Extreme SLX-OS Command Reference, 20.7.1

Supporting ExtremeRouting and ExtremeSwitching SLX 9740, SLX 9640, SLX 9540, SLX 9250, SLX 9150, Extreme 8820, Extreme 8720, and Extreme 8520

9039216-00 Rev AA
March 2025

Copyright © 2025 Extreme Networks, Inc. All rights reserved.

Legal Notice

Extreme 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 on Extreme Networks trademarks, see: https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

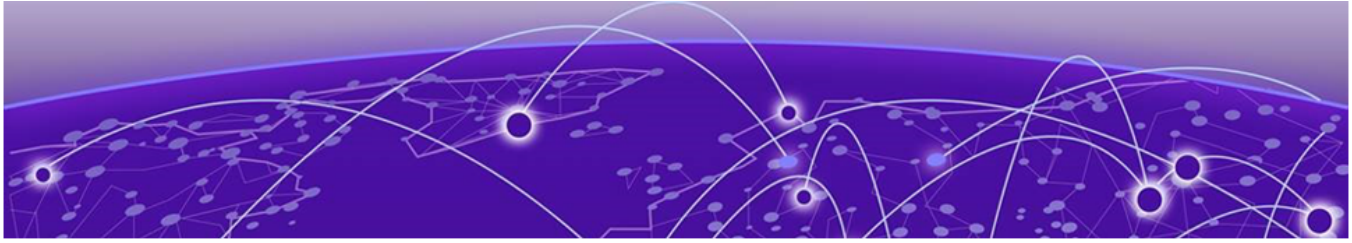


Table of Contents

Preface **41**
- Text Conventions 41
- Documentation and Training 43
  - Open Source Declarations 43
  - Training 43
- Help and Support 43
  - Subscribe to Product Announcements 44
- Send Feedback 44

About This Document **45**
- What's New in This Document 45
  - New commands 45
  - Modified commands 45
  - Deprecated commands 46
- Supported Hardware 46

Using the SLX-OS CLI **47**
- User accounts 47
- Accessing the CLI 48
- Command modes 48
  - Privileged EXEC mode 48
  - Global configuration mode 48
  - Using the do command as a shortcut 49
  - Using the top command as a shortcut 49
- Displaying CLI commands and command syntax 49
- Completing CLI commands 50
- Using the comment character ! 51
- CLI keyboard shortcuts 52
- Using CLI command output modifiers 52
- Unsupported input characters 53
- Debug and system diagnostic commands 53
- Command shortcuts (aliases) 53
  - Configuring global aliases 54
  - Configuring user-level aliases 54

Commands A - B **55**
- aaa accounting 58
- aaa authentication 61
- aaa authorization command 65
- accept-lifetime 67
- accept-tolerance 69
- action (management-heartbeat) 70
- acl-log-raslog 72

acl-mirror ... 74
acl-policy ... 76
action event-stream ... 77
action python-script ... 78
action-profile ... 80
Parameters: ... 80
action-timeout ... 81
activate (telemetry collector) ... 82
activate (telemetry server) ... 83
activate (VXLAN overlay gateway) ... 84
adaptive ... 85
add (telemetry) ... 87
additional-paths ... 89
additional-paths select ... 91
address-family ipv4 flowspec ... 93
address-family l2vpn evpn (BGP) ... 95
address-family unicast (BGP) ... 96
address-family unicast (IS-IS) ... 98
adjustment-interval ... 99
adjustment-threshold ... 100
admin-group ... 101
advertise capabilities ac-influenced-df-election ... 103
Supported In ... 103
advertise dot1-tlv ... 105
advertise dot3-tlv ... 106
advertise optional-tlv ... 107
advertise-backup ... 109
advertise-best-external ... 110
advertisement-interval (VRRP) ... 111
advertisement-interval-scale ... 112
agent-enable ... 114
Platform Availability ... 114
agent-port ... 115
Platform Availability ... 115
agent-uuid ... 116
Platform Availability ... 116
aggregate-address (BGP) ... 117
alias ... 119
alias-config ... 121
allow-conflicting-rules ... 122
allow-duplicate-rules ... 124
allow multiple-ep-per-port ... 126
always-compare-med ... 127
always-propagate ... 128
anycast-rp ... 130
area authentication (OSPFv3) ... 132
area nssa (OSPFv2) ... 134
area nssa (OSPFv3) ... 136
area prefix-list (OSPFv2) ... 138

area range (OSPFv2) 140
area range (OSPFv3) 142
area stub (OSPFv2) 144
area stub (OSPFv3) 146
area virtual-link (OSPFv2) 148
area virtual-link (OSPFv3) 150
area virtual-link authentication (OSPFv3) 152
arp 154
arp access-list 156
as-path-ignore 158
auth-check 159
auth-key 161
auth-mode 163
auth-port 165
auto-cost reference-bandwidth (OSPFv2) 166
auto-cost reference-bandwidth (OSPFv3) 168
auto-shutdown-new-neighbors 170
autobw-threshold table 171
backup-advertisement-interval 172
bandwidth-ceiling 173
banner 175
beacon enable 176
bestpath prefix-validation disable 178
bestpath prefix-validation disallow-invalid 179
bfd 180
bfd holdover-interval 182
bfd interval 184
bfd max-session-support 186
bfd shutdown 187
bgp-redistribute-internal 188
bmc 189
bmc factory reset 190
bpdu-drop-enable 191
breakout mode 192
bridge-domain 195
bridge-domain (EVPN) 197
bridge-priority 199
bsr-candidate 200
bypass-lsp 202
bypass-lsp (Telemetry) 203

Commands C - D 204

capability as4-enable 210
ccm-interval 211
cee-map 212
certutil import sshkey 213
certutil sshkey 215
certutil sshx509v3 217
cfm linktrace 219
cfm loopback 221

cfm y1731 domain 223
Parameters: 223
channel-group 224
chassis 227
cipherset 228
cisco-interoperability 230
class 231
class-map 233
clear arp 234
clear bfd neighbors 235
clear bgp evpn l2routes 236
clear bgp evpn local routes 237
clear bgp evpn neighbor 238
clear bgp evpn neighbor dynamic all 240
clear bgp evpn routes 241
clear bgp ip flowspec local 243
clear bgp ip flowspec neighbor 244
clear bgp ip flowspec routes 246
clear bgp ip neighbor ipv6 247
clear cfm y1731 client-signal-fail statistics 249
clear cfm y1731 statistics 250
clear cfm y1731 statistics delay-measurement 251
clear cfm y1731 statistics synthetic-loss-measurement 252
clear counters 253
clear counters access-list 254
clear counters access-list overlay type vxlan 257
clear counters storm-control 258
clear dot1x statistics 260
clear erp statistics 261
clear erp wtb-time 262
clear erp wtr-time 263
clear filter-change-update 264
clear ip arp inspection statistics 265
clear ip arp suppression-cache 266
clear ip arp suppression-statistics 267
clear ip bgp dampening 268
clear ip bgp flap-statistics 269
clear ip bgp local routes 270
clear ip bgp neighbor 271
clear ip bgp neighbor dynamic 273
clear ip bgp routes 274
clear ip bgp rpki server 275
clear ip bgp traffic 276
clear ip dhcp relay statistics 277
clear ip dhcp snooping binding 278
clear ip flowspec rules statistics 279
clear ip igmp groups 280
clear ip igmp statistics 281
clear ip multicast snooping mcache 282

clear ip pim mdt 283
clear ip ospf 284
clear ip route 286
clear ipv6 bgp dampening 287
clear ipv6 bgp flap-statistics 288
clear ipv6 bgp local routes 289
clear ipv6 bgp neighbor 290
clear ipv6 bgp neighbor dynamic 292
clear ipv6 bgp routes 293
clear ipv6 bgp traffic 294
clear ipv6 counters 295
clear ipv6 dhcp relay delegated-prefixes 296
clear ipv6 dhcp relay statistics 298
clear ipv6 mld groups 299
clear ipv6 mld snooping 301
clear ipv6 mld statistics 302
clear ipv6 multicast snooping mcache 303
clear ipv6 nd suppression-cache 304
clear ipv6 nd suppression-statistics 305
clear ipv6 neighbor 306
clear ipv6 ospf 307
clear ipv6 pim mcache 309
clear ipv6 pim rp-map 310
clear ipv6 pim traffic 311
clear ipv6 route 312
clear ipv6 vrrp statistics 313
clear isis all 315
clear isis counts 316
clear isis database 317
clear isis force-spf 318
clear isis force-v6spf 319
clear isis ipv6 spf-log 320
clear isis neighbor 321
clear isis route 322
clear isis spf-log 323
clear isis traffic 324
clear lacp 325
clear lacp counters 326
clear link-oam statistics 327
clear lldp neighbors 328
clear lldp statistics 330
clear logging raslog 332
clear loop-detection 334
clear loop-detection bridge-domain 335
clear mac-address-table 336
clear mpls auto-bandwidth-samples 338
clear mpls lsp 339
clear mpls statistics 340
clear mvrp statistics 342

clear overlay-gateway 343
clear policy-map-counters 344
clear qos flowcontrol statistics 345
clear spanning-tree counter 346
clear spanning-tree detected-protocols 347
clear statistics bridge-domain 348
clear statistics vlan 349
clear tm voq-stat ingress-device 350
clear tm voq-stat slot 351
clear tunnel statistics 352
clear udld statistics 353
clear vrrp statistics 354
CLI 356
client 359
client-interface 360
client-interface (Y1731) 361
client-interfaces-shutdown 363
client-pw 364
client-to-client-reflection 365
clock set 367
clock timezone 368
cluster 369
cluster-client auto 370
cluster-track 372
commit 374
compare-med-empty-aspath 375
compare-routerid 376
confederation identifier 377
confederation peers 378
configure terminal 379
config-drift-track 380
connector 381
control-word 382
console 384
copy 386
core-isolation-disable 389
core-isolation-track 390
cos (MPLS) 392
cos (Y1731) 394
convergence-time 395
crypto ca authenticate 396
crypto ca enroll 398
crypto ca import 400
crypto ca import-pkcs 402
crypto ca trustpoint 405
crypto cert expiry-level 406
crypto import 408
crypto key 410
csnp-interval 412

cspf-computation-mode ... 413
cspf-interface-constraint ... 415
cspf-group ... 416
cspf-group-computation ... 417
dampening ... 419
database-overflow-interval (OSPFv2) ... 421
database-overflow-interval (OSPFv3) ... 423
debug access-list-log buffer ... 425
debug arp packet buffer ... 426
debug dhcp packet buffer ... 428
debug dot1x packet ... 430
debug ip bgp ... 432
debug ip bgp neighbor ... 435
debug ip igmp ... 437
debug ip ospf shortcuts ... 439
debug ip pim ... 440
debug ipv6 bgp ... 442
debug ipv6 bgp neighbor ... 444
debug ipv6 dhcp pd ... 446
debug ipv6 mld ... 447
debug ipv6 ospf graceful-restart ... 449
debug ipv6 pim ... 450
debug lacp ... 452
debug lldp dump ... 454
debug lldp packet ... 455
debug spanning-tree ... 457
debug udld packet ... 459
default-information-originate (BGP) ... 461
default-information-originate (IS-IS) ... 462
default-information-originate (OSPFv2) ... 463
default-information-originate (OSPFv3) ... 465
default-ipv6-gateway ... 467
default-link-metric ... 469
default-local-preference ... 471
default-metric (BGP) ... 472
default-metric (IS-IS) ... 473
default-metric (OSPF) ... 474
default-passive-interface ... 475
delay ... 476
delay-link-event ... 477
delete ... 479
delete-packet ... 480
deploy ... 482
description (BD) ... 484
description (event-handler) ... 485
description (interfaces) ... 486
description (LLDP) ... 487
description (STP) ... 488
description (VRRP) ... 489

designated-forwarder-hold-time ... 490
destination ... 491
dhcp ztp cancel ... 492
dhcp ztp log ... 493
dir ... 495
default-metric (IS-IS) ... 496
disable-adjacency-check ... 497
disable-incremental-spf-opt ... 498
disable-inc-stct-spf-opt ... 499
disable-partial-spf-opt ... 500
disallow-oar-ac ... 501
discard-packet ... 502
discard-voq-packet ... 504
distance (BGP) ... 506
distance (IS-IS) ... 507
distance (OSPF) ... 508
distribute ... 510
distribute-list prefix-list (OSPFv3) ... 511
distribute-list route-map ... 512
domain-name ... 513
dot1ag-compliance ... 514
dot1x authentication ... 515
dot1x enable ... 516
dot1x filter-strict-security ... 517
dot1x max-req ... 519
dot1x port-control ... 520
dot1x quiet-period ... 522
dot1x reauthenticate ... 523
dot1x reauthentication ... 524
dot1x reauthMax ... 525
dot1x test eapol-capable ... 526
dot1x test timeout ... 527
dot1x timeout ... 528
dpod ... 530
dscp (QoS) ... 532
dscp (Tunnel) ... 534
dscp-ttl-mode ... 535
duplicate-mac-timer (EVPN default instance) ... 536
dynamic-bypass ... 537

Commands E - F ... 539

efa deploy ... 541
enable ... 544
enable (ERP) ... 545
enable (GRUB) ... 546
enable (maintenance mode) ... 548
enable-on-reboot (maintenance mode) ... 549
enable (management-heartbeat) ... 550
encryption-level ... 552
enable-all-interfaces ... 553

enforce-first-as 554
eol 555
erp 556
error-disable-timeout enable 557
error-disable-timeout interval 558
esi 560
esi (BGP EVPN Multi-homing) 562
ethernet-segment 563
event 564
event-handler 566
event-handler abort action 568
event-handler activate 569
evpn 572
exclude-any 573
exclude-interface 575
exp 577
export-vrf-leaked-routes 579
export-map 580
extend bridge-domain 581
extend vlan 582
external-lsdb-limit (OSPFv2) 583
external-lsdb-limit (OSPFv3) 584
facility-backup 585
fast-convergence 587
fast-external-fallover 588
fast-flood 589
fastboot 590
fast-wtr-time 591
fec mode 592
fec (telemetry) 594
filter-change-update-delay 595
filter-fec-in 596
filter-fec-out 598
firmware activate 599
firmware commit 600
firmware download 601
firmware download ftp 604
firmware download fullinstall 606
firmware download interactive 609
firmware download scp 611
firmware download sftp 613
firmware download tftp 615
firmware download usb 617
firmware peripheral-update cpld 619
firmware peripheral-update fpga 620
firmware recover 621
firmware restore 622
flex-cli show link-fault-signaling 623
flex-cli show local-fault interface 624

