAuth idle timeout defaults to 300 seconds.

Mode

All command modes.

Usage

Use "clear auto-tracking" on page 94-5, specifying the **port** option, to reset the auto-tracking agent idle timeout on the port to the default value.

Examples

This example shows how to set the auto-tracking idle timeout value for **port tg.1.1** to **350** seconds:

```
S Chassis(rw)->set auto-tracking port idle-timeout 350 tg.1.1
```

set auto-tracking port radius-timeout-profile

Use this command to configure a the policy profile to use when an authentication attempt results in no response from a RADIUS server used in the configured retransmission algorithm.

Syntax

set auto-tracking port radius-timeout-profile *profile-id port-string*

Parameters

profile-id	Specifies the RADIUS timeout policy profile ID.
port-string	The port to configure.

Defaults

No policy profile is set.

Mode

All command modes.

Usage

The RADIUS timeout profile allows you to provision a session that encounters a RADIUS timeout condition, on a per port basis, with a policy profile other than the default policy. The RADIUS timeout profile allows a MAC address that attempted to authenticate during a RADIUS outage to be dealt with in a non-default manner based upon the contents of the specified policy profile.

Examples

This example shows how to set the auto-tracking RADIUS timeout profile to **10** for port **tg.1.1**:

```
S Chassis(rw)->set auto-tracking port idle-timeout-profile 10 tg.1.1
```

set auto-tracking port radius-reject-profile

Use this command to configure a the policy profile to use when an authentication attempt results in an access reject response from the RADIUS server.

Syntax

set auto-tracking port radius-reject-profile *profile-id port-string*

Parameters

profile-id	Specifies the RADIUS access reject policy profile ID.
port-string	The port to configure.

Defaults

No policy profile is set.

Mode

All command modes.

Usage

The RADIUS access reject profile allows you to provision a session that encounters a RADIUS access reject response from the RADIUS server, on a per port basis, with a policy profile other than the default policy. The RADIUS access reject profile allows a MAC address that was rejected by the RADIUS server to be dealt with in a non-default manner based upon the contents of the specified policy profile.

The RADIUS access reject profile takes precedence over the RADIUS timeout profile configured using "set auto-tracking port radius-timeout-profile" on page 94-7 should a RADIUS timeout take place and a RADIUS access reject has already occurred for this session.

Examples

This example shows how to set the auto-tracking RADIUS access reject profile to **11** for port **tg.1.1**:

```
S Chassis(rw)->set auto-tracking port idle-timeout-profile 11 tg.1.1
```

set auto-tracking port session-timeout

Use this command to configure the auto-tracking port session timeout value in seconds.

Syntax

set auto-tracking port session-timeout *session-timeout port-string*

Parameters

session-timeout	Specifies the auto-tracking session timeout in seconds for the specified port. Valid values are **0** - **65535**. Default value is **0** (specifies that the global MultiAuth session timeout value as set by "set multiauth session-timeout" on page 96-14 is used.
port-string	The port to configure.

Defaults

The auto-tracking port session timeout defaults to **0**. A value of 0 specifies that the global MultiAuth session timeout value as set by "set multiauth session-timeout" on page 96-14 is used. The global MultiAuth session timeout defaults to **0** and specifies that no session timeout is applied to the port.

Mode

All command modes.

Usage

Use "clear auto-tracking" on page 94-5, specifying the **port** option, to reset the port auto-tracking session timeout to the default value.

Examples

This example shows how to set the auto-tracking session timeout value for **port tg.1.1** to **600** seconds:

```
S Chassis(rw)->set auto-tracking port session-timeout 600 tg.1.1
```

95

Anti-Spoofing Commands

This chapter describes the anti-spoofing set of commands and how to use them. For information about configuring anti-spoofing, refer to the "Authentication Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
show antispoof	95-2
set antispoof	95-2
clear antispoof	95-3
set antispoof notifications	95-4
clear antispoof notifications	95-4
set antispoof notifications interval	95-5
clear antispoof notifications interval	95-5
set antispoof duplicateIP	95-6
clear antispoof duplicateIP	95-6
show antispoof class	95-7
set antispoof class	95-8
set antispoof class threshold-index	95-9
clear antispoof class	95-11
set antispoof dhcp-snooping	95-11
set antispoof dhcp-snooping mac-verification	95-13
set antispoof dhcp-snooping port-mode	95-13
clear antispoof dhcp-snooping	95-14
set antispoof arp-inspection	95-15
clear antispoof arp-inspection	95-16
set antispoof ip-inspection	95-17
clear antispoof ip-inspection	95-18
show antispoof port	95-18
set antispoof port-class	95-19
clear antispoof port-class	95-20
show antispoof binding	95-21

For information about...	Refer to page...
clear antispoof binding	95-22
show antispoof counters	95-23
clear antispoof counters	95-24

show antispoof

Use this command to display global anti-spoofing configuration values.

Syntax

show antispoof

Parameters

None.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to display global anti-spoofing configuration values:

```
S Chassis(rw)->show antispoof
Anti-spoof Global State        : disabled
Maximum Number of Classes      : 3
Number of Thresholds Per Class : 6
SNMP Notifications             : enabled
SNMP Notification Interval     : 60
Duplicate IP Control           : disabled
Supported Action Types         : syslog trap quarantine
Supported Binding Types        : DHCP DAI IPSG
S Chassis(rw)->
```

set antispoof

Use this command to globally enable or disable anti-spoofing on the switch.

Syntax

set antispoof {**enable** | **disable**}

Parameters

enable	Globally enable anti-spoofing on the switch.
disable	Globally disable anti-spoofing on the switch (default).

Defaults

Anti-spoofing is globally disabled by default.

Mode

All command modes.

Usage

Anti-spoofing must be globally enabled to be operational on the switch. One or more anti-spoofing features must be enabled on the port for frame snooping to take place. Port enabled anti-spoofing features are:

- DHCP snooping (see "set antispoof dhcp-snooping" on page 95-11)
- DHCP snooping MAC verification (see "set antispoof dhcp-snooping mac-verification" on page 95-13)
- Dynamic ARP inspection (see "set antispoof arp-inspection" on page 95-15)
- IP source guard (see "set antispoof ip-inspection" on page 95-17)

Any action that will be taken when an anti-spoofing violation occurs is configured in an anti-spoofing class (see "set antispoof class" on page 95-8 and "set antispoof class threshold-index" on page 95-9).

Examples

This example shows how to globally enable anti-spoofing on the switch:

```
S Chassis(rw)->set antispoof enable
S Chassis(rw)->
```

clear antispoof

Use this command to reset the anti-spoofing global state or all anti-spoofing configuration to the default value.

Syntax

clear antispoof [**all**]

Parameters

all	(Optional) Resets all anti-spoofing configuration on the switch to default values. You are prompted to confirm that you want to delete all anti-spoofing configuration.

Defaults

If **all** is not specified, anti-spoofing is globally disabled by default. If **all** is specified, all anti-spoofing configuration is set to default values.

Mode

All command modes.

Examples

This example shows how to reset the global anti-spoofing state to the default value of disabled:

```
S Chassis(rw)->clear antispoof
S Chassis(rw)->
```

This example clears all anti-spoofing configuration.

```
S Chassis(rw)->clear antispoof all
Are you sure you want to delete all anti-spoof configuration (y/n) [n]?
S Chassis(rw)->
```

set antispoof notifications

Use this command to enable or disable the sending of anti-spoofing notifications.

Syntax

set antispoof notifications {**enable** | **disable**}

Parameters

enable	Enables the sending of anti-spoofing notifications (default).
disable	Disables the sending of anti-spoofing notifications.

Defaults

The sending of anti-spoofing notifications defaults to enabled.

Mode

All command modes.

Examples

This example shows how to disable the sending of anti-spoofing notifications:

```
S Chassis(rw)->set antispoof notifications disable
```

clear antispoof notifications

Use this command to reset the sending of anti-spoofing notifications setting to the default value.

Syntax

clear antispoof notifications

Parameters

None.

Defaults

The sending of anti-spoofing notifications defaults to enabled.

Mode

All command modes.

Examples

This example shows how to reset the sending of anti-spoofing notifications to the default value of enabled:

```
S Chassis(rw)->clear antispoof notifications
```

set antispoof notifications interval

Use this command to set the interval between the sending of anti-spoofing notifications.

Syntax

set antispoof notifications interval *interval*

Parameters

interval	Specifies the amount of interval in seconds to wait between sending anti-spoofing notifications. Valid values are **0** - **4294967295** seconds. Default value is **60** seconds.

Defaults

The interval between the sending of anti-spoofing notifications defaults to 60 seconds.