Parameters ... 624
flex-cli show local-fault slot ... 625
Parameters ... 625
flex-cli show remote-fault interface ... 626
Parameters ... 626
flex-cli show remote-fault slot ... 627
Parameters ... 627
flow-label ... 628
flowspec validation ... 629
force-switch ... 631
format RFC-5424 ... 632
forward-delay ... 634
default-metric (IS-IS) ... 636
default-metric (IS-IS) ... 637

Commands G - J ... 638

gNMI Server Configuration ... 644
graceful-restart (BGP) ... 645
graceful-restart (LDP) ... 648
graceful-restart (OSPFv2) ... 649
graceful-restart (OSPFv3) ... 651
graceful-restart helper (OSPFv3) ... 652
graceful-restart helper-disable (IS-IS) ... 653
graceful-shutdown ... 654
grub ... 656
guard-time ... 657
handle-isis-neighbor-down ... 658
hardware ... 660
hardware media-database activate ... 661
hardware smt ... 662
hello (LLDP) ... 663
hello (MPLS RSVP) ... 665
hello (UDLD) ... 667
hello padding ... 668
hello-acknowledgements ... 670
hello-interval (LD) ... 671
hello-interval (LDP) ... 672
hello-interval (PIM) ... 673
hello-interval-link ... 674
hello-interval-target ... 675
hello-time ... 676
hello-timeout (LDP) ... 678
hello-timeout-link ... 680
hello-timeout-target ... 681
helper-only ... 682
hold-time ... 683
holdoff-time ... 684
hop-limit ... 685
host-table aging-mode conversational ... 687
host-table aging-time conversational ... 688

hostname disable ... 689
http server ... 690
implicit-commit ... 692
import l2vpn evpn reoriginate ... 694
import vpnv4 unicast reoriginate ... 695
import vpnv6 unicast reoriginate ... 696
import-map ... 697
inactivity-timer ... 698
include-all ... 699
include-any ... 701
ingress-tunnel-accounting ... 703
ingress-vlan-mapped-ve-counter ... 704
init-route-calc-delay ... 705
insight enable ... 707
insight mode ... 709
install-igp-cost ... 710
instance ... 711
interface ethernet ... 713
interface loopback ... 715
interface management ... 716
interface port-channel ... 717
interface (telemetry) ... 720
interface management ... 721
interface ve ... 723
interval ... 724
interval (telemetry) ... 725
ip access-group ... 727
ip access-list ... 729
ip address ... 731
ip address (site) ... 733
ip anycast-address ... 734
ip arp gratuitous none ... 735
ip arp inspection ... 736
ip arp inspection filter ... 737
ip arp inspection trust ... 738
ip arp learn-any ... 739
ip arp-aging-timeout ... 740
ip dhcp relay ... 742
ip dhcp relay address ... 743
ip dhcp relay gateway ... 744
ip dhcp snooping ... 745
ip dhcp snooping enable ... 746
ip dhcp snooping information option ... 747
ip dhcp snooping trust ... 748
ip directed-broadcast ... 749
ip dns ... 750
ip extcommunity-list ... 753
ip flowspec rules statistics ... 755
ip forward ... 757

ip global-subnet-broadcast-acl 758
ip icmp-fragment enable 759
ip icmp rate-limiting 760
ip icmp redirect 761
ip icmp unreachable 762
ip igmp immediate-leave 763
ip igmp last-member-query-interval 764
ip igmp query-interval 765
ip igmp query-max-response-time 766
ip igmp router-alert-check-disable 767
ip igmp snooping enable 768
ip igmp snooping fast-leave 769
ip igmp snooping last-member-query-interval 770
ip igmp snooping mrouter interface 771
ip igmp snooping querier enable 772
ip igmp snooping query-interval 773
ip igmp snooping query-max-response-time 774
ip igmp snooping static-group 775
ip igmp snooping version 776
ip igmp ssm-map 777
ip igmp static-group 779
ip igmp version 780
ip interface loopback (overlay gateway) 781
ip irdp 782
ip large-community-list extended 783
ip large-community-list standard 785
ip mtu 787
ip option 789
ip ospf active 791
ip ospf area 792
ip ospf auth-change-wait-time 794
ip ospf authentication-key 796
ip ospf bfd 797
ip ospf cost 798
ip ospf database-filter 799
ip ospf dead-interval 801
ip ospf hello-interval 803
ip ospf ldp-sync 804
ip ospf md5-authentication 805
ip ospf mtu-ignore 807
ip ospf network 808
ip ospf passive 810
ip ospf priority 811
ip ospf retransmit-interval 812
ip ospf transmit-delay 813
ip pim dr-priority 814
ip pim snooping enable 815
ip pim-sparse 816
ip pim ttl-threshold 817

ip port (telemetry) 818
ip policy route-map 819
ip prefix-list 820
ip proxy-arp 822
ip receive access-group 823
ip route 825
ip route next-hop-recursion 828
ip route static bfd 829
ip route static bfd holdover-interval 831
ip router-id 832
ip router isis 833
ip source-guard enable 834
ip subnet-broadcast-acl 835
ip subnet-rate-limit 836
ip vrrp-extended auth-type 838
ip 840
ipv6 access-group 842
ipv6 access-list 844
ipv6 address 846
ipv6 anycast-address 848
show ipv6 dhcp relay 849
ipv6 dhcp relay distance 850
ipv6 dhcp relay address 851
ipv6 dhcp relay distance 853
ipv6 dhcp relay maximum-delegated-prefixes 854
ipv6 dns 855
ipv6 icmpv6 redirect 856
ipv6 icmpv6 rate-limiting 857
ipv6 icmpv6 unreachable 858
ipv6 mld snooping enable 859
ipv6 mld snooping fast-leave 860
ipv6 mld snooping last-member-query-interval 861
ipv6 mld snooping mrouter interface 862
ipv6 mld snooping mrouter logical-interface 864
ipv6 mld snooping querier enable 866
ipv6 mld snooping query-interval 868
ipv6 mld snooping query-max-response-time 870
ipv6 mld snooping static-group 871
ipv6 mld snooping version 873
ipv6 mld ssm-map enable 874
ipv6 nd cache expire 875
ipv6 nd cache interface-limit 876
ipv6 option disable 878
ipv6 ospf active 879
ipv6 ospf area 880
ipv6 ospf authentication ipsec 882
ipv6 ospf authentication ipsec disable 883
ipv6 ospf authentication spi 884
ipv6 ospf bfd 886

ipv6 ospf cost ... 887
ipv6 ospf dead-interval ... 888
ipv6 ospf hello-interval ... 890
ipv6 ospf hello-jitter ... 892
ipv6 ospf instance ... 893
ipv6 ospf mtu-ignore ... 894
ipv6 ospf network ... 895
ipv6 ospf passive ... 897
ipv6 ospf priority ... 898
ipv6 ospf retransmit-interval ... 899
ipv6 ospf suppress-linklsa ... 900
ipv6 ospf transmit-delay ... 901
ipv6 pim dr-priority ... 902
ipv6 pim snooping enable ... 903
ipv6 pim ttl-threshold ... 904
ipv6 pim-sparse ... 905
ipv6 policy route-map ... 906
ipv6 prefix-list ... 907
ipv6 protocol vrrp ... 909
ipv6 protocol vrrp-extended ... 910
ipv6 receive access-group ... 911
ipv6 route ... 913
ipv6 route next-hop-recursion ... 916
ipv6 route null ... 917
ipv6 route next-hop-vrf ... 919
ipv6 route static bfd ... 921
ipv6 route static bfd holdover-interval ... 923
ipv6 router isis ... 924
ipv6 router ospf ... 925
ipv6 router pim ... 926
ipv6 prefix-list ... 927
ipv6 subnet-zero drop ... 929
ipv6 vrrp-extended auth-type ... 930
ipv6 vrrp-extended-group ... 931
ipv6 vrrp-group ... 932
ipv6 vrrp-suppress-interface-ra ... 933
is-type ... 934
isis auth-check ... 936
isis auth-key ... 937
isis auth-mode ... 939
isis bfd ... 940
isis circut-type ... 941
isis hello-interval ... 942
isis hello-multiplier ... 943
isis hello padding ... 945
isis ipv6 metric ... 946
isis ldp-sync ... 948
isis metric ... 949
isis passive ... 951

isis point-to-point 952
isis priority 953
isis reverse-metric 955
iterations 957

Commands K - M 958
ka-int-count 962
ka-interval 963
ka-timeout 965
key 967
key (keychain) 968
key-add-remove-interval 969
key-algorithm 970
key-rollover-interval 971
key-string 972
keychain 973
keypair 974
label-withdrawal-delay 975
lacp auto 977
lacp default-up 978
lacp port-priority 979
lacp system-id 980
lacp system-priority 981
lacp timeout 982
lacp-pdu-forward enable 983
lag hash 985
ldap-server host 989
ldap-server maprole 992
ldp 993
ldp-enable 994
ldp-params 995
ldp-sync 996
left-interface vlan 998
license add 1000
license eula 1002
line vty exec-timeout 1004
link-error-disable 1005
link-fault-signal 1007
link-oam allow-loopback 1009
link-oam enable 1010
link-oam remote-failure 1011
link-oam remote-loop-back 1012
listen-limit 1013
listen-range 1015
lldp profile 1017
load-balance hash 1018
load-sharing 1022
local-as 1023
local-switching 1024
log (OSPFv2) 1025

log (OSPFv3) 1027
log adjacency 1029
log invalid-lsp-packets 1030
log-dampening-debug 1031
log-shell 1032
logging auditlog class 1033
logging raslog console 1034
logging raslog console stop 1035
logging syslog-facility local 1036
logging syslog-server 1037
logging syslog-server-host 1039
logging utility 1041
logical-interface 1043
loopback phy 1046
loop-detection 1047
loop-detection shutdown-disable 1049
loop-detection vlan 1051
lsp 1052
lsp (Telemetry) 1053
lsp-gen-interval 1054
lsp-interval 1055
lsp-refresh-interval 1056
lsr-id 1057
lvtep broadcast-local-bias 1058
ma-name 1060
mac access-group 1062
mac access-list extended 1064
mac access-list standard 1065
mac-address withdrawal 1066
mac-address-table aging-time 1068
mac-address-table mac-move 1069
mac-address-table static 1071
maid-format 1073
maintenance-mode (Interface) 1074
management-heartbeat manager (management-heartbeat) 1075
management-security 1077
manual-switch vlan 1078
map bridge-domain (overlay gateway) 1079
map cos to cos 1080
Supported In 1080
Related Commands 1081
map dscp 1082
map vlan 1084
map vni auto (VXLAN gateway) 1086
master-vlan (STP) 1087
match (route maps) 1088
match access-group 1092
match additional-paths advertise-set 1093
match as-path 1095

match bridge-domain ... 1096
match community ... 1097
match destination-port ... 1098
match dscp ... 1100
match extcommunity ... 1102
match fragment-type ... 1103
match ip ... 1105
match ip address acl ... 1106
match ip icmp-code ... 1107
match ip icmp-type ... 1109
match ipv6 address ... 1111
match ipv6 address acl ... 1112
match large-community ... 1113
match packet-length ... 1114
match port ... 1116
match protocol ... 1118
match rpki ... 1121
match source-port ... 1123
match tcp-flags ... 1125
match vlan ... 1128
max-age ... 1129
max-bypasses ... 1131
max-bypasses-per-mp ... 1133
max-lsp-lifetime ... 1135
max-mcache ... 1136
max-metric router-lsa ... 1137
max-metric router-lsa (OSPFv3) ... 1139
max-neighbor-reconnect-time ... 1141
max-neighbor-recovery-time ... 1142
maxas-limit ... 1143
maximum-paths (BGP) ... 1144
maximum-paths (IS-IS) ... 1146
maximum-paths (OSPF) ... 1147
maximum-paths ebgp ibgp ... 1148
measured-boot ... 1150
Platform Availability ... 1150
measurement-interval ... 1151
med-missing-as-worst ... 1152
member (cluster) ... 1153
member-bridge-domain ... 1155
member-vlan (STP) ... 1156
mep ... 1157
message-interval ... 1159
message-interval ... 1160
metric ... 1161
metric-style wide ... 1162
metric-type ... 1163
minimum-links ... 1164
mip-policy ... 1166

mode (LLDP) 1167
mode gre ip 1168
monitor session 1169
mpls reoptimize 1171
mpls-interface 1172
mtu (interface) 1173
mtu (PW) 1175
mtu-enforce 1176
multipath 1177
multiplier (LLDP) 1179
multiplier (UDLD) 1180
multi-topology 1181
mvrp applicant-mode 1182
mvrp enable 1184
mvrp registration-mode forbidden vlan 1186
mvrp timer 1188

Commands N - Q 1190

name (ERP) 1195
name-prefix 1196
nbr-timeout 1198
neighbor activate 1199
neighbor accept-lldp-neighbors 1201
neighbor additional-paths 1202
neighbor additional-paths advertise 1204
neighbor additional-paths disable 1206
neighbor advertisement-interval 1208
neighbor allowas-in 1210
neighbor alternate-as 1212
neighbor announce-rpki-state 1214
neighbor as-override 1216
neighbor bfd 1218
neighbor capability as4 1220
neighbor capability orf prefixlist 1222
neighbor default-originate 1224
neighbor description 1226
neighbor ebgp-btsh 1228
neighbor ebgp-multihop 1230
neighbor enable-peer-as-check 1231
neighbor encapsulation 1233
neighbor enforce-first-as 1234
neighbor filter-list 1236
neighbor flowspec redirect 1238
neighbor flowspec validation 1240
neighbor graceful-restart 1242
neighbor graceful-shutdown 1244
neighbor local-as 1247
neighbor maxas-limit in 1249
neighbor maximum-prefix 1251
neighbor next-hop-self 1254

neighbor next-hop-unchanged 1256
neighbor password 1258
neighbor peer-dampening 1260
neighbor peer-dampening (peer-group) 1262
neighbor peer-group 1264
neighbor peer-group-name alternate-as-range 1266
neighbor prefix-list 1267
neighbor remote-as 1269
neighbor remove-private-as 1271
neighbor route-map 1273
neighbor route-reflector-client 1275
neighbor rpki validation status disable 1277
neighbor send-community 1278
neighbor shutdown 1280
neighbor soft-reconfiguration inbound 1282
neighbor static-network-edge 1284
neighbor timers 1285
neighbor unsuppress-map 1287
neighbor update-source 1289
neighbor weight 1291
net 1293
network 1294
next-hop-enable-default 1296
next-hop-mpls 1297
next-hop-recursion 1299
next-hop-recursion (Policy Based Routing) 1300
no debug 1302
no-core-isolation 1304
node 1305
non-revertive-mode 1306
nonstop-routing (IS-IS) 1307
nonstop-routing (OSPF) 1308
notification-timer 1309
ntp authenticate 1310
ntp authentication-key 1311
ntp disable 1313
ntp peer 1314
ntp server 1316
ntp trusted-key 1318
operational-state 1319
optimized replication 1320
oscmd 1321
overlay access-group 1323
overlay access-list type vxlan extended 1324
overlay access-list type vxlan standard 1325
overlay-gateway 1326
overlay-service-policy 1328
overlay-transit 1330
partial-spf-interval 1331

password ... 1333
password-attributes ... 1335
password-attributes expiry-alert-level ... 1339
password-encryption convert-enc-to-level-10 ... 1342
password-policy (TPVM mode) ... 1343
path ... 1345
pdu-rate ... 1347
peer ... 1348
peer (MCT) ... 1351
peer-dampening ... 1352
peer-group ipv6prefix-over-ipv4peer ... 1354
peer-interface ... 1355
peer-keepalive (optional) ... 1356
penalty ... 1358
permit ip host ... 1359
ping ... 1361
pki ocsp ... 1364
police cir ... 1366
policy-map ... 1368
port-channel path-cost ... 1370
preempt-mode ... 1372
prefix-independent-convergence ... 1373
prefix-independent-convergence-static ... 1374
primary-path ... 1375
priority ... 1377
priority-group-table ... 1378
priority-table ... 1380
process-restart ... 1382
profile (LLDP) ... 1385
profile (telemetry) ... 1387
profile counters ... 1389
profile etcam ... 1391
profile lag ... 1393
profile qos ... 1395
profile route ... 1397
profile tcam ... 1400
profile tcam cam-share ... 1402
protocol ... 1404
protocol cfm ... 1405
protocol link-oam ... 1406
protocol lldp ... 1407
protocol loop-detection ... 1408
protocol mvrp ... 1409
protocol spanning-tree ... 1410
protocol udld ... 1412
protocol vrrp ... 1413
protocol vrrp-extended ... 1414
prune-wait ... 1415
pw-profile ... 1416

pw-profile (bridge domain) 1418
python 1419
qos cos 1422
qos cos-mutation 1423
qos cos-mutation 1424
Supported In 1424
Related Commands 1425
qos cos-traffic-class 1426
qos cpu slot 1427
qos dscp-cos 1429
qos dscp-mutation 1430
qos dscp-traffic-class 1431
qos-dscp-mode 1432
qos flowcontrol 1433
qos map cos-mutation 1435
qos map cos-mutation 1437
Supported In 1437
Related Commands 1437
qos map cos-traffic-class 1438
qos map dscp-cos 1440
qos map dscp-mutation 1442
qos map dscp-traffic-class 1444
qos map traffic-class-cos 1446
Supported In 1446
qos port-speed-up 1448
qos random-detect traffic-class 1449
qos red-profile 1450
qos remark dscp 1452
qos rx-queue cos-threshold 1453
qos rx-queue multicast 1454
qos rx-queue unicast traffic-class 1456
qos service-policy 1457
qos traffic-class 1458
qos traffic-class-cos 1459
Supported In 1459
qos trust dscp 1461
qos-mpls map dscp-exp 1462
qos-mpls map exp-dscp 1464
qos-mpls map exp-traffic-class 1465
qos-mpls map-apply dscp-exp 1467
qos-mpls map-apply exp-dscp 1468
qos-mpls map-apply exp-traffic-class 1469
qos-ttl-mode 1470
qos tx-queue scheduler strict-priority 1472

Commands R - Sh 1474

radius-server host 1477
raps-default-mac 1480
raps-mel 1481
raslog-duration 1482

rate-monitoring 1483
rd (EVPN VLAN/BD) 1485
rd auto (EVPN) 1486
reconnect-time 1487
record 1488
record-route 1489
recovery-time 1490
redistribute 1491
redundant-management enable 1495
refresh-reduction 1496
region 1498
registrar-server 1499
Platform Availability 1499
registrar-port 1500
Platform Availability 1500
reliable-messaging 1501
reload 1503
reload-delay 1504
reload-delay enable 1505
remark 1506
remote-mep 1507
Parameters: 1507
rename 1508
reoptimize-timer 1509
resequence access-list 1511
reservable-bandwidth 1513
resilient-hash 1515
retain route-target all 1517
retransmit-interval 1518
retries 1519
retry-limit 1520
retry-time 1521
reverse-metric 1522
revert-timer 1524
revertive global 1526
revertive hold-time 1528
revision 1529
rfc1583-compatibility (OSPF) 1530
rib-route-limit 1531
right-interface vlan 1533
rpl 1535
rpl-owner 1537
rpki priority 1538
server ssh 1539
server tcp 1541
rmon alarm 1543
rmon collection history 1545
rmon collection stats 1547
rmon event 1548

role name 1549
rollback apply checkpoint 1551
rollback checkpoint 1553
rollback enable 1555
root access console 1556
root enable 1557
route-map (BGP) 1558
route-precedence 1560
route-target 1562
route-target (EVPN) 1563
route-target (EVPN VLAN/BD) 1565
router bgp 1567
router isis 1568
router mpls 1569
router ospf 1570
router pim 1571
router-interface 1572
rp-address 1574
rp-candidate 1576
rpf ecmp rebalance 1578
rpf-mode 1579
rsvp 1581
rsvp-flooding-threshold 1582
rsvp-periodic-flooding-time 1584
rule 1585
rule-name 1587
rx-label-silence-time 1588
secure-port 1589
sample-recording 1590
scheduler 1592
seq (rules in IPv4 extended ACLs) 1594
seq (rules in IPv4 extended bACLs) 1599
seq (rules in IPv4 standard ACLs) 1603
seq (rules in IPv6 extended ACLs) 1606
seq (rules in IPv6 standard ACLs) 1611
seq (rules in IPv4 standard bACLs) 1614
seq (rules in MAC extended ACLs) 1617
seq (rules in MAC standard ACLs) 1623
service password-encryption 1625
service-policy (control plane) 1626
service-policy (interface) 1627
session 1629
set extcommunity 1631
set interface 1633
set ip dscp 1634
set ip interface null0 1635
set ip mirror 1636
set ip next-hop 1637
set ipv6 interface null0 1639

set ipv6 next-hop 1640
set large-community 1642
set large-community-list delete 1644
set police cir 1645
set sflow 1646
set traffic-action continue 1647
set-debug 1648
set-overload-bit 1649
sflow agent-address 1651
sflow collector 1653
sflow enable 1655
sflow polling-interval (global version) 1656
sflow sample-rate 1657
sflow update-destination-mac 1659
sflow update-dst-mac(global version) 1661
sflow source-interface 1662

Show A through Show I 1664

show access-list 1671
show access-list overlay transit 1675
show access-list overlay type vxlan acl-name 1676
show access-list-log buffer 1677
show access-list-log buffer config 1679
show arp 1680
show arp access-list 1683
show bfd 1684
show bfd neighbors 1686
show bfd neighbors application 1688
show bfd neighbors dest-ip 1690
show bfd neighbors details 1692
show bfd neighbors interface 1695
show bgp evpn ethernet-segment 1697
show bgp evpn evid 1698
show bgp evpn vni 1699
show bgp evpn interface tunnel 1700
show bgp evpn l2route 1702
show bgp evpn l2route next-hop 1705
show bgp evpn l2route unreachable 1706
show bgp evpn l3vni 1707
show bgp evpn neighbors 1710
show bgp evpn neighbors advertised-routes 1712
show bgp evpn neighbors routes 1714
show bgp evpn routes 1716
show bgp evpn routes best 1717
show bgp evpn routes detail 1719
show bgp evpn routes local 1720
show bgp evpn routes next-hop 1723
show bgp evpn routes no-best 1725
show bgp evpn routes not-installed-best 1727
show bgp evpn routes rd 1729

show bgp evpn routes rd type ... 1730
show bgp evpn routes type ... 1733
show bgp evpn routes type igmp-join-sync ... 1741
show bgp evpn routes type igmp-leave-sync ... 1742
show bgp evpn routes unreachable ... 1743
show bgp evpn summary ... 1744
show bgp ip flowspec ... 1745
show bgp ip flowspec neighbors ... 1747
show bgp ip neighbor ipv6 ... 1749
show bgp ip summary ipv6 ... 1752
show ip/ipv6 bgp peer-dampened ... 1753
show bmc config-history ... 1755
show bmc interface management status ... 1757
show bmc interface management ip ... 1758
show bmc password-status ... 1759
show bmc status ... 1760
show bridge-domain ... 1762
show capabilities ... 1768
show cee maps default ... 1769
show cert-util sshkey ... 1770
show cfm ... 1771
Parameters ... 1771
show cfm y1731 action-profile ... 1773
show cfm y1731 client-signal-fail ... 1774
show cfm y1731 delay-measurement ... 1775
Parameters ... 1775
show cfm y1731 synthetic-loss-measurement ... 1777
Parameters ... 1777
show cfm y1731 test-profile ... 1779
show chassis ... 1780
show cipherset ... 1782
show cli ... 1783
show clock ... 1784
show cluster ... 1785
show cluster track ... 1790
show config-drift-track ... 1791
show copy-support status ... 1792
show core-isolation track ... 1793
show crypto ca ... 1794
show crypto key ... 1795
show debug all ... 1796
show debug arp packet ... 1797
show debug dhcp packet ... 1799
show debug dhcp packet buffer ... 1800
show debug ip bgp all ... 1802
show debug ip igmp ... 1803
show debug ip ospf internal lsp-shortcuts ... 1804
show debug ip ospf all ... 1805
show debug ipv6 pim ... 1806

show debug lacp 1807
show debug lldp 1808
show debug spanning-tree 1809
show debug vrrp 1810
show defaults threshold 1811
show dot1x 1814
show environment fan 1817
show environment history 1818
show environment power 1820
show environment sensor 1824
show environment temp 1825
Parameters 1825
show erp 1828
show erp statistics 1829
show event-handler activations 1830
show file 1831
show firmware peripheral cpld 1833
show firmware peripheral fpga 1835
show firmwaredownloadhistory 1836
show firmwaredownloadstatus 1837
show grubversion 1839
show hardware media-database 1840
show hardware profile 1842
show hardware smt 1850
show history 1851
show http server status 1852
show hw route-info 1853
show interface 1855
show interface stats brief 1860
show interface stats detail 1862
show interface stats utilization-watermark 1865
show interface status 1868
show inventory 1869
show ip arp inspection 1870
show ip arp inspection interfaces 1872
show ip arp suppression-cache 1874
show ip arp suppression-statistics 1875
show ip arp suppression-status 1877
show ip bgp 1879
show ip bgp attribute-entries 1880
show ip bgp dampened-paths 1881
show ip bgp filtered-routes 1882
show ip bgp flap-statistics 1883
show ip bgp neighbors 1885
show ip bgp neighbors advertised-routes 1888
show ip bgp neighbors flap-statistics 1889
show ip bgp neighbors last-packet-with-error 1890
show ip bgp neighbors received 1892
show ip bgp neighbors received-routes 1893

show ip bgp neighbors rib-out-routes 1894
show ip bgp neighbors routes 1895
show ip bgp neighbors routes-summary 1897
show ip bgp peer-group 1898
show ip bgp routes 1899
show ip bgp routes community 1902
show ip bgp routes large-community 1903
show ip bgp routes large-community access-list 1905
show ip bgp routes large-community reg-expression 1906
show ip bgp rpki details 1907
show ip bgp rpki server summary 1908
show ip bgp rpki table 1909
show ip bgp summary 1910
show ip bgp vpnv4 routes large-community 1912
show ip bgp vpnv4 routes large-community access-list 1913
show ip bgp vpnv4 routes large-community reg-expression 1914
show ip bgp vpnv6 routes large-community 1915
show ip bgp vpnv6 routes large-community access-list 1916
show ip bgp vpn6 routes large-community reg-expression 1917
show ip dhcp relay address 1918
show ip dhcp relay gateway 1920
show ip dhcp relay statistics 1921
show ip dhcp snooping 1922
show ip flowspec rules 1924
show ip igmp groups 1928
show ip igmp interface 1929
show ip igmp snooping 1930
show ip igmp ssm-map 1932
show ip igmp statistics bridge-domain 1933
show ip igmp statistics interface 1934
show ip igmp statistics vlan 1935
show ip interface 1936
show ip multicast snooping 1939
show ip ospf 1940
show ip ospf area 1941
show ip ospf border-routers 1943
show ip ospf config 1944
show ip ospf database 1945
show ip ospf filtered-lsa area 1948
show ip ospf interface 1949
show ip ospf lsp-shortcuts 1951
show ip ospf neighbor 1952
show ip ospf redistribute route 1953
show ip ospf routes 1954
show ip ospf summary 1956
show ip ospf traffic 1958
show ip ospf virtual link 1959
show ip ospf virtual neighbor 1960
show ip pim bsr 1961

show ip pim interface ... 1964
show ip pim mcache ... 1965
show ip pim mdt ... 1966
show ip pim neighbor ... 1969
show ip pim rp-candidate ... 1971
show ip pim rp-hash ... 1973
show ip pim rp-map ... 1974
show ip pim rp-set ... 1975
show ip pim rpf ... 1977
show ip pim traffic ... 1978
show ip route ... 1981
show ip source guard binding entries ... 1985
show ip subnet-rate-limit stats ... 1986
show ipv6 bgp ... 1987
show ipv6 bgp attribute-entries ... 1988
show ipv6 bgp dampened-paths ... 1989
show ipv6 bgp filtered-routes ... 1990
show ipv6 bgp flap-statistics ... 1991
show ipv6 bgp neighbors ... 1993
show ipv6 bgp neighbors advertised-routes ... 1995
show ipv6 bgp neighbors flap-statistics ... 1997
show ipv6 bgp neighbors last-packet-with-error ... 1998
show ipv6 bgp neighbors received ... 2000
show ipv6 bgp neighbors received-routes ... 2001
show ipv6 bgp neighbors rib-out-routes ... 2002
show ipv6 bgp neighbors routes ... 2004
show ipv6 bgp neighbors routes-summary ... 2006
show ipv6 bgp peer-group ... 2010
show ipv6 bgp routes ... 2011
show ipv6 bgp routes community ... 2014
show ipv6 bgp routes large-community ... 2015
show ipv6 bgp routes large-community access-list ... 2016
show ipv6 bgp routes large-community reg-expression ... 2017
show ipv6 bgp summary ... 2018
show ipv6 counters interface ... 2020
show ipv6 dhcp relay address interface ... 2021
show ipv6 dhcp relay delegated-prefixes ... 2022
show ipv6 dhcp relay prefix-delegation-information ... 2024
show ipv6 dhcp relay statistics ... 2025
show ipv6 interface ... 2027
show ipv6 mld groups ... 2029
show ipv6 mld snooping ... 2031
show ipv6 mld snooping mrouter ... 2032
show ipv6 mld statistics ... 2033
show ipv6 multicast snooping ... 2035
show ipv6 multicast snooping mcache ... 2036
show ipv6 nd ... 2037
show ipv6 nd suppression-cache ... 2039
show ipv6 nd suppression-statistics ... 2041

show ipv6 nd suppression-status....2042
show ipv6 neighbor....2044
show ipv6 ospf....2047
show ipv6 ospf area....2048
show ipv6 ospf database....2049
show ipv6 ospf interface....2052
show ipv6 ospf memory....2053
show ipv6 ospf neighbor....2055
show ipv6 ospf redistribute route....2057
show ipv6 ospf routes....2058
show ipv6 ospf spf....2059
show ipv6 ospf summary....2060
show ipv6 ospf virtual-links....2062
show ipv6 ospf virtual-neighbor....2063
show ipv6 pim anycast-rp....2064
show ipv6 pim bsr....2065
show ipv6 pim group....2066
show ipv6 pim interface....2067
show ipv6 pim mcache....2069
show ipv6 pim neighbor....2070
show ipv6 pim rp-candidate....2072
show ipv6 pim rp-hash....2073
show ipv6 pim rp-map....2074
show ipv6 pim rp-set....2075
show ipv6 pim rpf....2076
show ipv6 pim settings....2077
show ipv6 pim traffic....2078
show ipv6 prefix-list....2079
show ipv6 route....2080
show ipv6 static route....2082
show ipv6 vrrp....2083
show isis....2088
show isis config....2093
show isis counts....2094
show isis database....2098
show isis hostname....2102
show isis interface....2103
show isis neighbors....2109
show isis routes....2113
show isis spf-log....2115
show isis traffic....2119
show selinux status....2120
show system internal bgp evpn nhid....2122
show mac-address-table....2123
show ip arp suppression-cache....2124