Mode

All command modes.

Examples

This example shows how to set the interval between the sending of anti-spoofing notifications to 5 seconds:

```
S Chassis(rw)->set antispoof notifications interval 5
S Chassis(rw)->
```

clear antispoof notifications interval

Use this command to reset the interval between the sending of anti-spoofing notifications to the default value.

Syntax

clear antispoof notifications interval

Parameters

None.

Defaults

The interval between sending of anti-spoofing notifications defaults to 60 seconds.

Mode

All command modes.

Examples

This example shows how to reset the interval between the sending of anti-spoofing notifications of the same type to the same user to the default value of **60** seconds:

```
S Chassis(rw)->clear antispoof notifications interval
S Chassis(rw)->
```

set antispoof duplicateIP

Use this command to enable or disable anti-spoofing duplicate IP address detection.

Syntax

set antispoof duplicateIP {**enable** | **disable**}

Parameters

enable	Enables anti-spoofing duplicate IP address detection.
disable	Disables anti-spoofing duplicate IP address detection.

Defaults

Anti-spoofing duplicate IP address detection defaults to disabled.

Mode

All command modes.

Usage

If duplicate IP address detection is enabled, when new source MAC and IP address bindings are created or a binding currently in the binding table is modified, anti-spoofing runs an IP address lookup on the bindings table to verify that the IP address is not currently in use. If the IP address is currently in use, a Syslog message and trap are sent if notifications are enabled.

Examples

This example shows how to enable anti-spoofing duplicate IP address detection:

```
S Chassis(rw)->set antispoof duplicateIP enable
S Chassis(rw)->
```

clear antispoof duplicateIP

Use this command to reset anti-spoofing duplicate IP address detection to the default value.

Syntax

clear antispoof duplicateIP

Parameters

None.

Defaults

Anti-spoofing duplicate address detection defaults to disabled.

Mode

All command modes.

Examples

This example shows how to reset anti-spoofing duplicate IP address detection to the default value of disabled:

```
S Chassis(rw)->clear antispoof duplicateIP
S Chassis(rw)->
```

show antispoof class

Use this command to display anti-spoofing class information.

Syntax

show antispoof class [*class-index*]

Parameters

class-index	(Optional) Specifies a class index of the anti-spoofing class to display.

Defaults

If a class index is not specified, all anti-spoofing classes display.

Mode

All command modes.

Examples

This example shows how to display information for anti-spoofing class 1:

```
S Chassis(rw)->show antispoof class 1
Anti-spoof Class         : 1
Anti-spoof Class Name    :
Anti-spoof Class Timeout : 0
Index  Value  Sys Trap Quar Quarantine-Profile
-----  -----  ---- ---- ---- ------------------
    1     24  ena  ena  ena                 15
    2      0  dis  dis  dis                  0
    3      0  dis  dis  dis                  0
    4      0  dis  dis  dis                  0
    5      0  dis  dis  dis                  0
    6      0  dis  dis  dis                  0
```

```
S Chassis(rw)->
```

Table 95-1 provides an explanation of the command output.

Table 95-1 show antispoof class Output Display

Output...	What it displays...
Anti-spoof Class	Anti-spoofing class index (see "set antispoof class" on page 95-8).
Anti-spoof Class Name	Anti-spoofing class name. If not configured, this field is blank (see "set antispoof class" on page 95-8).
Anti-spoof Class Timeout	Timeout for bindings associated with this class (see "set antispoof class" on page 95-8).
Index	Threshold index (see "set antispoof class threshold-index" on page 95-9).
Value	The threshold value for the number of IP address changes detected by anti-spoofing for this threshold index (see "set antispoof class threshold-index" on page 95-9).
Sys	Syslog action state: enabled (ena) or disabled (dis) (see "set antispoof class threshold-index" on page 95-9).
Trap	SNMP notification (trap) action state: enabled (ena) or disabled (dis) (see "set antispoof class threshold-index" on page 95-9).
Quar	Quarantine action state: enabled (ena) or disabled (dis) (see "set antispoof class threshold-index" on page 95-9).
Quarantine-Profile	The quarantine profile index value assigned to this threshold index. This policy profile is applied when quarantine action is enabled. (See "set antispoof class threshold-index" on page 95-9.)

set antispoof class

Use this command to configure an anti-spoofing port class name or timeout value.

Syntax

set antispoof class *class-index* {**name** *name* | **timeout** *timeout*}

Parameters

class-index	Specifies the class index that uniquely identifies the anti-spoofing class. Valid values are **1** - **3**.
name *name*	Specifies a descriptive name for this class of up to 32 printable characters.
timeout *timeout*	Specifies a timeout value, in seconds, after which bindings associated with the class reset counters. Valid values are **0** - **4294967295** seconds. The default value is **600** seconds.

Defaults

- If an anti-spoofing class name is not specified, the name defaults to a NULL string.
- The anti-spoofing class threshold reset timeout defaults to **600** seconds.

Mode

All command modes.

Usage

An anti-spoofing class determines the action to be taken when anti-spoofing violations on a port reach the configured threshold. This command sets the class name and timeout value. See "set antispoof class threshold-index" on page 95-9 for details on configuring class thresholds and actions.

Examples

This example shows how to set the anti-spoofing class index **1** name to **antispoof1**:

```
S Chassis(rw)->set antispoof class 1 name antispoof1
```

This example shows how to set the anti-spoofing class index **1** timeout value to **6000**:

```
S Chassis(rw)->set antispoof class 1 timeout 6000
```

set antispoof class threshold-index

Use this command to configure thresholds and actions for an anti-spoofing port class.

Syntax

set antispoof class *class-index* **threshold-index** *thresh-index* [**threshold-value** *thresh-value*] [**quarantine-profile** *quar-profile*] [**action** {[**syslog**] [**trap**] [**quarantine**]}]

Parameters

class-index	Specifies the class index of the threshold index to configure. Valid values are **1** - **3**.
thresh-index	Specifies the anti-spoofing class threshold index to configure. Valid values are **1** - **6**.
threshold-value *thresh-value*	Specifies the aggregate number of changes for any enabled anti-spoofing type on the port to trigger the configured action. Valid values are **0** - **65535**. Default value is **0** (threshold is disabled).
quarantine-profile *quar-profile*	Specifies the quarantine policy profile index associated with this class.
action	The anti-spoofing class actions to be taken if the threshold value for this threshold is reached. Specifying an action type enables that action.
syslog	Specifies that a Syslog message is sent if the threshold value is reached.
trap	Specifies that a notification is sent if the threshold value is reached.
quarantine	Specifies that the quarantine policy profile as configured by quarantine-profile is applied if the threshold value is reached.

Defaults

- The class threshold-value defaults to 0 (threshold is disabled).
- The class quarantine-profile defaults to 0 (quarantine is disabled).

- If no action is specified, no action will be taken if the threshold is met. All actions default to disabled.

Mode

All command modes.

Usage

There are three anti-spoofing detection types: DHCP snooping, dynamic ARP inspection, and IP source guard. Each anti-spoofing detection type can be enabled on a port. Each port enabled anti-spoofing detection type tracks actionable anti-spoofing violations on the port based upon the detection type:

- **DHCP snooping** – A DHCP packet has been received on an untrusted switch port. Valid DHCP assigned addresses for clients on untrusted ports are determined by snooping DHCP server packets on trusted ports.
- **Dynamic ARP inspection** – An ARP packet has been received with a sender and target MAC to IP address binding that does not agree with a binding entry in the source MAC address to source IP address table.
- **IP source guard** – An IP packet has been received on the port with a source MAC and IP address that does not agree with a binding entry in the source MAC address to source IP address table.

An anti-spoofing class specifies one or more actions to be taken when the number of actionable violations configured in a class threshold occur on the port within the class timeout interval. The class timeout is configured using "set antispoof class" on page 95-8.

Anti-spoofing supports the configuration of up to 3 classes. Each port can be configured with a single class. If you only have a single anti-spoofing detection type enabled on the port, DHCP snooping for example, the action class thresholds and actions can be set for that anti-spoofing detection type. If multiple anti-spoofing types are configured on a port, DHCP snooping and dynamic ARP inspection for example, the class thresholds and actions must take into account any combination of anti-spoofing events for the configured anti-spoofing types.

Action CLI entries are not additive. Any specified action overwrites any previous class action configuration.

If the quarantine action is specified, ensure that a quarantine policy has been created and associated with the threshold. Extreme Networks **highly recommends that you use quarantine policies to classify the user traffic upon violation hits.** Quarantine policy profiles are configured using "set policy profile" on page 43-4. Policy rules using "set policy rule" on page 43-23 can be associated with the quarantine policy profile. The admin profile is not supported in a quarantine context.