Show J through Show Z....2125
show lacp....2130
show license....2131
show link-oam info....2133

show link-oam info detail ... 2134
show link-oam statistics ... 2136
show link-oam statistics detail ... 2137
show lldp ... 2139
show lldp interface ... 2140
show lldp neighbors ... 2142
show lldp statistics ... 2145
show loop-detection ... 2146
show mac-address-table ... 2149
show management-heartbeat manager ... 2150
show media ... 2151
show media interface ... 2152
show media optical-monitoring interface ... 2155
show media tunable-optic-sfpp ... 2158
show monitor ... 2160
show mpls autobw-template ... 2162
show mpls autobw-threshold-table ... 2163
show mpls bypass-lsp ... 2164
show mpls dynamic-bypass interface ... 2167
show mpls interface ... 2168
show mpls ldp ... 2169
show mpls lsp ... 2172
show mpls policy ... 2180
show mpls rsvp ... 2181
show mpls rsvp interface ... 2183
show mpls rsvp session ... 2186
show mpls statistics ... 2194
show mpls te database ... 2197
show mvrp ... 2199
show mvrp attributes ... 2200
show mvrp interface ... 2202
show mvrp statistics ... 2204
show netconf ... 2206
show netconf capabilities ... 2207
show notification stream ... 2208
show ntp status ... 2209
show ntp status association detail ... 2210
show ntp status associations ... 2212
show overlay-gateway ... 2214
show onieversion ... 2216
show policy-map ... 2217
show port-channel ... 2221
show port-channel load-balance ... 2223
show port port-channel ethernet ... 2225
show port-security ... 2226
show process cpu ... 2229
show process info ... 2231
show process memory ... 2232
show qos cpu cfg ... 2234

show qos cpu info ... 2237
show qos flowcontrol interface ... 2238
show qos interface all ... 2240
show qos interface ... 2244
show qos interface port-channel ... 2247
show qos interface ve ... 2254
show qos maps ... 2256
show qos maps cos-mutation ... 2259
Supported In ... 2259
Related Commands ... 2260
show qos maps cos-traffic-class ... 2261
show qos maps dscp-cos ... 2262
show qos maps dscp-mutation ... 2263
show qos maps dscp-traffic-class ... 2264
show qos maps traffic-class-cos ... 2266
Supported In ... 2266
show qos maps traffic-class-dscp ... 2267
show qos-mpls maps dscp-exp ... 2268
show qos-mpls maps exp-dscp ... 2269
show qos-mpls maps exp-traffic-class ... 2270
show qos tx-queue interface ... 2271
show rmon ... 2272
show rmon history ... 2274
show remote-attestation ... 2275
Platform Availability ... 2275
show rollback checkpoint ... 2276
show rollback diff checkpoint ... 2278
show rollback feature-status ... 2279
show rollback log ... 2280
show rollback patch checkpoint ... 2281
show rollback status ... 2282
show route-map ... 2284
show run router mpls cspf-group ... 2287
show running-config ... 2288
show running-config aaa ... 2289
show running-config aaa accounting ... 2290
show running-config aaa authorization ... 2291
show running-config aaa authorization command ... 2292
show running-config access-list overlay type vxlan ... 2293
show running-config arp ... 2294
show running-config control-plan ip subnet-rate-limit ... 2296
show running-config dpod ... 2297
show running-config event-handler ... 2298
show running-config ip access-list ... 2300
show running-config ip receive ... 2301
show running-config ipv6 ... 2302
show running-config ipv6 access-list ... 2304
show running-config keychain ... 2305
show running-config lag hash ... 2306

show running-config ldap-server ... 2308
show running-config mac access-list ... 2309
show running-config password-attributes ... 2310
show running-config radius-server ... 2312
show running-config rmon ... 2313
show running-config role ... 2314
show running-config rule ... 2315
show running-config sflow ... 2317
show running-config ssh ... 2318
show running-config ssh server ... 2319
show running-config ssh server key-exchange ... 2321
show running-config system-monitor ... 2322
show running-config telemetry collector ... 2324
show running-config telemetry profile ... 2325
show running-config telemetry profile (MPLS) ... 2327
show running-config telemetry profile (queue) ... 2329
show running-config telemetry server ... 2331
show running-config username ... 2332
show sflow ... 2334
show span path session ... 2336
show spanning-tree ... 2337
show ssh client status ... 2339
show ssh server status ... 2340
show startup-config ... 2341
show statistics access-list ... 2342
show statistics access-list overlay type vxlan ... 2346
show statistics bridge-domain ... 2347
show statistics vlan ... 2349
show statistics vpn ... 2351
show storm-control ... 2352
show support ... 2354
show system maintenance ... 2355
show system maintenance rate-monitoring ... 2356
show system monitor tm ... 2357
show tech-support ... 2358
show telemetry client-cert ... 2361
show telemetry collector name ... 2362
show telemetry collector summary ... 2363
show telemetry server status ... 2364
show telnet server status ... 2365
show threshold monitor ... 2366
show threshold monitor ecmp ... 2368
show threshold monitor host ... 2369
show threshold monitor nexthop ... 2371
show threshold monitor route ... 2373
show threshold monitor sfp ... 2375
show tm voq-stat ingress-device all discards ... 2378
show tm voq-stat ingress-device all egress-port ethernet ... 2380
show tm voq-stat ingress-device all max-buffer-util ... 2382

show tm voq-stat ingress-device all max-queue-depth 2383
show tm voq-stat ingress-device ethernet 2385
show tm voq-stat slot 2388
show topology-group 2390
show tpm 2391
show tpvm 2393
show tpvm config 2396
show tpvm config password-policy 2398
show tunnel 2400
show udld 2402
show udld interface 2403
show udld statistics 2405
show users 2406
show version 2407
show vlan brief 2409
show vlan detail 2411
show vrf 2412
show vrrp 2415
show ztp status 2420

Commands Shu - Z 2422

shortcuts ospf 2427
shutdown 2428
shutdown (link-oam) 2430
shutdown (STP) 2431
shutdown-time 2432
shutdown (cluster) 2433
shutdown (interface) 2434
shutdown (LIF) 2435
shutdown-time 2436
shutdown-time 2437
site 2438
snmp trap link-status disable 2440
snmp-server community 2443
snmp-server contact 2444
snmp-server context 2445
snmp-server enable trap 2447
snmp-server engineid local 2448
snmp-server group 2450
snmp-server host 2452
snmp-server location 2455
snmp-server mib community-map 2456
snmp-server preserve-statistics disable 2458
snmp-server sys-descr 2459
snmp-server trap 2460
snmp-server use-vrf 2461
snmp-server user 2463
snmp-server v3host 2466
snmp-server view 2468
soft-preemption 2470

soft-preemption cleanup-timer 2471
source 2472
source (monitor session) 2474
source-interface (LDAP) 2479
source-interface (RADIUS) 2481
spanning-tree autoedge 2483
spanning-tree bpdu-mac 2484
spanning-tree cost 2485
spanning-tree edgeport 2486
spanning-tree guard root 2488
spanning-tree link-type 2489
spanning-tree portfast 2490
spanning-tree priority 2492
spanning-tree restricted-role 2493
spanning-tree restricted-tcn 2494
spanning-tree shutdown 2495
speed (Ethernet) 2496
spf-interval 2498
spt-threshold infinity 2500
ssh 2501
ssh client cipher 2504
ssh client cipher non-cbc 2505
ssh client key-exchange 2506
ssh client mac 2507
ssh server algorithm 2508
ssh server certificate 2509
ssh server cipher 2510
ssh server key 2511
ssh server key-exchange 2513
ssh server mac 2514
ssh server max-auth-tries 2515
ssh server max-idle-timeout 2516
ssh server max-login-timeout 2517
ssh server rekey-interval 2518
ssh server rekey-volume 2519
ssh server use-vrf shutdown 2520
ssl-profile 2521
ssm-enable 2522
start (CFM) 2524
start (Y1731) 2525
Parameters: 2525
start-shell 2526
static-network 2528
statistics 2529
statistics (bridge domain) 2530
statistics (VLAN) 2531
stop (CFM) 2532
stop (Y1731) 2534
Parameters: 2534

storm-control ingress (global) ... 2535
storm-control ingress (interface) ... 2537
subnet ... 2539
sub-ring ... 2540
summary-address (IS-IS) ... 2541
summary-address (OSPFv2) ... 2543
summary-address (OSPFv3) ... 2545
summary-prefix ... 2547
support autoupload-param ... 2549
suppress-arp ... 2550
suppress-nd ... 2551
switch-attributes ... 2552
switchport ... 2553
switchport access ... 2554
switchport mode ... 2555
switchport mode trunk-no-default-native ... 2556
switchport port-security ... 2558
switchport port-security mac-address ... 2559
switchport port-security max ... 2560
switchport port-security shutdown-time ... 2561
switchport port-security sticky ... 2562
switchport port-security violation ... 2564
switchport trunk allowed ... 2565
switchport trunk native-vlan-untagged ... 2566
switchport trunk native-vlan-xtagged ... 2567
switchport trunk tag native-vlan ... 2569
sync-interval ... 2570
sysmon fe-acces-check ... 2572
sysmon link-crc-monitoring ... 2574
sysmon sfm-walk ... 2575
system maintenance ... 2577
system maintenance turn-off ... 2579
system-description ... 2580
system-monitor tm ... 2581
system-monitor-mail ... 2582
system-monitoring power alert state removed action raslog ... 2584
system power-cycle-db-shutdown ... 2585
system-name ... 2586
table-map ... 2587
tacacs-server ... 2589
tag-type ... 2592
Parameter: ... 2592
tdpa ... 2594
telemetry client-cert ... 2596
telemetry collector ... 2597
telemetry profile ... 2598
telemetry profile (MPLS) ... 2602
telemetry server ... 2604
telnet ... 2605

telnet server ... 2607
terminal ... 2608
test-profile ... 2610
threshold ... 2611
threshold (ETH-DM) ... 2613
Parameters: ... 2613
threshold (ETH-SLM) ... 2614
Parameters: ... 2614
threshold-monitor ... 2616
threshold-monitor acl ... 2618
threshold-monitor Cpu ... 2621
threshold-monitor memory ... 2623
threshold-monitor bfd-sessions ... 2625
threshold-monitor ecmp ... 2627
threshold-monitor hardware-resources ... 2629
threshold-monitor host ... 2631
Supported In ... 2632
threshold-monitor lif ... 2633
threshold-monitor mac-table ... 2635
threshold-monitor nexthop ... 2637
threshold-monitor route ... 2639
threshold-monitor sfp ... 2641
threshold-monitor vxlan-tunnel ... 2645
threshold-timer (management-heartbeat) ... 2647
tie-breaking ... 2648
timeout (link-oam) ... 2650
timeout (RADIUS) ... 2651
timeout (Y1731) ... 2652
Parameters: ... 2652
timer ... 2653
timers (BGP) ... 2655
timers (OSPFv2) ... 2657
timers (OSPFv3) ... 2659
tls min-version ... 2661
tlv-type ... 2663
to ... 2664
topology-group ... 2665
tpvm ... 2666
tpvm config dns ... 2670
tpvm config hostname ... 2671
tpvm config ldap ... 2672
tpvm config ldap ca-cert ... 2675
tpvm config ntp ... 2677
tpvm config timezone ... 2678
tpvm config trusted-peer ... 2679
tpvm deploy ... 2682
tpvm download ... 2685
tpvm fileinfo ... 2687
tpvm (mode) ... 2688

ldap host ... 2689
ldap ca-cert ... 2692
ntp (tpvm mode) ... 2694
tpvm dns ... 2695
hostname (tpvm mode) ... 2697
timezone (tpvm mode) ... 2698
trusted-peer (tpvm mode) ... 2699
auto-boot (tpvm mode) ... 2702
disk (tpvm mode) ... 2703
password (tpvm mode) ... 2705
allow-pwless (tpvm mode) ... 2706
interface management (tpvm mode) ... 2707
interface insight (tpvm mode) ... 2709
deploy (tpvm mode) ... 2710
tpvm upgrade ... 2713
tpvm snapshot ... 2716
traceroute ... 2717
track (VRRP) ... 2719
traffic-engineering (LSP) ... 2721
traffic-engineering (MPLS) ... 2724
transit-session-accounting ... 2726
transport ... 2727
trigger ... 2728
trigger-function ... 2730
trigger-mode ... 2732
trustpoint sign ... 2734
ttl ... 2735
tunable-optics ... 2736
tunneled-arp-trap enable ... 2741
tx-frame-count ... 2742
Parameters: ... 2742
tx-interval ... 2743
Parameters: ... 2743
tx-label-silence-timer ... 2744
type ... 2745
Parameters: ... 2745

Commands U - Z ... 2746

udld enable ... 2748
underflow-limit ... 2749
underlay-mdt-default-group ... 2751
underlay-mdt-group ... 2752
undeploy-force ... 2754
unlock username ... 2755
user-id ... 2756
update onie ... 2758
update-time ... 2759
usb ... 2761
usb dir ... 2762
usb remove ... 2763

use-v2-checksum 2764
user (alias configuration) 2765
username 2766
username 2770
vc-id 2771
vc-mode 2772
version (ERP) 2774
virtual-ip 2775
virtual-mac 2777
vlan 2778
vlan (EVPN) 2779
vpn-statistics 2781
vrf 2782
vrf (epvn IRB) 2783
vrf forwarding 2785
vrf-lite-capability 2786
vrrp-acceptmode-disable 2787
vrrp-extended-group 2788
vrrp-group 2789
vtep-discovery 2791
write erase 2792
wtb-time 2793
wtr-time 2794
y1731 2795

Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches or routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
`{ x | y | z }`	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation

Release Notes

Hardware and Software Compatibility for Extreme Networks products

Extreme Optics Compatibility

Other Resources such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the Open Source Declaration page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the Extreme Networks Training page.

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

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

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load 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 related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

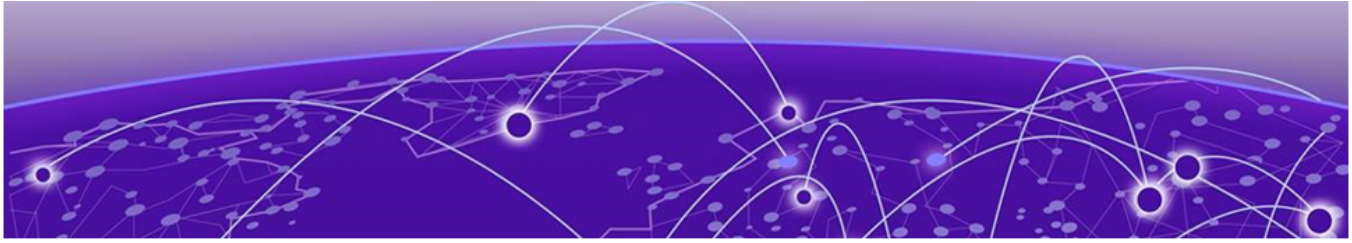
Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at https://www.extremenetworks.com/documentation-feedback/ .

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.



About This Document

What's New in This Document on page 45
Supported Hardware on page 46

What's New in This Document

This document is released with the SLX-OS 20.7.1 software release.

New commands

No new commands were added in this release.

Modified commands

The following commands were modified:

- `dscp` (QoS)
- `exp`
- `qos-mpls map-apply dscp-dscp`
- `qos-mpls map-apply exp-dscp`
- `qos-mpls map-apply exp-traffic-class`
- `qos-mpls map dscp-exp`
- `qos-mpls map exp-dscp`
- `qos-mpls map exp-traffic-class`
- `neighbor` (BGP Router Mode)

The following **show** commands were enhanced to show additional information or their examples were updated.

- `show ip bgp`
- `show ipv6 bgp`
- `show qos-mpls maps dscp-exp`
- `show qos-mpls maps exp-dscp`
- `show qos-mpls maps exp-traffic-class`

Deprecated commands

The following commands were deprecated in this release:

- `qos-mpls map traffic-class-exp`
- `qos-mpls map-apply traffic-class-exp`
- `show qos-mpls maps traffic-class-exp`

Supported Hardware

For instances in which a topic or part of a topic applies to some devices but not to others, the topic specifically identifies the devices.

SLX-OS 20.7.1 supports the following hardware platforms.

- Extreme 8820
- Extreme 8720
- Extreme 8520
- ExtremeSwitching SLX 9540
- ExtremeSwitching SLX 9250
- ExtremeSwitching SLX 9150
- ExtremeRouting SLX 9740
- ExtremeRouting SLX 9640

Note

All configurations and software features that are applicable to SLX 9150 and SLX 9250 devices are also applicable for the Extreme 8520 and Extreme 8720 devices respectively.

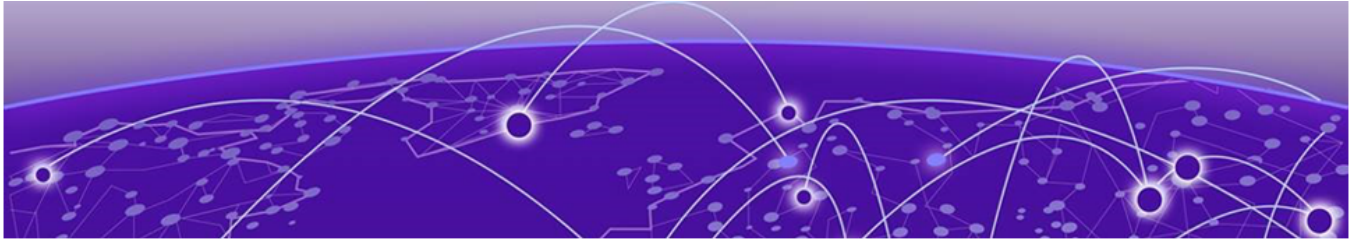
All configurations and software features that are applicable to SLX 9740 devices are also applicable for the Extreme 8820 devices.

The "Measured Boot with Remote Attestation" feature is only applicable to the Extreme 8520, Extreme 8720, and Extreme 8820 devices. It is not supported on the SLX 9150 and SLX 9250 devices.

Note

Although many software and hardware configurations are tested and supported for this release, documenting all possible configurations and scenarios is beyond this document's scope.

For information about other releases, see the documentation for those releases.



Using the SLX-OS CLI

User accounts on page 47
Accessing the CLI on page 48
Command modes on page 48
Displaying CLI commands and command syntax on page 49
Completing CLI commands on page 50
Using the comment character ! on page 51
CLI keyboard shortcuts on page 52
Using CLI command output modifiers on page 52
Unsupported input characters on page 53
Debug and system diagnostic commands on page 53
Command shortcuts (aliases) on page 53

User accounts

A user account specifies that user's level of access to the device CLI.

The SLX-OS software uses role-based access control (RBAC) as the authorization mechanism. A *role* is a container for rules, which specify which commands can be executed and with which permissions. When you create a user account you need to specify a role for that account. In general, *user* (as opposed to *user-level*) refers to any account—to which any role can be assigned—user, admin, or a non-default role.

The software ships with two default accounts—admin and user—and two corresponding default roles:

- **admin**—Accounts with admin permissions can execute all commands supported on the device. (For the initial admin login, refer to the relevant *Hardware Installation Guide*.)
- **user**—Accounts with user-level permissions can execute all **show** commands supported on the device. User-level accounts can also execute the following operational commands: **cfm**, **execute-script**, **exit**, **mtrace**, **no**, **ping**, **rasman**, **ssh**, **sysmon**, **telnet**, **timestamp**, **trace-l2**, and **traceroute**.

For more information on user accounts and roles, refer to the *Extreme SLX-OS Security Configuration Guide*.

Accessing the CLI

After an IP address is assigned to the device, you can access the CLI through a serial console connection to the Ethernet management port or a Telnet or SSH session using the device management IP address.

For more information on a serial console connection, see the relevant *SLX-OS Hardware Installation Guide*. For information on a session connection, see the *Extreme SLX-OS Management Configuration Guide*.

The procedure to access the CLI is the same through either the console interface or through a Telnet or SSH session; both access methods bring you to the login prompt. The following example shows the admin role logging into the device:

```
device login: admin
Password:**********
device#
```

Note
Multiple users can open sessions on the device and issue commands. The device supports a maximum of 32 CLI sessions.

Command modes

The SLX-OS CLI uses an industry-standard hierarchical shell familiar to networking administrators.

Privileged EXEC mode

Privileged EXEC mode supports all clear, show, and debug commands. In addition, you can enter some configuration commands that do not make changes to the system configuration. The following example shows the privileged EXEC prompt. At this prompt, you issue the **`configure terminal`** command to enter global configuration mode.

```
device# configure terminal
device(config)#
```

Global configuration mode

Global configuration mode supports commands that can change the device configuration. For any changes to be persistent, you must save the system configuration before rebooting the device. The global configuration mode provides access to sub-configuration modes for individual interfaces, VLANs, routing protocols, and other configuration areas. The following example shows how you access the interface sub-configuration mode by issuing the **`interface`** command with a specified interface.

```
device(config)# interface ethernet 0/1
device(config-if-eth-0/1)#
```

Using the do command as a shortcut

You can use the **do** command to save time when you are working in any configuration mode and you want to run a command in privileged EXEC mode.

For example, if you are configuring an Ethernet interface and you want to execute a privileged EXEC mode command, such as the **dir** command, you would first have to exit the Interface configuration mode. By using the **do** command with the **dir** command, you can ignore the need to change configuration modes, as shown in the following example.

```
device(config-if-eth-1/2)# do dir
total 32
drwxrwxr-x 3 21487 1011  4096 Mar 26 17:58 .
drwxrwxr-x 3 21487 1011  4096 Mar 13 06:45 ..
-rw-r--r-- 1 root  sys    495 Mar 16 15:41 defaultconfig.cluster
-rw-r--r-- 1 root  sys    210 Mar 16 15:41 defaultconfig.standalone
drwxrwxr-x 5 root  sys   4096 Mar 26 17:57 flex-cli
-rw-r--r-- 1 root  root 11093 Mar 26 18:04 startup-config

16908197888 bytes total (8438681600  bytes free)
```

Using the top command as a shortcut

You can use the **top** command to save time when you want to add or remove a top-level configuration while staying at the same command level.

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# top ip access-list extended acl_01
2018/06/03-07:44:41, [SSMD-1400], 30282, DCE, INFO, SLX, IPv4 access list acl_01 is
created.
```

Displaying CLI commands and command syntax

You can display commands and syntax information in any mode and from any point in the command hierarchy.

Enter a question mark (?) in any command mode to display the list of commands available in that mode.

```
device# ?
Possible completions:
  alias              Creat/Update Alias
  beacon             Enable/Disable beacon
  cd                 Change working directory
  certutil           Security Certificate Management Operations
  cfm
  cipherset          Configure FIPS-compliant secure ciphers for RADIUS/LDAP
  clear              Clear parameter
  clock              set switch date, time, and timezone
  cluster            Cluster
  configure          Manipulate software configuration information
  copy               RAS copy operation
  crypto             Crypto Certificate Management Operations
  debug              Debugging Options
  delete             delete a file
  devtools           Enable/disable development tools
  df                 show filesystem disk space usage
```

```
  dhcp               Commands to manage DHCP auto-deployment
  (output truncated)
```

To display a list of commands that start with the same characters, type the characters followed by a question mark (**?**).

```
device# e?
Possible completions:
  event-handler    Event Handler Commands
  execute-script   Run user-level BASH scripts
  exit             Exit the management session
```

To display the keywords and arguments associated with a command, enter the keyword followed by a space a then a question mark (?).

```
device# terminal ?
Possible completions:
 length    Sets Terminal Length for this session
 monitor   Enables terminal monitoring for this session
 no        Sets Terminal Length for this session to default :24.
 timeout   Sets the interval that the EXEC command interpreter wait for user input.
```

If the question mark (?) is typed within an incomplete keyword, but the keyword matches several keywords, the CLI displays help for all the matching keywords.

```
device# show d?
Possible completions:
  debug      Display the udld debug configuration
  defaults   Display default configuration
  dot1x      Show dot1x
```

The CLI accepts abbreviations for commands. This example is the abbreviation for the **`show qos interface all`** command.

```
device# sh q i a
```

If the device does not recognize a command after you press **Enter**, an error message displays.

```
device# hookup
                ^
syntax error: unknown argument.
```

If you enter an incomplete command, an error message displays.

```
device# show
                   ^
syntax error: unknown argument.
```

Completing CLI commands

To complete the spelling of commands or keywords automatically, begin typing the command or keyword and then press **Tab**. For example, at the CLI command prompt, type `te` and press **Tab**:

```
device# te
```

The CLI displays the following command.

```
device# terminal
```

If there is more than one command or keyword associated with the characters typed, the CLI displays all choices. For example, at the CLI command prompt, type `show l` and press **Tab**.

```
device# show l
```

The CLI displays the following command.

```
Possible completions:
  lacp              LACP commands
  latch-detection   Show Latch-Detection
  license           Display license keys installed on the switch.
  link-oam          Show link-OAM information
  lldp              Link Layer Discovery Protocol(LLDP).
  logging           Show logging
  loop-detection    System-wide Loop-Detection status information
```

Using the comment character !

Use the *!* (exclamation mark) to indicate that the content that follows it are not a part of the command and will be ignored. Use *!* (Exclamation Mark) to add comments to your command.

The following is an example of comments added to a command:

```
do dir ! execute the directory command.
```

The first example shows the use of the *!* symbol to introduce a blank line for better visibility and grouping of commands within the output of a command. The second example shows how the mark is used to indicate empty lines within the output of the **`show running-config`** command.