Examples

This example shows how to configure class threshold **1** of class **1** with a threshold value of **1** and actions to send Syslog messages, to send notifications, and to apply quarantine policy profile **1**:

```
S Chassis(rw)->set antispoof class 1 threshold-index 1 threshold-value 1
quarantine-profile 1 action syslog trap quarantine
```

clear antispoof class

Use this command to clear anti-spoofing class configuration.

Syntax

clear antispoof class *class-index* [**name**] [**timeout**] [**threshold-index** *thresh-index*]

Parameters

class-index	Specifies the class index value.
name	(Optional) Specifies the current name value is reset to the default value of NULL string.
timeout	(Optional) Specifies the timeout value is reset to the default of **600** seconds.
threshold-index *thresh-index*	(Optional) Specifies the threshold index to be reset to the default value of **0** (no threshold is applied).

Defaults

If no option is specified, all configuration for the specified class index is cleared. If an option is specified, only the specified option is affected.

Mode

All command modes.

Examples

This example shows how to clear all configuration for the anti-spoofing class index **1**:

```
S Chassis(rw)->clear antispoof class 1
```

This example shows how to reset threshold index **1** configuration to the default threshold values for the anti-spoofing class index **1**:

```
S Chassis(rw)->clear antispoof class 1 threshold-index 1
```

This example shows how to reset the timeout value for for the anti-spoofing class index **1** to the default value of **600**:

```
S Chassis(rw)->clear antispoof class 1 timeout
```

set antispoof dhcp-snooping

Use this command to globally enable or disable the DHCP snooping anti-spoofing feature on the specified port.

Syntax

set antispoof dhcp-snooping {**enable** | **disable**} *port-string*

Parameters

enable	Enables DHCP snooping on the specified port.
disable	Disables DHCP snooping on the specified port.
port-string	The port or port range.

Defaults

DHCP snooping defaults to disabled on all ports.

Mode

All command modes.

Usage

Malicious users can spoof DHCP server response packets allowing them to give false information to a user for such fields as the default gateway or domain name resolution server. Unauthorized servers can mis-configure clients so that client traffic goes through the wrong gateway, allowing an attacker access to that traffic or for purposes of denying a client access to network resources. A malicious user can send packets from the same source MAC address requesting IPs for different users by changing the client hardware address field in the DHCP packet.

The DHCP acknowledgement packet contains the authoritative user MAC and IP addresses. By enabling DHCP snooping on a port, when a DHCP acknowledgement packet is received, if the port is trusted and the user's MAC address has been authenticated and exists in the multiauth session table, a source MAC address to source IP address binding for the user is created and populated in the source MAC address to IP address binding table.

DHCP acknowledgement packets received on an untrusted port are recorded, but allowed to be further processed. Anti-spoofing tracks client DHCP assigned addresses on untrusted ports by snooping DHCP server packets on trusted ports as described above. If a client packet address is not in the binding table, a violation occurs. If the class action threshold is met, actions taken are based upon the class configuration assigned to that port. The class is configured using "set antispoof class threshold-index" on page 95-9. The class is assigned to the port using "set antispoof port-class" on page 95-19.

DHCP snooping port mode determines the anti-spoofing behavior towards traffic traversing the port. Port mode can be set to trusted, untrusted or bypass. See "set antispoof dhcp-snooping port-mode" on page 95-13 for port mode details. DHCP server acknowledgement messages only populate the source MAC to IP address table on trusted ports. DHCP server acknowledgement messages on bypass ports are ignored for purposes of populating the source MAC to IP address table. Untrusted ports should have a policy configuration that will drop DHCP server packets on that port.

When a DHCP server message contains a new user IP address for a MAC address binding for which the binding's lease has not expired, a Syslog message is sent, but the threshold violation counter is not incremented.

If dynamic ARP inspection (see "set antispoof arp-inspection" on page 95-15) or IP source guard (see "set antispoof ip-inspection" on page 95-17) are set to disabled (default) or inspection only, DHCP snooping must be enabled for a source MAC to IP address binding to be created.

Note: If IP source guard and dynamic ARP inspection are disabled or configured for inspection only away from the edge of a network, DHCP exchange packets could be missed due, for example, to link loss at the distribution or core layer. DHCP renewals from end users at the edge may not occur and the binding table would not be repopulated. Be aware that, under these circumstances, users could suffer unintended threshold violations and be denied network resources.

Source MAC to IP address bindings will timeout if:

- The DHCP lease expires
- A DHCP release frame is received on the port
- A manual clear is entered using "clear antispoof binding" on page 95-22

Examples

This example shows how to enable DHCP snooping on port **ge.1.2**:

```
S Chassis(rw)->set antispoof dhcp-snooping enable ge.1.2
```

set antispoof dhcp-snooping mac-verification

Use this command to enable or disable the DHCP snooping MAC verification on the specified port or port range.

Syntax

set antispoof dhcp-snooping mac-verification {**enable** | **disable**} *port-string*

Parameters

enable	Enables DHCP snooping MAC verification on the specified port or port range.
disable	Disables DHCP snooping MAC verification on the specified port or port range.
port-string	Specifies the port or port range.

Defaults

DHCP snooping MAC verification is disabled by default on all ports.

Mode

All command modes.

Usage

The DHCP client packet contains an L2 source MAC address and an L3 client hardware address. With DHCP snooping MAC verification enabled, DHCP snooping verifies that the source MAC address and the client hardware address match in DHCP client packets that transit untrusted ports. If the addresses do not match, the packet is dropped. DHCP MAC verification is a network edge feature that should be enabled on ports transited by client packets from the intended client. For DHCP snooping MAC verification to be operational:

- DHCP snooping must be enabled using "set antispoof dhcp-snooping" on page 95-11
- The port must be set to untrusted using "set antispoof dhcp-snooping port-mode" on page 95-13

Examples

This example shows how to enable DHCP snooping MAC verification on port ge.1.2:

```
S Chassis(rw)->set antispoof dhcp-snooping mac-verification ge.1.2
```

set antispoof dhcp-snooping port-mode

Use this command to set the DHCP snooping port mode on the specified port or port range.

Syntax

set antispoof dhcp-snooping port-mode {**trusted** | **bypass** | **untrusted**} *port-string*

Parameters

trusted	Source MAC address and source IP addresses of DHCP server acknowledgment messages will be used to populate the source MAC address and source IP address binding table.
bypass	DHCP server packets are ignored for purposes of populating the source MAC address and source IP address binding table.
untrusted	DHCP server packets received on the port increment the untrusted server counter.
port-string	Specifies the port or port range.

Defaults

DHCP snooping port mode defaults to untrusted on all ports.

Mode

All command modes.

Usage

In a DHCP snooping context, there are three configurable port modes that determine anti-spoofing behavior:

Trusted – When port mode is set to trusted, DHCP server traffic is accepted and used to create bindings in the source MAC address to IP address binding table for the user. Binding verification does not take place on trusted ports.

Bypass – When port mode is set to bypass, snooping of DHCP server traffic does not take place on the port.

Untrusted – When port mode is set to untrusted, the untrusted server counter is incremented when DHCP server traffic is detected on the port.

Note: Untrusted ports should have a policy configuration that will drop DHCP server packets on that port.

Bindings created as a result of DHCP exchanges on trusted ports using DHCP snooping take precedence over bindings created through dynamic ARP inspection or IP source guard.

Examples

This example shows how to set the DHCP snooping port mode on port **ge.1.2** to trusted:

```
S Chassis(rw)->set antispoof dhcp-snooping port-mode trusted ge.1.2
S Chassis(rw)->
```

clear antispoof dhcp-snooping

Use this command to clear the anti-spoofing DHCP snooping configuration for the specified port or port range.

Syntax

clear antispoof dhcp-snooping {**mac-verification** *port-string* | **port-mode** *port-string* | *port-string*}

Parameters

mac-verification *port-string*	Specifies the port or port range for anti-spoofing DHCP snooping MAC verification to be reset to the default value of disabled.
port-mode *port-string*	Specifies the port or port range for the anti-spoofing DHCP snooping port mode to be reset to the default value of untrusted.
port-string	Specifies the port or port range for the anti-spoofing DHCP snooping state to be reset to the default value of disabled.

Defaults

- Anti-spoofing DHCP snooping is disabled on all ports by default.
- Anti-spoofing DHCP snooping port mode defaults to untrusted on all ports.
- Anti-spoofing DHCP snooping MAC verification defaults to disabled on all ports.

Mode

All command modes.