```
configure terminal
!
crypto ca trustpoint t1 ! configure a trustpoint
keypair k1 ! configure the keypair
!
do show running-config crypto ! view the configuration


SLX(config-management-heartbeat-manage) # no action
SLX(config-management-heartbeat-manage)# do show running-config management-heartbeat
manager
management-heartbeat manager
 enable
 threshold-timer 1
 action no-action
!
SLX(config-management-heartbeat-manage)#
```

CLI keyboard shortcuts

The following table lists CLI keyboard shortcuts.

Table 4: SLX-OS CLI keyboard shortcuts

Keystroke	Description
Ctrl+A	Moves the cursor to the beginning of the command line.
Ctrl+B (or the left arrow key)	Moves the cursor back one character.
Ctrl+C	Escapes and terminates command prompts and ongoing tasks (such as lengthy displays), and displays a fresh command prompt.
Ctrl+E	Moves the cursor to the end of the command line.
Ctrl+F (or the right arrow key)	Moves the cursor forward one character.
Ctrl+N (or the down arrow key)	Displays commands in the history buffer with the most recent command displayed last.
Ctrl+P (or the up arrow key)	Displays commands in the history buffer with the most recent command displayed first.
Ctrl+U or **Ctrl+X**	Deletes all characters from the cursor to the beginning of the command line.
Ctrl+W	Deletes the last word you typed.
Ctrl+Z	Returns to privileged EXEC mode. Using Ctrl+Z in privileged EXEC mode executes partial commands.
Esc B	Moves the cursor back one word.
Esc F	Moves the cursor forward one word.

Note

In privileged EXEC mode, use the **`show history`** command to list the commands most recently entered. The device retains the history of the last 1000 commands entered for the current session.

Using CLI command output modifiers

You can filter the output of the CLI **`show`** commands by using the output modifiers described below.

Table 5: CLI command output modifiers

Output modifier	Description
append	Appends the output to a file.
redirect	Redirects the command output to the specified file.
include	Displays the command output that includes the specified expression.

Table 5: CLI command output modifiers (continued)

Output modifier	Description
exclude	Displays the command output that excludes the specified expression.
begin	Displays the command output that begins with the specified expression.
last	Displays only the last few lines of the command output.
tee	Redirects the command output to the specified file. Notice that this modifier also displays the command output.
until *string*	Ends the output when the output text matches the string.
count	Counts the number of lines in the output.
linnum	Enumerates the lines in the output.
more	Paginates the output.
nomore	Suppresses the pagination of the output.
FLASH	Redirects the output to flash memory.

Unsupported input characters

We specify if some input characters are not supported for a user-defined object.

However, characters dependent on combinations of the **AltGr** key and another key are never supported.

Note
The **AltGr** key is the **Alt** key to the right of the spacebar.

Debug and system diagnostic commands

Debug and system diagnostic commands, such as "debug" and "show system internal" commands, are developed and intended for specialized troubleshooting.

Extreme Networks recommends that you work closely with Extreme technical support in executing such commands and interpreting their results.

Note
Not all diagnostic commands are documented.

Command shortcuts (aliases)

Aliases are command shortcuts that you can define globally or for individual user accounts.

Configuring global aliases

Global aliases (command shortcuts) are accessible to any logged-in user.

1. In privileged EXEC mode, enter the **configure terminal** command.

```
device# configure terminal
```

2. Enter the **alias-config** command to access alias configuration mode.

```
device(config)# alias-config
```

3. Enter the **alias** command, specifying the alias and its corresponding command.

```
device(config-alias-config)# alias ck "show clock"
```

4. Verify the alias.

```
device(config-alias-config)# exit
device(config)#  exit
device# ck
device#  show clock
2016-06-14 13:03:55 Etc/GMT
```

Configuring user-level aliases

User-level command aliases (command shortcuts) are defined for an individual user account.

1. In privileged EXEC mode, enter the **configure terminal** command.

```
device# configure terminal
```

2. Enter the **alias-config** command to access alias configuration mode.

```
device(config)# alias-config
```

3. Enter the **user** command to access user-alias configuration mode.

```
device(config-alias-config)# user jdoe
```

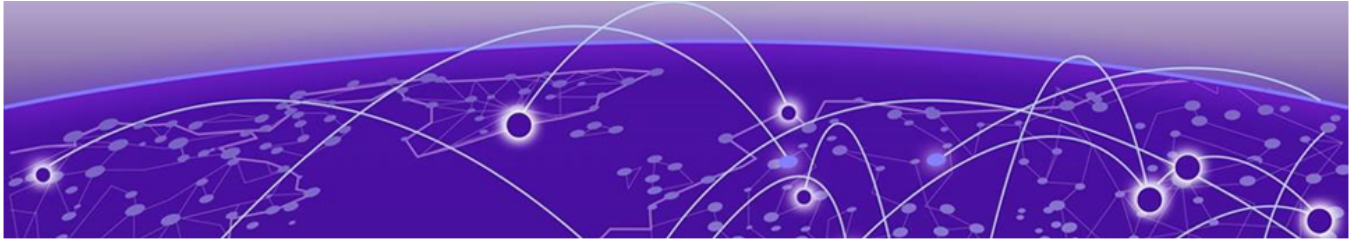
4. Enter the **alias** command, specifying the alias and its corresponding command.

```
device(config-user-jdoe)# alias int2 "interface ethernet 1/2"
```

5. Verify the alias.

Note
The following verification example assumes that the user jdoe defined the user-level alias "int2". If an admin defined the alias for this user, the example would show the admin logging out of the CLI and jdoe logging into the CLI.

```
device(config-alias-config)# exit
device(config-user-jdoe)# exit
device(config-alias-config)# exit
device(config)# int2

<Displayed automatically:>
device(config)#interface ethernet 1/2
device(config-if-eth-1/2)#
```



Commands A - B

aaa accounting on page 58
aaa authentication on page 61
aaa authorization command on page 65
accept-lifetime on page 67
accept-tolerance on page 69
action (management-heartbeat) on page 70
acl-log-raslog on page 72
acl-mirror on page 74
acl-policy on page 76
action event-stream on page 77
action python-script on page 78
action-profile on page 80
action-timeout on page 81
activate (telemetry collector) on page 82
activate (telemetry server) on page 83
activate (VXLAN overlay gateway) on page 84
adaptive on page 85
add (telemetry) on page 87
additional-paths on page 89
additional-paths select on page 91
address-family ipv4 flowspec on page 93
address-family l2vpn evpn (BGP) on page 95
address-family unicast (BGP) on page 96
address-family unicast (IS-IS) on page 98
adjustment-interval on page 99
adjustment-threshold on page 100
admin-group on page 101
advertise capabilities ac-influenced-df-election on page 103
advertise dot1-tlv on page 105
advertise dot3-tlv on page 106
advertise optional-tlv on page 107
advertise-backup on page 109
advertise-best-external on page 110
advertisement-interval (VRRP) on page 111

advertisement-interval-scale on page 112
agent-enable on page 114
agent-port on page 115
agent-uuid on page 116
aggregate-address (BGP) on page 117
alias on page 119
alias-config on page 121
allow-conflicting-rules on page 122
allow-duplicate-rules on page 124
allow multiple-ep-per-port on page 126
always-compare-med on page 127
always-propagate on page 128
anycast-rp on page 130
area authentication (OSPFv3) on page 132
area nssa (OSPFv2) on page 134
area nssa (OSPFv3) on page 136
area prefix-list (OSPFv2) on page 138
area range (OSPFv2) on page 140
area range (OSPFv3) on page 142
area stub (OSPFv2) on page 144
area stub (OSPFv3) on page 146
area virtual-link (OSPFv2) on page 148
area virtual-link (OSPFv3) on page 150
area virtual-link authentication (OSPFv3) on page 152
arp on page 154
arp access-list on page 156
as-path-ignore on page 158
auth-check on page 159
auth-key on page 161
auth-mode on page 163
auth-port on page 165
auto-cost reference-bandwidth (OSPFv2) on page 166
auto-cost reference-bandwidth (OSPFv3) on page 168
auto-shutdown-new-neighbors on page 170
autobw-threshold table on page 171
backup-advertisement-interval on page 172
bandwidth-ceiling on page 173
banner on page 175
beacon enable on page 176
bestpath prefix-validation disable on page 178
bestpath prefix-validation disallow-invalid on page 179
bfd on page 180

bfd holdover-interval on page 182
bfd interval on page 184
bfd max-session-support on page 186
bfd shutdown on page 187
bgp-redistribute-internal on page 188
bmc on page 189
bmc factory reset on page 190
bpdu-drop-enable on page 191
breakout mode on page 192
bridge-domain on page 195
bridge-domain (EVPN) on page 197
bridge-priority on page 199
bsr-candidate on page 200
bypass-lsp on page 202
bypass-lsp (Telemetry) on page 203

aaa accounting

Enables accounting for command or login information; information is forwarded to the accounting server.

Syntax

aaa accounting { **commands** | **exec** } **default start-stop** [**none** | **radius** | **tacacs+**]

no aaa accounting { **commands** | **exec** } **default start-stop** [**none** | **radius** | **tacacs+**]

Command Default

Accounting is disabled.

Parameters

commands

Causes command accounting.

exec

Causes login accounting.

default

Causes the sending of logged information to the default server.

start-stop

Causes the sending of a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server.

none

Disables accounting services.

radius

Specifies using the RADIUS server for accounting.

tacacs+

Specifies using the TACACS+ server for accounting.

Modes

Global configuration mode

Usage Guidelines

Before enabling login (EXEC) or command accounting for RADIUS, at least one RADIUS server must be configured on the device.

In RADIUS command accounting:

- All command accounting packets are sent to the initial RADIUS server configured (rather than any RADIUS server used for authentication). When the initial server fails, packets are sent to the next configured server in round-robin fashion.
- Commands with a partial timestamp are not accounted.

The following configuration commands are not accounted:

- **abort**
- **end**
- **exit**
- **help**
- **no vlan**
- **service**
- **top**

The following operational commands are not accounted:

- **cipherset**
- **copy**
- **delete**
- **dir**
- **dot1x**
- **exit**
- **help**
- **history**
- **logout**
- **oscmd**
- **ping**
- **rename**
- **reload**
- **resequence**
- **send**
- **show cipherset**
- **show cli**
- **show file**
- **show history**
- **show netconf-state**
- **show parser dump**
- **show startup-config**
- **ssh**

- **telnet**
- **traceroute**
- **quit**
- **help**

The **no** form of the command disables accounting. You can also disable accounting by using the **aaa accounting** command specifying the **none** option.

Examples

The following example configures command accounting, with the CLI information being forwarded to the TACACS+ server.

```
device(config)# aaa accounting commands default start-stop tacacs+
```

The following example configures command accounting, with the CLI information being forwarded to the RADIUS server.

```
device(config)# aaa accounting commands default start-stop radius
```

The following example disables login accounting by specifying the **none** option; command accounting (when also configured) remains active.

```
device(config)# aaa accounting exec default start-stop none
```

The following example disables login accounting by using the **no aaa accounting** command; command accounting (when also configured) remains active.

```
device(config)# no aaa accounting exec default start-stop
```

aaa authentication

Configures the Authentication, Accounting, and Authorization (AAA) log-in sequence.

Syntax

```
aaa authentication login { default | ldap | local | oauth2 | radius
   | tacacs+ } [ { local | local-auth-fallback | ldap-auth-fallback |
   oauth2-auth-fallback | radius-auth-fallback | tacacs+-auth-fallback }
   [ local-auth-fallback ] ]

no aaa authentication login
```

Command Default

The default server is Local.

Parameters

login

Specifies the type of server that will be used for AAA on the device. The local server is the default. Specify one of the following options.

default

Specifies the default mode (local server). Authenticates the user against the local database only. If the password does not match or the user is not defined, the login fails.

ldap

Specifies the Lightweight Directory Access Protocol (LDAP) servers.

local

Specifies the local device database if previous authentication methods are inactive.

oauth2

Specifies the OAuth2 token.

radius

Specifies the RADIUS servers.

tacacs+

Specifies the TACACS+ servers.

ldap-auth-fallback

Specifies that LDAP authentication be used if the previous authentication methods are not active or the authentication attempt fails. This is an optional parameter.

oauth2-auth-fallback

Specifies that OAuth2 authentication be used if the previous authentication methods are not active or the authentication attempt fails. This is an optional parameter.

radius-auth-fallback

Specifies that RADIUS authentication be used if the previous authentication methods are not active or the authentication attempt fails. This is an optional parameter.

tacacs+-auth-fallback

Specifies that TACACS+ authentication be used if the previous authentication methods are not active or the authentication attempt fails. This is an optional parameter.

local-auth-fallback

Specifies the local device database if previous authentication methods are not active or if authentication fails. This is an optional parameter.

Modes

Global configuration mode

Usage Guidelines

This command selects the order of authentication sources to be used for user authentication during the login process. Three sources of authentication are supported, primary, secondary, and tertiary. The secondary and tertiary authentication sources are optional. They are only used if they are configured and the preceding authentication source fails or is not reachable.

Note

Configuring secondary source of authentication is optional. Configuring tertiary source is also optional, however, it can only be configured when a secondary source is also configured.

Note

Fallback to the next authentication source will only happen if the previous authentication server is not available or not reachable. Fallback will not happen if the previous authentication server is available to authenticate and if wrong credentials are passed to it or if the server rejects the parameters passed to it for other reasons.

Caution

SSH imposes an immutable timeout of 120 seconds. Administrators should be aware that all authentication must complete within this time period.

It is recommended that retries and timeouts for the authentication servers be configured in a way that the authentication process (including fallback) completes within SSH's timeout value of 120 seconds.

For example, let us assume that there are five (5) servers configured for the primary authentication and five (5) servers for the secondary authentication. While authentication happens, connection will be tried to first primary server for the configured retry attempts for that server. If the server is unreachable, the next server in the list will be tried for the configured retry attempts. This process will be repeated till, either, one of the servers respond or all servers timeout. During this process of testing the various servers, there is a possibility that the SSH's timeout value is exceeded. Due to this, fallback to the next authentication method might not happen and your authentication may fail.

Authentication modes can only be set and cannot be added or deleted. For example, to change a configuration from *radius local* to *radius* only, execute the **no aaa authentication login** command to resets the configuration to the default mode, and then reconfigure the AAA mode with the desired setting.

Similarly, in a configuration with primary and secondary sources of authentication, the primary mode cannot be modified alone. For example, you cannot change from *radius local* or *radius ldap-auth-fallback local-auth-fallback* to *tacacs+ radius-auth-fallback* or *tacacs+ local local-auth-fallback* respectively. First remove the existing configuration and then configure it to the required configuration.

However, in a configuration where the primary and secondary sources of authentication are configured, it is possible to change the secondary source without using the **no aaa authentication login** command. For example, if you want to change the existing configuration from *radius tacacs+* to *radius ldap*, then issue the command **aaa authentication login radius ldap** directly.

With OAuth2 authentication, the log-in request from the north-bound interface uses the OAuth2 token as a password. The device authenticates the user based on the validity of the OAuth2 token.

Also, for OAuth2 authentication only, both the **local** and **local-auth-fallback** options allow fallback to the local database if the secondary source of authentication is configured as *local* or *local-auth-fallback*. In this scenario, they behave in the same manner.

If login fails through the primary source because none of the configured servers respond or the login is rejected by the server, authentication is done again through the secondary source or local option. If the authentication using the secondary source also fails, then *local-auth-fallback* is used if configured.

When “local-auth-fallback” option is specified as the tertiary option, local authentication is tried only when the primary and the secondary AAA authentication

service are either “unreachable” or “not available”. Unlike the “local” option, local authentication is not be attempted if the authentication with primary or secondary service fails.

Use the **no** form of the command to restore the authentication mode to local mode.

Examples

This example changes the AAA server to TACACS+ using the local device database as a secondary source of authentication.

```
device# configure terminal
device(config)# aaa authentication login tacacs+ local
Broadcast message from root (pts/0) Tue Apr  5 16:34:12 2011...
```

This example changes the AAA server from TACACS+ and no secondary source or tertiary source of authentication is configured.