Examples

This example shows how to reset anti-spoofing DHCP snooping to the default state of disabled on port **ge.1.2**:

```
S Chassis(rw)->clear antispoof dhcp-snooping ge.1.2
```

This example shows how to reset anti-spoofing DHCP snooping port mode to the default value of untrusted on port **ge.1.2**:

```
S Chassis(rw)->clear antispoof dhcp-snooping port-mode ge.1.2
```

set antispoof arp-inspection

Use this command to enable or disable dynamic ARP inspection (DAI) on a port or range of ports.

Syntax

set antispoof arp-inspection {**enable** | **disable** | **inspection-only**} *port-string*

Parameters

enable	Enables dynamic ARP inspection on the specified port or ports.
disable	Disables dynamic ARP inspection on the specified port or ports
inspection-only	Specifies that dynamic ARP inspection will inspect ARP packets, but will not populate the source MAC address to source IP address binding table.
port-string	The port to configure for anti-spoofing ARP inspection.

Defaults

Anti-spoofing ARP inspection is disabled on all ports by default.

Mode

All command modes.

Usage

Man-in-the-middle (MITM) attacks can take advantage of ARP, allowing a hacker to redirect user traffic through his own device to and from the default gateway. This redirected packet can be used by the hacker to spy on the private information being sent from the user. Using gratuitous ARP replies, an attacker can manipulate other devices' ARP tables such that the attacker appears to be another user to a gateway or the gateway to other users on the network.

With anti-spoofing ARP inspection enabled, a source MAC address to source IP address binding database is utilized to ensure that ARP packets have legitimate source MAC address to source IP bindings. When ARP packets enter the switch, the source MAC address and source IP address are compared to the entry in the source MAC to IP address binding table. If the packet data conflicts with the table, the IP change causes the anti-spoofing threshold counter to increment. If the threshold is met, any configured actions are taken against the user. Actions can include sending a Syslog message, sending a notification, or quarantining the user based upon a quarantine policy. Thresholds and actions are configured in an anti-spoofing class using "set antispoof class threshold-index" on page 95-9

When DAI is enabled, the sender and target MAC and IP address bindings are inspected for reply packets and the sender MAC and IP address bindings are inspected for request packets. This information is used to populate the binding table. If DAI is enabled and the user's MAC address has been authenticated and exists in the multiauth session table, an entry in the binding table will be created. If DAI is set to inspection only, packets are only inspected and a new binding is not entered into the binding table. Successfully limiting reception of ARP packets to the bound addresses in the binding table prevents a malicious user from inserting itself between the end user and a gateway, poisoning a network device's ARP cache or performing MITM attacks.

Examples

This example shows how to enable anti-spoofing ARP inspection on ports **ge.1.2** through **ge.1.5**:

```
S Chassis(rw)->set antispoof arp-inspection enable ge.1.2-5
```

This example shows how to configure anti-spoofing ARP inspection on ports **ge.1.2** through **ge.1.5** for packet inspection only:

```
S Chassis(rw)->set antispoof arp-inspection inspection-only ge.1.2-5
```

clear antispoof arp-inspection

Use this command to reset anti-spoofing ARP inspection to the default value on a port or range of ports.

Syntax

clear antispoof arp-inspection *port-string*

Parameters

port-string	The port on which anti-spoofing ARP inspection is cleared.

Defaults

Anti-spoofing ARP inspection is disabled on all ports by default.

Mode

All command modes.

Examples

This example shows how to reset anti-spoofing ARP inspection on ports **ge.1.2** through **ge.1.5** to the default value of disabled:

```
S Chassis(rw)->clear antispoof arp-inspection ge.1.2-5
```

set antispoof ip-inspection

Use this command to enable or disable anti-spoofing IP source guard on a port or range of ports.

Syntax

set antispoof ip-inspection {**enable** | **disable** | **inspection-only**} *port-string*

Parameters

enable	Enables anti-spoofing IP source guard on the specified port or ports.
disable	Disables anti-spoofing IP source guard on the specified port or ports.
inspection-only	Specifies that packets will be snooped, but anti-spoofing IP source guard will not be used to populate the source MAC address to source IP address binding table.
port-string	The port to configure for anti-spoofing IP source guard.

Defaults

Anti-spoofing IP address inspection is disabled on all ports by default.

Mode

All command modes.

Usage

A malicious user can spoof a user's IP address, allowing the malicious user to bypass security features on the network based on a user's subnet, such as authentication based upon IP address. The malicious user would then have access to network resources that would otherwise be denied to the user. Such a user could flood a victim with traffic from many different source IP addresses for the purpose of denying other users access to network resources.

When IP source guard is enabled, all IP packets are inspected. The source MAC address and source IP address are compared against the contents of the binding table, and a check is performed to ensure that the user's MAC address has been authenticated and exists in the multiauth session table.

If the address combination is not currently in the binding table and the user's MAC address has been authenticated and exists in the multiauth session table, a new entry for this address combination is added to the binding table. If the address combination is not currently in the binding table the violation counter is incremented. If the threshold is met, any configured actions are taken against the user. Actions can include sending a Syslog message, sending a notification, or quarantining the user based upon a quarantine policy. Thresholds and actions are configured in an anti-spoofing class using "set antispoof class threshold-index" on page 95-9.

When IP source guard is enabled, packets are both inspected and used to populate the source MAC address to IP address binding table. If IP source guard is set to inspection only, packets are only inspected and a new binding is not entered into the binding table. Reception of IP packets on the switch is limited to the bound addresses in the binding table.

Enabling IP source guard allows anti-spoofing protection when a switch resides outside of the DHCP or ARP server paths.

Examples

This example shows how to enable anti-spoofing IP address inspection on ports **ge.1.2** through **ge.1.5**:

```
S Chassis(rw)->set antispoof ip-inspection enable ge.1.2-5
```

This example shows how to configure anti-spoofing IP address inspection on ports **ge.1.2** through **ge.1.5** for packet inspection only:

```
S Chassis(rw)->set antispoof ip-inspection inspection-only ge.1.2-5
```

clear antispoof ip-inspection

Use this command to reset anti-spoofing IP address inspection to the default value on a port or range of ports.

Syntax

clear antispoof ip-inspection *port-string*

Parameters

port-string	The port on which anti-spoofing IP address inspection is cleared.

Defaults

Anti-spoofing IP address inspection is disabled on all ports by default.

Mode

All command modes.

Examples

This example shows how to reset anti-spoofing IP address inspection on ports **ge.1.2** through **ge.1.5** to the default value of disabled:

```
S Chassis(rw)->clear antispoof ip-inspection ge.1.2-5
```

show antispoof port

Use this command to display anti-spoofing port configuration.

Syntax

show antispoof port [*port-string*] [**-interesting**]

Parameters

port-string	(Optional) Specifies the port or port range to display
-interesting	(Optional) Only display ports configured for anti-spoofing.

Defaults

If no option is specified, all ports display.

Mode

All command modes.

Examples

This example shows how to display anti-spoofing port configuration for port **ge.2.5**:

```
S Chassis(rw)->show antispoof port ge.2.5
Port      Type      DHCP MacV    ArpInsp     IpInsp Class Untrusted-Counter
--------  --------- ---- ----  ---------  --------- ----- -----------------
ge.2.5    Untrusted  dis  dis    enabled    enabled     2                 0
S Chassis(rw)->
```

This example shows how to display anti-spoofing port configuration for all ports configured for anti-spoofing:

```
S Chassis(rw)->show antispoof port -interesting
Port      Type      DHCP MacV    ArpInsp     IpInsp Class Untrusted-Counter
--------  --------- ---- ----  ---------  --------- ----- -----------------
ge.2.5    Untrusted  dis  dis    enabled    enabled     2                 0
ge.2.6    Untrusted  dis  dis    enabled    enabled     2                 0
ge.2.7    Untrusted  dis  dis    enabled    enabled     2                 0
ge.2.8    Untrusted  dis  dis    enabled    enabled     2                 0
S Chassis(rw)->
```

Table 95-2 provides an explanation of the command output.

Table 95-2 show antispoof port Output Display

Output...	What it displays...
Port	The port for the displayed anti-spoofing configuration information.
Type	DHCP snooping port type: trusted, bypass, or untrusted
DHCP	DHCP snooping state: enabled (ena) or disabled (dis).
MacV	DHCP MAC address Verification state: enabled (ena) or disabled (dis).
ArpInsp	ARP inspection state: enabled (ena) or disabled (dis).
IpInsp	IP address inspection state: enabled (ena) or disabled (dis).
Class	Anti-spoofing class index value.
Untrusted-Counter	Number of DHCP packets received on the port if port-mode is set to untrusted.

set antispoof port-class

Use this command to assign an anti-spoofing class to a port or range of ports.

Syntax

set antispoof port-class *class-index port-string*

Parameters

class-index	Specifies an anti-spoofing class index to assign to the specified port or port range.
port-string	Specifies the port or port range to which the specified class is assigned.

Defaults

None.

Mode

All command modes.

Usage

Anti-spoofing classes configure the threshold of anti-spoofing violations that trigger an action as well as the action to take. Once a class is assigned to a port, if a violation threshold is reached on the port, the configured actions will be performed. See "set antispoof class threshold-index" on page 95-9 for class configuration details. Use this command to assign a class to a port.

Examples

This example shows how to assign anti-spoofing class index 1 to port **ge.1.2**:

```
S Chassis(rw)->set antispoof port-class 1 ge.1.2
```

clear antispoof port-class

Use this command to remove the anti-spoofing class from the specified port or port range.

Syntax

clear antispoof port-class *port-string*

Parameters

port-string	Specifies the port or port range to clear.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to delete the anti-spoofing port class configuration for port **ge.1.2**:

```
S Chassis(rw)->clear antispoof port-class ge.1.2
```

show antispoof binding

Use this command to display anti-spoofing source MAC address to source IP address bindings.

Syntax

show antispoof binding [**port** *port-string*] [**mac** *mac-addr*] [**ip** *ip-addr*] [**all**] [**-verbose**]

Parameters

port *port-string*	(Optional) Display anti-spoofing source MAC address to source IP address bindings information for the specified port or port range.
mac *mac-addr*	(Optional) Display anti-spoofing source MAC address to source IP address binding information for the specified source MAC address.
ip *ip-addr*	(Optional) Display anti-spoofing source MAC address to source IP address binding information for the specified source IP address.
all	(Optional) Display anti-spoofing source MAC address to source IP address binding information for all terminated and active entries.
-verbose	(Optional) Display a detailed level of information.

Defaults

- If no binding option is specified, all bindings display.
- If the **-verbose** option is not specified, a standard level of information displays.

Mode

All command modes.

Examples

This example shows how to display all anti-spoofing source MAC to source IP address bindings on the switch:

```
S Chassis(rw)->show antispoof binding
MAC Address             IP Address        Port  Assignment Type
-----------------  ---------------  ----------  ---------------
00-05-01-00-00-00          1.2.3.5     ge.1.47             IPSG
00-05-02-00-00-00          1.2.3.4     ge.1.48             IPSG
S Chassis(rw)->
```

This example shows how to display a detailed level of information for all anti-spoofing source MAC to source IP address bindings on the switch:

```
S Chassis(rw)->show antispoof binding -verbose
MAC Address      : 00-05-01-00-00-00
IP Address       : 1.2.3.5
Port             : ge.1.47
Assignment Type  : IPSG
Duration Time    : 6313 seconds
Expiration Time  : 65535 seconds
```

```
MAC Address       : 00-05-02-00-00-00
IP Address        : 1.2.3.4
Port              : ge.1.48
Assignment Type   : IPSG
Duration Time     : 6313 seconds
Expiration Time   : 65535 seconds
S Chassis(rw)->
```

Table 95-3 provides an explanation of the command output.

Table 95-3 show antispoof port Output Display

Output...	What it displays...
MAC Address	Binding source MAC address.
IP Address	Binding source IP address.
Port	Port associated with the binding source MAC and IP addresses.
Assignment Type	Anti-spoofing type that created the binding: • **DAI** – Dynamic ARP inspection • **DHCP** – DHCP snooping • **IPSG** – IP source guard
Duration Time	The elapsed time since the binding was created or the timer period reset on the port. This time resets to 0 when it reaches the expiration time.
Expiration Time	The anti-spoofing port class timeout or lease expiration if the binding is a DHCP binding. Threshold violation counters reset when this timeout expires.

clear antispoof binding

Use this command to delete an anti-spoofing user source MAC address to source IP address binding from the binding table.

Syntax

clear antispoof binding {**port** *port-string* | **mac** *mac-addr* | **ip** *ip-addr*}

Parameters

port *port-string*	Clears anti-spoofing user binding for the specified port or port range.
mac *mac-addr*	Clears anti-spoofing user binding for the specified source MAC address. Valid MAC address formats are *xx-xx-xx-xx-xx-xx* or *xx:xx:xx:xx:xx:xx* where *x* is a hex value.
ip *ip-addr*	Clears anti-spoofing user binding for the specified source IP address.

Defaults

None.

Mode

All command modes.

Usage

Use "show antispoof binding" on page 95-21 to display the contents of the source MAC address to source IP address binding table.

Examples

This example shows how to delete the anti-spoofing user binding for port **ge.1.2** from the source MAC address to source IP address binding table:

```
S Chassis(rw)->clear antispoof binding port ge.1.2
```

show antispoof counters

Use this command to display anti-spoofing statistics.

Syntax

show antispoof counters [**port** *port-string*] [**mac** *mac-addr*] [**ip** *ip-addr*] [**all**] [**-verbose**]

Parameters

port *port-string*	(Optional) Display anti-spoofing statistics for the specified port or port range.
mac *mac-addr*	(Optional) Display anti-spoofing statistics for the specified source MAC address.
ip *ip-addr*	(Optional) Display anti-spoofing statistics for the specified source IP address.
all	(Optional) Display anti-spoofing statistics for all ports (same as no options specified).
-verbose	(Optional) Display a detailed level of information.

Defaults

- If no binding option is specified, all bindings display.
- If the **-verbose** option is not specified, a standard level of information displays.

Mode

All command modes.

Examples

This example shows how to display all anti-spoofing statistics on the switch:

```
S Chassis(rw)->show antispoof counters
MAC Address             IP Address        Port    IP Count
-----------------  ---------------  ----------  ----------
00-05-01-00-00-00          1.2.3.5     ge.1.47           0
00-05-02-00-00-00          1.2.3.4     ge.1.48           0

S Chassis(rw)->
```

This example shows how to display detailed anti-spoofing statistics:

```
S Chassis(rw)->show antispoof counters -verbose
MAC Address       : 00-05-01-00-00-00
IP Address        : 1.2.3.5
Port              : ge.1.47
IP Counter        : 0

MAC Address       : 00-05-02-00-00-00
IP Address        : 1.2.3.4
Port              : ge.1.48
IP Counter        : 0

S Chassis(rw)->
```

Table 95-4 provides an explanation of the command output.

Table 95-4 show antispoof port Output Display

Output...	What it displays...
MAC Address	Specifies the source MAC address for the displayed statistics
IP Address	Binding source IP address.
Port	Port associated with the binding source MAC and IP addresses.
IP Count(er)	Specifies the number of IP address changes for this source MAC address.

clear antispoof counters

Use this command to reset the anti-spoofing threshold counters to 0 by port, MAC address, or IP address.

Syntax

clear antispoof counters {**port** *port-string* | **mac** *mac-addr* | **ip** *ip-addr*}

Parameters

port *port-string*	Clears anti-spoofing class threshold counters for the specified port or port range.
mac *mac-addr*	Clears anti-spoofing class threshold counters for the specified source MAC address. Valid MAC address formats are *xx-xx-xx-xx-xx-xx* or *xx:xx:xx:xx:xx:xx* where *x* is a hex value.
ip *ip-addr*	Clears anti-spoofing class threshold counters for the specified source IP address.

Defaults

None.

Mode

All command modes.

Usage

Use "show antispoof counters" on page 95-23 to display class threshold counters.

Examples

This example shows how to reset the anti-spoofing class threshold values to **0** for port **ge.1.2**:

```
S Chassis(rw)->clear antispoof counters port ge.1.2
```

96

MultiAuth Commands

This chapter describes the MultiAuth set of commands and how to use them. For information about configuring MultiAuth, refer to the "Authentication Configuration" chapter of the *Extreme Networks S-Series Configuration Guide*.

For information about...	Refer to page...
set multiauth mode	96-2
clear multiauth mode	96-2
show multiauth	96-3
show multiauth counters	96-4
set multiauth precedence	96-5
clear multiauth precedence	96-6
show multiauth port	96-6
set multiauth port	96-7
clear multiauth port	96-8
show multiauth station	96-8
clear multiauth station	96-9
show multiauth session	96-9
show multiauth idle-timeout	96-11
set multiauth idle-timeout	96-11
clear multiauth idle-timeout	96-12
show multiauth session-timeout	96-13
set multiauth session-timeout	96-14
clear multiauth session-timeout	96-15
clear multiauth session	96-16
set multiauth sessions-unique-per-port	96-17
clear multiauth sessions-unique-per-port	96-17
set multiauth trap	96-18
clear multiauth trap	96-19
show multiauth trap	96-19

Note: Multiple authentication mode must be globally enabled on the device using the **set multiauth mode** command as described in “set multiauth mode” on page 96-2.

set multiauth mode

Use this command to set the system authentication mode to use multiple authenticators simultaneously or to strictly adhere to 802.1X.