```
device# configure terminal
device(config)# no aaa authentication login tacacs+ local
device(config)# aaa authentication login tacacs+
device(config)# show running-config aaa
aaa authentication login tacacs+
```

This example configures OAuth2 authentication, with radius is configured as the secondary authentication, and the tertiary authentication is also configured.

```
device# configure terminal
device(config)# aaa authentication login oauth2 radius-auth-fallback local-auth-fallback
```

This example resets authentication mode to the default.

```
device# configure terminal
device(config)# no aaa authentication login oauth2 local-auth-fallback
```

aaa authorization command

Enables AAA command authorization.

Syntax

aaa authorization command { **none** | **tacacs+** [**local**] }

no aaa authorization command

Command Default

By default, AAA command authorization is disabled.

Parameters

none

Disables command authorization.

tacacs+

Specifies using TACACS+ servers for command authorization.

local

Specifies using local authorization when the TACACS+ server is not active.

Modes

Global configuration mode.

Usage Guidelines

You can only enable command authorization when at least one TACACS+ server host is configured. When a TACACS+ server is not configured and you attempt to enable command authorization, the following error message is displayed and added to syslog.

```
% Error: No active TACACS server configuration exists to support the mode.
```

Similarly, when command authorization is enabled and there is only one TACACS+ server configured, you cannot remove the TACACS+ server (using the **no tacacs-server** command).

When, based on TACACS+ server configuration, the TACACS+ server rejects a command authorization request, the following error message is displayed and added to syslog.

```
Aborted: permission denied
```

With the current version of `confd`, custom RPC REST queries do not work when the **aaa authorization command tacacs+ local** form of the command is configured.

The **no aaa authorization command** command disables command authorization.

Examples

The following example shows how to enable AAA command authorization on a TACACS+ server and specify using local authorization if the TACACS+ server is not active.

```
device# configure terminal
device(config)# aaa authorization command tacacs+ local
```

The following example shows how to disable AAA command authorization.

```
device(config)# no aaa authorization command
```

accept-lifetime

Defines the time period when a key is active.

Syntax

accept-lifetime [**local** { **true** | **false**}] { *start-time* | **infinite** | *end-time* }

no accept-lifetime

Command Default

By default, the key lifetime is infinite. The key is always valid.

Parameters

local { **true** | **false**}

By default, the device treats the start time and end time as UTC. Specify the local key word to use local times.

start-time

Specifies the time of day and date when the key becomes active. In HH:MM:SS|MM/DD/YYYY format.

end-time

Specifies the time of day and date when the key expires. In HH:MM:SS|MM/DD/YYYY format.

infinite

Indicates that the accept lifetime of the key never expires.

Modes

Key configuration mode

Usage Guidelines

Use the **no** form of the command to revert to the default lifetime.

Examples

The following example configures a lifetime from June 6 2020 to December 4 2020 (UTC) for key 10 in key chain 1.

```
device# configure terminal
device(config)# keychain keychain1
device(config-keychain1)# key 10
device(config-keychain1-key10)# accept-lifetime 00:00:00|06/04/2020 23:59:59|12/04/2020
```

The following example configures a lifetime from June 6 2020 to December 4 2020 (local) for key 10 in key chain 1.

```
device# configure terminal
device(config)# keychain keychain1
device(config-keychain1)# key 10
device(config-keychain1-key10)# accept-lifetime local true 00:00:00|06/04/2020 23:59:59|
12/04/2020
```

accept-tolerance

Defines the number of seconds for which expired or soon-to-be activated keys can be used for validating received packets.

Syntax

accept-tolerance *number-of-seconds*

no accept-tolerance

Command Default

By default, the accept tolerance time is 600 seconds.

Parameters

number-of-seconds

Specifies the number of seconds by which activation time is decreased or expiration time is decreased. The default is 600. Valid values range from 0 to 600.

Modes

Keychain configuration mode

Usage Guidelines

Use the **no** form of the command to revert to the default of 600 seconds.

You can use the command to extend the validity of an expired key to ensure a smooth key rollover for the processing of a received packet.

You can use the command to decrease the activation time of a new key so that a received packet can be authenticated with the new key.

A longer accept tolerance period can reduce security if an old key was exposed.

Examples

The following example configures an accept tolerance of 500 seconds in key chain 1.

```
device# configure terminal
device(config)# keychain keychain1
device(config-keychain1)# accept-tolerance 500
```

action (management-heartbeat)

Specifies an action to be performed when the SLX device does not receive heartbeat messages from EFA within a preconfigured threshold time duration.

Syntax

action { **maintenance-mode-enable** | **no-action** }

no action

Parameters

maintenance-mode-enable

Sets the SLX device into the maintenance mode.

no-action

This is the default. No action is performed when the SLX device does not receive a heartbeat message from EFA within the threshold time.

Modes

Management Heartbeat mode

Usage Guidelines

You can assign only one action from the list.

Examples

The following example configures the action which sets the SLX device into maintenance mode.

```
SLX(config-management-heartbeat-manage) # action management-mode-enable
SLX(config-management-heartbeat-manage)# do show running-config management-heartbeat
manager
management-heartbeat manager
 enable
 threshold-timer 1
 action maintenance-mode-enable
!
SLX(config-management-heartbeat-manage)#
```

The following example configures the action as *no-action*. When the SLX devices does not receive any heartbeat messages from EFA and the threshold time has exceed, no action is taken.

```
SLX(config-management-heartbeat-manage) # action no-action
SLX(config-management-heartbeat-manage)# do show running-config management-heartbeat
manager
management-heartbeat manager
 enable
 threshold-timer 1
 action no-action
```

```
!
SLX(config-management-heartbeat-manage)#
```

The following example resets the current action to the default action. The default action for Management Heartbeat context is *no-action*.

```
SLX(config-management-heartbeat-manage) # no action
SLX(config-management-heartbeat-manage)# do show running-config management-heartbeat
manager
management-heartbeat manager
 enable
 threshold-timer 1
 action no-action
!
SLX(config-management-heartbeat-manage)#
```

acl-log-raslog

Enables Raslog messages for ACL rules with **log** keywords, and specifies how long the system waits before sending an ACL Raslog message.

Syntax

acl-log-raslog [**log-interval** *minutes*]

no acl-log-raslog

no acl-log-raslog log-interval

Command Default

ACL Raslogs are not enabled.

Parameters

log-interval *minutes*

Specifies, in minutes, the interval between ACL Raslog message. Values range from 1 through 10 minutes. The default value is 5 minutes.

Modes

ACL policy configuration mode

Usage Guidelines

When this feature is enabled, the initial Raslog message is generated at the first match for an ACL rule that includes the **log** keyword. Consequent Raslog messages are generated according to the current **no acl-log-raslog** value.

To restore the default disablement of this feature, use the **no acl-log-raslog** form of this command.

To restore the default 5-minute setting of this feature, use the **no acl-log-raslog log-interval** form of this command.

Examples

The following example enables ACL Raslogs on the device.

```
device# configure terminal
device(config)# acl-policy
device(config-acl-policy)# acl-log-raslog
```

The following example disables ACL Raslogs on the device.

```
device# configure terminal
device(config)# acl-policy
device(config-acl-policy)# no acl-log-raslog
```

The following example changes the current **log-interval** setting to 8 minutes.

```
device# configure terminal
device(config)# acl-policy
device(config-acl-policy)# acl-log-raslog log-interval 8
```

The following example restores the current **log-interval** setting to the default value of 5 minutes.

```
device# configure terminal
device(config)# acl-policy
device(config-acl-policy)# acl-log-raslog log-interval 8
```

The following output is an ACL Raslog example.

```
MAC ACL mac_2 permitted 1 packets on intf eth1/6 [SA:0010.1010.1001, DA:0001.0300.0500,
Type:0, VLAN:101, SIP:0.0.0.0, DIP:0.0.0.0, l3_proto:none, src_port:0, dst_port:0]

IP ACL v4acl denied 1 packets on intf eth1/6  [SA:0001.0300.0400,DA:0001.0300.0500,
Type:800, VLAN:100, SIP:2.2.2.2, DIP:6.6.6.6, l3_proto:udp, src_port:66, dst_port:77]

IPv6 ACL v6acl permitted 1 packets on intf po44  [SA:0001.0300.0400,DA:0001.0300.0500,
Type:86dd, VLAN:100, SIP:fe80::201:3ff:fe00:400,
DIP:3555:5555:6666:6666:7777:7777:8888:8888,
l3_proto:udp, src_port:63, dst_port:63]
```

acl-mirror

Defines a destination for ACL-based mirroring of a physical interface. This command will be deprecated in the future.

Syntax

acl-mirror source { **ethernet** *slot* **/** *port* | **port-channel** *index* | **ve** *index* } **destination** { **ethernet** *slot* **/** *port* | **port-channel** *index* }

no acl-mirror source { **ethernet** *slot* **/** *port* | **port-channel** *index* | **ve** *index* } **destination** { **ethernet** *slot* **/** *port* | **port-channel** *index* }

Command Default

No ACL mirror is defined.

Parameters

source

Specifies the interface for which you are defining a mirror.

ethernet

Specifies a physical Ethernet interface.

slot

Specifies a valid slot number. For devices that do not support linecards, specify `0`.

port

Specifies a valid port number.

port-channel *index*

Specifies a valid port-channel interface number.

ve *index*

Specifies a valid virtual ethernet interface number.

destination

Specifies the physical-interface or port-channel mirror to use as the destination for mirroring.

ethernet

Specifies a physical Ethernet interface.

slot

Specifies a valid slot number. For devices that do not support linecards, specify `0`.

port

Specifies a valid port number.

port-channel *index*

Specifies a port-channel interface.

Modes

Global configuration mode

Usage Guidelines

ACL mirroring applies to extended-ACL rules that include the **mirror** keyword.

ACL mirroring is supported only for ACLs applied to incoming traffic.

Only one destination mirror port is supported per source port.

There are parsing priorities among the **copy-sflow**, **log**, and **mirror** keywords, as follows:

- Although in a standard-ACL rule you can include **log** and **copy-sflow**, only one of the two is processed, as follows:
  - In a permit rule, the order of precedence is **copy-sflow** > **log**.
  - In a deny or hard-drop rule, the order of precedence is **log** > **copy-sflow**.
- Although in an extended-ACL rule you can include **log**, **mirror**, and **copy-sflow**, only one of the three is processed, as follows:
  - In a permit rule, the order of precedence is **mirror** > **copy-sflow** > **log**.
  - In a deny or hard-drop rule, the order of precedence is **log** > **copy-sflow** > **mirror**.

Only one destination port is supported per device.

To cancel an ACL mirroring destination, use the **no** form of this command.

Examples

The following example defines a physical port as the source port for mirroring.

```
device# config term
device(config)# acl-mirror source ethernet 0/1 destination ethernet 0/2
```

The following example defines a port-channel as the source for mirroring.

```
device# configure
device(config)# acl-mirror source ethernet 0/1 destination port-channel 2
```

The following example defines a Virtual Ethernet port as the source for mirroring.

```
device# config term
device(config)# acl-mirror source ve 99 destination port-channel 2
```

The following example displays the *running config* output for *acl-mirror*

```
device# show running-config acl-mirror
acl-mirror source port-channel 10 destination ethernet 0/9
acl-mirror source ve 10 destination ethernet 0/9
```

acl-policy

Accesses the ACL policy configuration mode, from which you can change the default settings regarding conflicting and duplicate ACL rules.

Syntax

acl-policy

Modes

Global configuration mode

Usage Guidelines

To return to global configuration mode, enter the **exit** command.

Examples

The following example accesses the ACL policy configuration mode and then disables the default restriction on duplicate rules within ACLs.

```
device# configure terminal
device(config)# acl-policy
device(config-acl-policy)# allow-duplicate-rules
```

action event-stream

Activates the event-stream action within the event-stream configuration mode.

Syntax

action event-stream

no action event-stream

Command Default

The action is not active.

Modes

Event-stream configuration mode.

Usage Guidelines

Use the **no action event-stream** command to halt the event stream action.

If an action does not exist in the database, a new action is created validated. If the event-stream is already activated on the device, then adding or updating an event action also takes immediate effect.

Examples

Example for activating the event stream.

```
device# configure terminal
device(config)# telemetry profile event-stream profile1
device(config-event-stream-profile1)# action event-stream
```

Example for deactivating the event stream.

```
device# configure terminal
device(config)# telemetry profile event-stream profile1
device(config-event-stream-profile1)# no action event-stream
```

action python-script

Specifies a Python file that runs when a trigger condition occurs.

Syntax

action python-script *file-name*

no action python-script *file-name*

Parameters

file-name

Specifies a Python script file-name. Valid values range from 4 through 32 characters (including the **.py** extension). The first character must be alphabetic.

Modes

Event-handler configuration mode

Usage Guidelines

You can assign only one action to a given event-handler profile.

You can also specify the Python file as part of the **event-handler** command.

To change the file assigned to a profile, you do not need to enter the **no** form of this command. You only need to enter **action python-script** *file-name*, specifying the new file name.

Running this command copies the Python script file from the `flash://` directory to the database. After specifying a file for all relevant event-handler profiles, you can delete it from the `flash://` directory.

If the event-handler for which you are modifying this command is active on the device, the changes take effect with no need to de-activate and re-activate the event-handler.

A Python event-handler script runs only if all of the following occur:

- Using the **copy** command, copy the Python file to the `flash://` location on the device.
- Using the **event-handler** command, create an event-handler profile.
- In configuration mode for that profile:
  - Using the **trigger** command, create one or more triggers.
  - Using the **action** command, specify the Python script that will be triggered.
- Using the **event-handler activate** command, activate an instance of the event handler.
- The trigger event occurs.

If an event-handler profile is not activated, the **no** form of this command deletes its action.

Examples

The following example specifies Python files for two event-handler profiles.

```
device# configure terminal
device(config)# event-handler eventHandler1
device(config-event-handler-eventHandler1)# action python-script example.py
device(config-event-handler-eventHandler1)# event-handler eventHandler2
device(config-event-handler-eventHandler2)# action python-script example2.py
```

action-profile

Creates an action profile.

Syntax

action-profile *action-profile-name*

no action-profile

Parameters:

action-profile-name

Specifies the action profile name. An action profile can be up to 32 characters.

Modes

Y1731 configuration mode

Usage Guidelines

Use the **no** form of the command to delete the corresponding configured action profile also its association with source and remote MEP pair.

Examples

This example shows how to create an action profile.