Syntax

```
set multiauth mode {multi | strict}
```

Parameters

multi	Allows the system to use multiple authenticators simultaneously.
strict	Sets the system authentication mode to strict 802.1X.

Defaults

None.

Mode

All command modes.

Usage

In order for multiple authentication to function on the device, each possible method of authentication must be enabled globally and configured appropriately on the desired ports per its corresponding command set as described in:

- Chapter 89, **802.1X Authentication Commands** for 802.1x
- Chapter 90, **Port Web Authentication (PWA) Commands** for PWA
- Chapter 91, **MAC Authentication Commands** for MAC authentication
- Chapter 92, **Convergence End Points (CEP) Phone Detection Commands** for CEP
- Chapter 93, **RADIUS Snooping Commands** for radius-snooping

Example

This example shows how to enable multiple authentication:

```
S Chassis(rw)->set multiauth mode multi
```

clear multiauth mode

Use this command to clear the system authentication mode.

Syntax

```
clear multiauth mode
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

This command resets the system authentication mode to the default value of **strict**. Strict mode limits authentication to 802.1x for a single user on a port.

Example

This example shows how to clear the system authentication mode:

```
S Chassis(rw)->clear multiauth mode
```

show multiauth

Use this command to display system-configured MultiAuth values.

Syntax

show multiauth

Parameters

None.

Defaults

None.

Mode

All command modes.

Example

This example shows how to display multiple authentication session-timeout values, for an active session:

```
S Chassis(su)->show multiauth
Multiple authentication system configuration
-------------------------------------------------
Supported types           : dot1x, pwa, mac, cep, radius-snooping, auto-tracking,
quarantine-agent
Maximum number of users       : 8192
Current number of users       : 2
System mode                   : multi
Sessions-Unique-Per-Port Admin: disabled
Sessions-Unique-Per-Port Oper : disabled
Reauth Timeout Action         : terminate
Default precedence            : quarantine-agent, dot1x, pwa, mac, cep,
radius-snooping, auto-tracking
```

```
Admin precedence              :
Operational precedence        : quarantine-agent, dot1x, pwa, mac, cep,
radius-snooping, auto-tracking
```

show multiauth counters

Use this command to display MultiAuth counter values.

Syntax

show multiauth counters [[**cep** | **dot1x** | **mac** | **pwa** | **radius-snooping**] [**chassis**] | **port** *port-string*]]

Parameters

cep	Displays CEP authentication MultiAuth statistics.
dot1x	Displays 802.1x authentication MultiAuth statistics.
mac	Displays MAC authentication MultiAuth statistics.
pwa	Displays PWA authentication MultiAuth statistics.
radius-snooping	Displays radius-snooping MutliAuth statistics.
port-string	Specifies a port or range of ports to display.

Defaults

Displays MultiAuth counter information for all parameters.

Mode

All command modes.

Example

This example shows how to display multiple authentication session-timeout values, for an active session:

```
S Chassis(su)->show multiauth counters
Location   Authentication Type
           dot1x      pwa        mac        cep
           ---------- ---------- ---------- ----------
chassis    0          0          0          0
ge.1.1     0          0          0          0
ge.1.2     0          0          0          0
.
.
.
lag.0.45   0          0          0          0
lag.0.46   0          0          0          0
lag.0.47   0          0          0          0
lag.0.48   0          0          0          0
```

set multiauth precedence

Use this command to set the system's multiple authentication administrative precedence.

Syntax

```
set multiauth precedence {[quarantine-agent] [dot1x] [pwa] [mac] [cep]
[radius-snooping] [auto-tracking]}
```

Parameters

quarantine-agent	Sets precedence for the quarantine-agent authentication.
dot1x	Sets precedence for 802.1X authentication.
pwa	Sets precedence for port web authentication.
mac	Sets precedence for MAC authentication.
cep	Sets precedence for CEP authentication.
radius-snooping	Sets precedence for radius-snooping.
auto-tracking	Sets precedence for auto-tracking authentication.

Defaults

From high to low precedence: **quarantine-agent**, **dot1x**, **pwa**, **mac**, **cep**, **radius-snooping**, **auto-tracking**.

Mode

All command modes.

Usage

When a user is successfully authenticated by more than one method at the same time, the precedence of the authentication methods will determine which RADIUS-returned filter ID will be processed and result in an applied traffic policy profile.

MultiAuth authentication precedence defaults to the following order from high to low: quarantine-agent, 802.1x, PWA, MAC, CEP, radius-snooping, auto-tracking. You may change the precedence for one or more methods by setting the authentication methods in the order of precedence from high to low. Any methods not entered are given a lower precedence than the methods entered in their pre-existing order. For instance, if you start with the default order and only set quarantine-agent, PWA and MAC, the new precedence order will be quarantine-agent, PWA, MAC, 802.1x, CEP, and auto-tracking.

Note: It is recommended that if you are using the quarantine-agent authentication method that it always have the highest precedence. It is also highly recommended that you keep the auto-tracking authentication method at the lowest precedence, otherwise all lower precedence authentication methods will be excluded.

Example

This example shows how to set precedence from highest to lowest for **quarantine-agent** and **MAC** authentication (the new order of precedence will be quarantine-agent, MAC, 802.1x, PWA, CEP, and auto-tracking):

```
S Chassis(rw)->set multiauth precedence quarantine-agent mac
```

clear multiauth precedence

Use this command to clear the system's multiple authentication administrative precedence.

Syntax

clear multiauth precedence

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

This command resets the multiauth precedence order to the default value of: quarantine-agent, 802.1x, PWA, MAC, CEP, radius-snooping, auto-tracking.

Example

This example shows how to clear the multiple authentication precedence:

```
S Chassis(rw)->clear multiauth precedence
```

show multiauth port

Use this command to display multiple authentication properties for one or more ports.

Syntax

show multiauth port [*port-string*]

Parameters

port-string	(Optional) Displays multiple authentication information for specific port(s).

Defaults

If *port-string* is not specified, multiple authentication information will be displayed for all ports.

Mode

All command modes.

Example

This example shows how to display multiple authentication information for all ports:

```
S Chassis(rw)->show multiauth port
Port         Mode           Max       Allowed    Current
                           users       users      users
```

```
------------ ------------ ---------- ---------- ----------
ge.1.1       auth-opt     8          8          0
ge.1.2       auth-opt     8          8          0
ge.1.3       auth-opt     8          8          0
.
.
.
lag.0.60     auth-opt     128        128        0
lag.0.61     auth-opt     128        128        0
lag.0.62     auth-opt     128        128        0
```

set multiauth port

Use this command to set multiple authentication properties for one or more ports.

Syntax

set multiauth port {**mode** {**auth-opt** | **auth-reqd** | **force-auth** | **force-unauth**} | **numusers** *numusers port-string*}

Parameters

mode auth-opt | **auth-reqd** | **force-auth** | **force-unauth**	Specifies the port(s)' multiple authentication mode as: • **auth-opt** — Authentication optional • **auth-reqd** — Authentication required • **force-auth** — Authentication considered • **force-unauth** — Authentication disabled
numusers *numusers*	Specifies the number of users allowed authentication on port(s).
port-string	Specifies the port(s) on which to set multiple authentication properties.

Defaults

None.

Mode

All command modes.

Usage

S-Series modules support up to 128 authenticated users per port by default. The maximum number of users supported on a port is 2024.

Use the **numusers** parameter to increase the number of users beyond the default value.

Examples

This example shows how to set the port multiple authentication mode to required on ge.3.14:

```
S Chassis(rw)->set multiauth port mode auth-reqd ge.3.14
```

clear multiauth port

Use this command to clear multiple authentication properties for one or more ports.

Syntax

clear multiauth port {**mode** | **numusers**} *port-string*

Parameters

mode	Clears the port(s)' multiple authentication mode.
numusers	Clears the value set for the number of users allowed authentication on port(s).
port-string	Specifies the port(s) on which to clear multiple authentication properties.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to clear the port multiple authentication mode on all 1-Gigabit Ethernet ports:

```
S Chassis(rw)->clear multiauth port mode ge.*.*
```

show multiauth station

Use this command to display multiple authentication station (end user) entries.

Syntax

show multiauth station [**mac** *address*] [**port** *port-string*]

Parameters

mac *address*	(Optional) Displays multiple authentication station entries for specific MAC address(es).
port *port-string*	(Optional) Displays multiple authentication station entries for specific port(s).

Defaults

If no options are specified, multiple authentication station entries will be displayed for all MAC addresses and ports.

Mode

All command modes.

Example

This example shows how to display multiple authentication station entries. In this case, two end user MAC addresses are shown:

```
S Chassis(rw)->show multiauth station
Port         Address type Address
------------ ------------ ------------------------
ge.1.20      mac          00-10-a4-9e-24-87
ge.2.16      mac          00-b0-d0-e5-0c-d0
```

clear multiauth station

Use this command to clear one or more multiple authentication station entries.

Syntax

clear multiauth station {[**mac** *address*] [**port** *port-string*]}

Parameters

mac *address*	Clears multiple authentication station entries for specific MAC address(es).
port *port-string*	Specifies the port(s) for which to clear multiple authentication station entries.

Defaults

None.

Mode

All command modes.

Example

This example shows how to clear the multiple authentication station entry associated with port ge.1.20:

```
S Chassis(rw)->clear multiauth station port ge.1.20
```

show multiauth session

Use this command to display multiple authentication session entries.

Syntax

show multiauth session [**all**] [**agent** {**quarantine-agent** | **dot1x** | **mac** | **pwa** | **cep** | **radius-snooping** | **auto-tracking**}] [**mac** *address*] [**port** *port-string*]

Parameters

all	(Optional) Displays information about all sessions, including those with terminated status.

agent quarantine-agent | **dot1x** | **mac** | **pwa** | **cep** | **radius-snooping** | **auto-tracking**	(Optional) Displays quarantine-agent, 802.1X, MAC, CEP, port web authentication, radius-snooping, or auto-tracking session information.
mac *address*	(Optional) Displays multiple authentication session entries for specific MAC address(es).
port *port-string*	(Optional) Displays multiple authentication session entries for specific port(s).

Defaults

If no options are specified, multiple authentication session entries will be displayed for all sessions, authentication types, MAC addresses, and ports.

Mode

All command modes.

Example

This example shows how to display auto-tracking agent multiple authentication session information:

```
S Chassis(rw)->show multiauth session agent auto-tracking

Multiple authentication session entries
---------------------------------------

Port            : ge.7.18        Station address   : 00-00-ac-d3-32-01
Auth status     : success        Last attempt      : TUE OCT 02 15:45:00 2012
Agent type      : auto-tracking  Session applied   : true
Server type     : radius         VLAN-Tunnel-Attr  : None
Policy index    : 4              Policy name       : Guest Access (active)
Session timeout : 300            Session duration  : 0,00:03:24
Idle timeout    : 120            Idle time         : 0,00:00:00
Termination time: Not Terminated
Auth Server IP  : 172.10.3.100

Port            : ge.7.18        Station address   : 00-00-ac-d3-32-02
Auth status     : success        Last attempt      : TUE OCT 02 15:44:57 2012
Agent type      : auto-tracking  Session applied   : true
Server type     : radius         VLAN-Tunnel-Attr  : None
Policy index    : 4              Policy name       : Guest Access (active)
Session timeout : 300            Session duration  : 0,00:03:27
Idle timeout    : 120            Idle time         : 0,00:00:00
Termination time: Not Terminated
Auth Server IP  : 172.10.3.100
.
.
```

```
.
S Chassis(rw)->
```

show multiauth idle-timeout

Use this command to display the multiple authentication timeout value for an idle session.

Syntax

show multiauth idle-timeout

Parameters

None.

Defaults

None.

Mode

All command modes.

Usage

This will display the idle-timeout values, in seconds, for the following authentication types: dot1x, pwa, mac, cep, and radius-snooping.

Example

This example shows how to display timeout values for an idle session, for each of the authentication types:

```
S Chassis(rw)->show multiauth idle-timeout
Authentication type  Timeout (sec)
-------------------- -------------
dot1x                300
pwa                  300
mac                  300
cep                  300
radius-snooping      300
auto-tracking        300
quarantine-agent     300
```

set multiauth idle-timeout

Use this command to set the maximum number of consecutive seconds an authenticated session may be idle before termination of the session.

Syntax

set multiauth idle-timeout [**quarantine-agent** | **dot1x** | **pwa** | **mac** | **cep** | **radius-snooping** | **auto-tracking**] *timeout*

Parameters

quarantine-agent	(Optional) Specifies the authentication type quarantine-agent.
dot1x	(Optional) Specifies the authentication type IEEE 802.1X Port-Based Network Access Control.
pwa	(Optional) Specifies the authentication type Port Web Authentication (PWA).
mac	(Optional) Specifies the authentication type Mac authentication.
cep	(Optional) Specifies the authentication type Convergence End Point (CEP) authentication.
radius-snooping	(Optional) Specifies the authentication type radius-snooping authentication.
auto-tracking	(Optional) Specifies the authentication type auto-tracking.
timeout	Specifies the timeout value in seconds. The value can range from 0 to 65535. A value of 0 means that no idle timeout will be applied unless an idle timeout value is provided by the authenticating server. The default timeout value is 300 seconds.

Defaults

If no authentication method is specified, the timeout value is set for all methods.

Mode

All command modes.

Usage

A value of zero indicates that no idle timeout will be applied unless an idle timeout value is provided by the authenticating server. For example, if a session is authenticated by a RADIUS server, that server may encode a Idle-Timeout Attribute in its authentication response.

Examples

This example shows how to set the idle-timeout session for cep and mac authentication to 500 seconds:

```
S Chassis(rw)->set multiauth idle-timeout cep 500
S Chassis(rw)->set multiauth idle-timeout mac 500
```

This example shows how to set the idle-timeout session for all the authentication types to 400 seconds:

```
S Chassis(rw)->set multiauth idle-timeout 400
```

clear multiauth idle-timeout

Use this command to reset the maximum number of consecutive seconds an authenticated session may be idle before termination of the session to the default value of 300 seconds.

Syntax

clear multiauth idle-timeout [**quarantine-agent** | **cep** | **dot1x** | **mac** | **pwa** | **radius-snooping** | **auto-tracking**]

Parameters

quarantine-agent	(Optional) Specifies the authentication type quarantine-agent.
cep	(Optional) Specifies the authentication type Convergence End Point (CEP) Authentication.
dot1x	(Optional) Specifies the authentication type IEEE 802.1X Port-Based Network Access Control.
mac	(Optional) Specifies the authentication type Mac authentication.
pwa	(Optional) Specifies the authentication type Port Web Authentication (PWA).
radius-snooping	(Optional) Specifies the authentication type radius-snooping authentication.
auto-tracking	(Optional) Specifies the authentication type auto-tracking.

Defaults

If no authentication type is specified, the idle timeout value is returned to 300 seconds for all authentication types.

Mode

All command modes.

Examples

This example shows how to clear the idle-timeout session values for cep and mac authentication types, back to the default value of 300 seconds:

```
S Chassis(rw)->clear multiauth idle-timeout cep
S Chassis(rw)->clear multiauth idle-timeout mac
```

This example shows how to clear the idle-timeout session values for all authentication types, back to the default value of 300 seconds:

```
S Chassis(rw)->set multiauth idle-timeout
```

show multiauth session-timeout

Use this command to display session-timeout values, in seconds, for all authentication methods.

Syntax

show multiauth session-timeout

Parameters

None

Defaults

None.

Mode

All command modes.

Example

This example shows how to display multiple authentication session-timeout values, for an active session:

```
S Chassis(rw)->show multiauth session-timeout
Authentication type  Timeout (sec)
-------------------- -------------
dot1x                0
pwa                  0
mac                  0
cep                  0
radius-snooping      0
auto-tracking        0
quarantine-agent     0
S Chassis(rw)->
```

set multiauth session-timeout

Use this command to set the maximum number of seconds an authenticated session may last before termination of the session.

Syntax

set multiauth session-timeout [**quarantine-agent** | **cep** | **dot1x** | **mac** | **pwa** | **radius-snooping** | **auto-tracking**] *timeout*

Parameters

quarantine-agent	(Optional) Specifies the authentication type quarantine-agent.
cep	(Optional) Specifies the authentication type Convergence End Point (CEP) authentication.
dot1x	(Optional) Specifies the authentication type IEEE 802.1X Port-Based Network Access Control.
mac	(Optional) Specifies the authentication type Mac authentication.
pwa	(Optional) Specifies the authentication type Port Web Authentication (PWA).
radius-snooping	(Optional) Specifies the authentication type radius-snooping authentication.
auto-tracking	(Optional) Specifies the authentication type auto-tracking.
timeout	Specifies the timeout value in seconds. The value can range from **0** to **65535**. A value of **0** means that no session timeout will be applied unless a session timeout value is provided by the authenticating server. The default value is **0**.

Defaults

If no authentication type is specified, the timeout value is set for all types.

The session timeout defaults to 0 (no session timeout is applied).

Mode

All command modes.

Usage

A value of zero may be superseded by a session timeout value provided by the authenticating server. For example, if a session is authenticated by a RADIUS server, that server may encode a Session-Timeout Attribute in its authentication response.

Examples

This example shows how to set the session-timeout value for an active session, for cep and mac authentication to 500 seconds:

```
S Chassis(rw)->set multiauth session-timeout cep 500
S Chassis(rw)->set multiauth session-timeout mac 500
```

This example shows how to set the session-timeout value for an active session, for all the authentication types to 600 seconds:

```
S Chassis(rw)->set multiauth session-timeout 600
```

clear multiauth session-timeout

Use this command to clear session-timeout values, for one or all authentication methods, back to the default values.

Syntax

clear multiauth session-timeout [**quarantine-agent** | **cep** | **dot1x** | **mac** | **pwa** | **radius-snooping** | **auto-tracking**]

Parameters

quarantine-agent	(Optional) Specifies the authentication type quarantine-agent.
cep	(Optional) Specifies the authentication type Convergence End Point (CEP) authentication.
dot1x	(Optional) Specifies the authentication type IEEE 802.1X Port-Based Network Access Control.
mac	(Optional) Specifies the authentication type Mac authentication.
pwa	(Optional) Specifies the authentication type Port Web Authentication (PWA).
radius-snooping	(Optional) Specifies the authentication type radius-snooping authentication.
auto-tracking	(Optional) Specifies the authentication type auto-tracking.

Defaults

If no authentication type is specified, the session timeout value is returned to 0 (no session timeout is applied) for all authentication types.

Mode

All command modes.

Examples

This example shows how to clear the session-timeout values, for an active session, for cep and mac authentication types, to the default value of 300 seconds:

```
S Chassis(rw)->clear multiauth idle-timeout cep
S Chassis(rw)->clear multiauth idle-timeout mac
```

This example shows how to clear the session-timeout values, for an active session, for all authentication types, to the default value of 300 seconds:

```
S Chassis(rw)->clear multiauth idle-timeout
```

clear multiauth session

Use this command to clear multiauth sessions for the specified MAC address and port.

Syntax

clear multiauth session *mac-address port-string* [**quarantine-agent** | **cep** | **dot1x** | **mac** | **pwa** | **radius-snooping** | **auto-tracking**]

Parameters

mac-address	Specifies the MAC address of the session to clear.
port-string	Specifies the port of the session to clear.
quarantine-agent	(Optional) Specifies the authentication type quarantine-agent.
cep	(Optional) Specifies the authentication type Convergence End Point (CEP) authentication.
dot1x	(Optional) Specifies the authentication type IEEE 802.1X Port-Based Network Access Control.
mac	(Optional) Specifies the authentication type Mac authentication.
pwa	(Optional) Specifies the authentication type Port Web Authentication (PWA).
radius-snooping	(Optional) Specifies the authentication type radius-snooping authentication.
auto-tracking	(Optional) Specifies the authentication type auto-tracking.

Defaults

If no authentication agent is specified, all sessions for the specified MAC address and port are cleared. Otherwise, only sessions for the specified authentication agent are cleared.

Mode

All command modes.

Examples

This example shows how to clear the session-timeout values, for an active session, for cep and mac authentication types, to the default value of 300 seconds:

```
S Chassis(rw)->clear multiauth idle-timeout cep
S Chassis(rw)->clear multiauth idle-timeout mac
```

This example shows how to clear the session-timeout values, for an active session, for all authentication types, to the default value of 300 seconds:

```
S Chassis(rw)->clear multiauth idle-timeout
```

set multiauth sessions-unique-per-port

Use this command to enable or disable the MultiAuth authentication sessions unique per port configuration.

Syntax

```
set multiauth sessions-unique-per-port {enabled | disabled}
```

Parameters

enabled	Enables the MultiAuth authentication sessions unique per port configuration. Defaults to **enabled**.
disabled	Disables the MultiAuth authentication sessions unique per port configuration.

Defaults

MultiAuth sessions unique per port configuration is enabled by default.

Mode

All command modes.

Usage

When MultiAuth sessions unique per port configuration is enabled when a MultiAuth session roams from one port to another port, the session authenticates on the new port.

When MultiAuth sessions unique per port is disabled, a multiauth session moves, or roams, from one port to another port on the same system without having to authenticate. All session information maintained, only the port where the session is establish is changed and displayed in the **show multiauth session** command output.

Examples

This example shows how to disable MultiAuth sessions unique per port configuration allowing a session to roam from one port to another without reauthenticating:

```
S Chassis(rw)->set multiauth sessions-unique-per-port disabled
S Chassis(rw)->
```

clear multiauth sessions-unique-per-port

Use this command to reset the MultiAuth sessions unique per port configuration to the default value.

Syntax

```
clear multiauth sessions-unique-per-port
```

Parameters

None.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to reset the MultiAuth sessions unique per port configuration to the default behavior of authenticating a session each time it moves between ports:

```
S Chassis(rw)->clear multiauth sessions-unique-per-port
S Chassis(rw)->
```

set multiauth trap

Use this command to set the MultiAuth trap setting for system, module and port.

Syntax

set multiauth trap {**system** {**enabled** | **disabled**} | **module** {**enabled** | **disabled**} | **port** *portstring* {**all** | **success** | **failed** | **terminated** | **max-reached**}}

Parameters

system	Configures MultiAuth system trap settings as follows: **enabled** - traps are sent when max users reached in system **disabled** - traps are not sent when max users reached in system
module	Configures MultiAuth module trap settings as follows: **enabled** - traps are sent when max users reached in module **disabled** - traps are not sent when max users reached in module
port *portstring*	Configures MultiAuth port trap settings for the port specified in *portstring*.
all	Enables sending all traps for the specified port.
success	Enables sending success traps for the specified port.
failed	Enables sending failed traps for the specified port.
terminated	Enables sending terminated traps for the specified port.
max-reached	Enables sending max number users reached traps for the specified port.

Defaults

All sending of MultiAuth traps disabled.

Mode

All command modes.

Examples

This example shows how to enable the MultiAuth system trap setting:

```
S Chassis(rw)->set multiauth trap system enabled
```

This example shows how to enable all MultiAuth port trap setting:

```
S Chassis(rw)->set multiauth trap port ge.1.1 all
```

clear multiauth trap

Use this command to clear the system's multiple authentication trap settings.

Syntax

clear multiauth trap {**system** | **module** | **port** *portstring* {**all** | **success** | **failed** | **terminated** | **max-reached**}}

Parameters

port *portstring*	Clears the configuration of MultiAuth port trap settings for the port specified in *portstring*.
all	Enables sending all traps for the specified port.
success	Enables sending success traps for the specified port.
failed	Enables sending failed traps for the specified port.
terminated	Enables sending terminated traps for the specified port.
max-reached	Enables sending max number users reached traps for the specified port.

Defaults

None.

Mode

All command modes.

Examples

This example shows how to disable the MultiAuth system trap setting:

```
S Chassis(rw)->clear multiauth trap system
```

This example shows how to disable all MultiAuth port trap settings:

```
S Chassis(rw)->clear multiauth trap port ge.1.1 all
```

show multiauth trap

Use this command to display multiple authentication trap settings for the specified context.

Syntax

show multiauth trap [**system** | **module** | **port** *portstring*]

Parameters

system	Displays the multiple authentication trap system setting.
module	Displays the multiple authentication trap module setting.
port *portstring*	Displays the configuration setting for MultiAuth port traps for the port specified in *portstring*.

Defaults

If no parameter is specified, statistics for all traps are displayed.

Mode

All command modes.

Example

This example shows how to display multiple authentication trap settings for port ge.1.1-4:

```
S Chassis(rw)->show multiauth trap port ge.1.1-4
Location       Trap configuration
               Success     Failed      Terminated  Max-Reached
-------------  ----------  ----------  ----------  ----------
ge.1.1         Disabled    Disabled    Disabled    Disabled
ge.1.2         Disabled    Disabled    Disabled    Disabled
ge.1.3         Disabled    Disabled    Disabled    Disabled
ge.1.4         Disabled    Disabled    Disabled    Disabled

S Chassis(rw)->
```

This example shows how to display the multiple authentication trap system setting:

```
S Chassis(rw)->show multiauth trap system
System : Disabled
S Chassis(rw)->
```