```
device# configure terminal
device (config-cfm)# y1731
device(config-cfm-y1731)# action-profile a1
device(config-cfm-y1731-action-profile-a1)# event ccm-up actions all
```

action-timeout

For an implementation of an event-handler profile, specifies the maximum number of minutes to wait for an action-script to complete execution. If the action-timeout expires, then script execution ends.

Syntax

action-timeout *minutes*

no action-timeout

Command Default

No action timeout is defined.

Parameters

minutes

Specifies the number of minutes to wait for an action-script to complete execution. If you specify "0", no timeout is set. Valid timeout values are any positive integer.

Modes

Event-handler activation mode

Usage Guidelines

To restore the default setting of no timeout, enter the **no** form of this command.

Examples

The following example specifies an action timeout of 30 minutes.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# action-timeout 30
```

activate (telemetry collector)

Activates the telemetry data stream—as defined by the telemetry profiles—to the external telemetry collector.

Syntax

activate

no activate

Command Default

The collector is deactivated.

Modes

Telemetry-collector configuration mode

Usage Guidelines

Activates the collector object, which streams telemetry information to the external telemetry collector.

Use the **no activate** command to disable streaming to the external telemetry collector.

Examples

Typical command execution.

```
device# configure terminal
device(config)# telemetry collector collector1
device(config-collector-collector1)# ip 10.24.12.87 port 8080
device(config-collector-collector1)# encoding json
device(config-collector-collector1)# profile system-profile
default_system_utilization_statistics
device(config-collector-collector1)# activate
```

activate (telemetry server)

Activates the internal gRPC telemetry-server.

Syntax

activate

no activate

Command Default

The internal gRPC telemetry-server is deactivated.

Modes

Telemetry-server configuration mode

Usage Guidelines

This command activates the internal gRPC telemetry-server.

To disable the internal gRPC telemetry-server, use the **no** form of this command.

Examples

Typical command execution.

```
device# configure terminal
device(config)# telemetry server
device(config-server-mgmt-vrf)# activate
device(config-server-mgmt-vrf)#
```

activate (VXLAN overlay gateway)

Activates a VXLAN overlay gateway instance.

Syntax

activate

no activate

Command Default

By default, a gateway is not activated during initial configuration.

Modes

Overlay gateway configuration mode

Usage Guidelines

It is recommended that you configure all gateway parameters before activating the gateway. This operation enables all tunnels that are associated with this gateway.

The following conditions that must be in place before you can execute the **activate** command:

- Loopback interfaces must be configured on all gateways. Refer to the **interface loopback** command,
- The IP address of the VXLAN gateway must be configured. Refer to the **ip interface** command.

Use the **no activate** command in VXLAN overlay gateway configuration mode to deactivate the gateway. All associated tunnels are also deactivated.

Examples

The following example activates a VXLAN gateway named gateway1. The gateway was previously configured by means of the **overlay-gateway** command:

```
device# configure terminal
device(config)# overlay-gateway gateway1
device(config-overlay-gw-gateway1)# activate
```

adaptive

Bypass LSPs can be made adaptive using the **adaptive** command. Bypass LSPs are non-adaptive by default. The user can modify the adaptive bypass LSPs adaptive-parameters without disabling the LSP. If the LSP is UP, then modifying an adaptive parameter, like exclude-interface or bandwidth, leads to the creation of a new instance of the bypass LSP. Adaptiveness can be manually enabled by using the **adaptive** command and can be disabled by **no** form of the same command. Use the **adaptive** to set the adaptive option for the dynamic bypass LSPs to be created for the MPLS protected interface.

Syntax

adaptive [**disable** | **enable**] [**record**]

Command Default

By default, LSPs are not adaptive.

By default, dynamic bypass LSPs are adaptive.

Parameters

disable

Disables the **adaptive** command.

enable

Enables the **adaptive** command.

record

Specifies RSVP session route recording.

Modes

MPLS LSP configuration mode

MPLS router MPLS interface dynamic bypass configuration mode

Examples

The following example configures an LSP named *to20* as an adaptive LSP.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp to20
device(config-router-mpls-lsp-to20)# adaptive
```

The following example enables the adaptive command for dynamic bypass MPLS Ethernet interface *0/8*.

```
device# configure
device(config)# router mpls
```

```
device(config-router-mpls)# mpls-interface ethernet 0/8
device(config-router-mpls-if-ethernet-0/8-dynamic-bypass)#  adaptive enable
```

add (telemetry)

Restores a previously removed field to a telemetry profile.

Syntax

add *telemetry-field*

no add *telemetry-field*

Command Default

All default fields are included in the telemetry profile.

Parameters

telemetry-field

Specifies the telemetry field to be included.

Modes

Telemetry profile configuration mode

Usage Guidelines

Use the **no add** command to remove a field.

Examples

The following example adds the add-discard-byte-count field to the default_queue_statistics profile.

```
device# configure terminal
device(config)# telemetry profile queue default_queue_statistics
device(config-queue-default_queue_statistics)# add add-discard-byte-count
```

The following example adds the max-queue-depth field to the default_enhanced_queue_max_queue_depth_statistics profile.

```
device# configure terminal
device(config)# telemetry profile enhanced-queue-max-queue-depth
default_enhanced_queue_max_queue_depth_statistics
device(config-enhanced-queue-max-queue-depth-
default_enhanced_queue_max_queue_depth_statistics)# add max-queue-depth
```

The following example removes the max-queue-depth field from the default_enhanced_queue_max_queue_depth_statistics profile.

```
device# configure terminal
device(config)# telemetry profile enhanced-queue-max-queue-depth
default_enhanced_queue_max_queue_depth_statistics
device(config-enhanced-queue-max-queue-depth-
default_enhanced_queue_max_queue_depth_statistics)# no add max-queue-depth
```

You must change profile configuration modes to change fields in another profile. Below is an example of adding fields to multiple profiles.

```
device# configure terminal
device(config)# telemetry profile interface default_interface_statistics
device(config-interface-default_interface_statistics)# add out-pkts
device(config-interface-default_interface_statistics)# exit
device(config)# telemetry profile queue default_queue_statistics
device(config-queue-default_queue_statistics)# add enq-byte-count
device(config-queue-default_queue_statistics)# add enq-pkt-count
```

The following example adds the out-packets and out-bytes fields to the default_mpls_traffic_lsp_statistics profile.

```
device(config)# telemetry profile mpls-traffic-lsp default_mpls_traffic_lsp_statistics
device(config-mpls-traffic-lsp-default_mpls_traffic_lsp_statistics)# add out-packets
device(config-mpls-traffic-lsp-default_mpls_traffic_lsp_statistics)# add out-bytes
```

additional-paths

Enables an additional-paths capability for all peers in a Border Gateway Protocol (BGP) address family.

Syntax

additional-paths { **receive** [**send**] | **send** }

no additional-paths receive

no additional-paths send

Command Default

Peer devices configured under a BGP address family are not capable of receiving or sending additional-paths.

Parameters

receive

Enables all peer devices configured under a BGP address family to receive additional-paths.

send

Enables all peer devices configured under a BGP address family to send additional-paths.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Note
Changes to the additional-paths capability for peers in a BGP address family take effect only after the BGP session is restarted.

Peers exchange and negotiate additional-path capability during session establishment.

Additional-paths can be enabled as receive only, send only, or both receive and send.

The **no** form of the command disables the specified (receive or send) additional-paths capability.

To remove the configuration when both the **receive** and **send** options have been set, you should enter both the **no additional-paths** command, specifying the **receive** option to disable the receive additional-paths capability, and the **no additional-paths** command, specifying the **send** option to disable the send additional-paths capability.

Examples

The following example shows how to enable peers configured under the IPv4 unicast address family to both receive and send additional-paths.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# additional-paths receive send
```

The following example shows how to disable the capability to receive additional-paths for all peers in the IPv4 unicast address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# no additional-paths receive
```

additional-paths select

Configures routes that are eligible for selection as additional-paths by peers configured under a Border Gateway Protocol (BGP) address family.

Syntax

additional-paths select { **all** [**best** *num*] [**group-best**] | **best** *num* | **group-best** }

no additional-paths select all

no additional-paths select best *num*

no additional-paths select group-best

Parameters

all

Causes all routes to be eligible for selection as additional-paths. A maximum of 16 routes is allowed.

best *num*

Specifies the number of best paths allowed for selection as additonal-paths. The number ranges from 2 through 16.

group-best

Causes all group-best paths to be eligible for selection as additional-paths. Only routes with a rank less than or equal to 16 are allowed. Even when it is the group best, a route with a rank greater than 16 is not eligible for selection as an additional path.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **all**, **best**, and **group-best** options are not mutually exclusive. When you perform a combination of these commands, the combined configuration is applied to the BGP address family.

The **no** form of the command removes the specified configuration.

When more than one option is configured, it is recommended that you disable each configured option separately; for example, disable the **all** configuration by using the **no additional-paths select** command specifying the **all** option, and so on.

Examples

The following example shows how to configure all (up to a maximum of 16) routes to be eligible for selection as additional-paths by all peers in the IPv4 unicast address family.

```
device# configure terminal
device(condig)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-router-ipv4u)# additional-paths select all
```

The following example shows how to restore the default configuration when the **all**, **best**, and **group-best** options were previously configured for the IPv4 unicast address family. It is recommended that you disable each configuration option separately.

```
device# configure terminal
device(condig)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-router-ipv4u)# no additional-paths select all
device(config-bgp-router-ipv4u)# no additional-paths select best 2
device(config-bgp-router-ipv4u)# no additional-paths select group-best
```

address-family ipv4 flowspec

Enables Border Gateway Protocol flow specification (BGP flowspec) IPv4 address family.

Syntax

address-family ipv4 flowspec [**vrf** *vrf-name*]

no address-family ipv4 flowspec [**vrf** *vrf-name*]

Command Default

BGP flowspec IPv4 address family is disabled.

Parameters

vrf *vrf-name*

Specifies the name of a VRF instance in which the BGP flowspec IPv4 address family is to be configured.

Modes

BGP configuration mode

Usage Guidelines

BGP flowspec IPv4 address-family configuration is only allowed in a VRF that is already configured with an IPv4 unicast address family.

When the **vrf** option is not specified, the **address-family ipv4 flowspec** command enables the BGP flowspec IPv4 address family for the default VRF; the IPv4 unicast address family is always configured on the default VRF.

The **no** form of the command disables BGP flowspec IPv4 address family.

You must disable BGP flowspec in a VRF by using the **no address-family ipv4 flowspec** command before removing the IPv4 unicast address-family configuration from the VRF.

This command is only supported on SLX 9540, SLX 9640, SLX 9740 and Extreme 8820 devices.

Examples

The following example shows how to enable BGP flowspec address family in the default VRF.

```
        device# configure terminal
device(config)# router bgp
```

```
device(config-bgp-router)# address-family ipv4 flowspec
device(config-bgp-ipv4fs)#
```

The following example shows how to enable BGP flowspec address family in a VRF named red.

```
                device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 flowspec vrf red
device(config-bgp-ipv4fs-vrf)#
```

address-family l2vpn evpn (BGP)

Enables the L2VPN address family configuration mode to configure a variety of BGP EVPN options.

Syntax

address-family l2vpn evpn

no address-family l2vpn evpn

Command Default

Disabled.

Modes

BGP configuration mode

Usage Guidelines

Use this command in BGP configuration mode to enter BGP address-family L2VPN EVPN configuration mode. The L2VPN EVPN configuration mode supports the EVPN Subsequent Address Family Identifier (SAFI), an address qualifier that provides additional information about the Network Layer Reachability Information (NLRI) type for a given attribute. The **no** form of this command removes the L2VPN EVPN address family configuration from the device and removes all configurations under the L2VPN address family.

Examples

This example enables BGP address family L2VPN EVPN configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)#
```

address-family unicast (BGP)

Enables the IPv4 or IPv6 address family configuration mode to configure a variety of BGP unicast routing options.

Syntax

address-family { **ipv4** | **ipv6** } **unicast** [**vrf** *vrf-name*]

no address-family { **ipv4** | **ipv6** } **unicast** [**vrf** *vrf-name*]

Command Default

Disabled.

Parameters

ipv4

Specifies an IPv4 address family.

ipv6

Specifies an IPv6 address family.

vrf *vrf-name*

Specifies a VRF instance.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to remove IPv4 or IPv6 address family configurations from the device.

Examples

The following example enables BGP IPv4 address-family configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)#
```

The following example enables BGP IPv6 address-family configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)#
```

The following example enables BGP IPv4 address-family configuration mode for VRF "green".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast vrf green
device(config-bgp-ipv4u-vrf)#
```

This example enables BGP IPv6 address-family configuration mode for VRF "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)#
```

address-family unicast (IS-IS)

Enables the IPv4 or IPv6 address family configuration mode for configuring a variety of Intermediate System-to-Intermediate System (IS-IS) unicast routing options.

Syntax

address-family { **ipv4** | **ipv6** } **unicast**

Command Default

Disabled.

Parameters

ipv4

Specifies the IPv4 address family.

ipv6

Specifies the IPv6 address family.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example enables IS-IS address-family IPv4 unicast configuration mode.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)#
```

The following example enables IS-IS address-family IPv6 unicast configuration mode.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv6 unicast
device(config-router-isis-ipv6u)#
```

adjustment-interval

There are two mechanisms of configuring LSP level parameters. The direct configuration and template-based configuration.

Syntax

adjustment-interval *value*

no adjustment-interval *value*

Command Default

The adjustment-interval is disabled.

Parameters

value

Specifies the time interval after which the LSP bandwidth must be adjusted. The range is from 300 through 259200 seconds (30 days). The default value is 86400 seconds (one day).

Modes

MPLS LSP configuration mode.

Usage Guidelines

The **no** option disables the auto-bandwidth for the LSP. The bandwidth immediately is set back to the traffic-engineering configured value.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example sets the bandwidth reallocation interval to 86400 seconds for LSP *xyz*.

```
device>enable
device# configure terminal
device(config)# router mpls
device(config-mpls)# lsp xyz
device(config-mpls-lsp-xyz)# auto-bandwidth
device(config-mpls-lsp-xyz-auto-bandwidth)# adjustment-interval 86400
```

adjustment-threshold

Specifies the automatic bandwidth adjustment sensitivity of an LSP to changes in bandwidth utilization.

Syntax

adjustment-threshold use-threshold-table

no adjustment-threshold

Command Default

The adjustment threshold is set to the default value.

Parameters

use-threshold-table

Specifies that the template use the autobw-threshold table to determine the threshold.

Modes

MPLS sub-configuration modes

config-mpls-template-template1

config-mpls-lsp-lsp1-autobw

Usage Guidelines

When automatic bandwidth adjustment is configured, bandwidth demand for the current interval is calculated and compared to the LSP current bandwidth allocation.

The **no** form of the command sets the adjustment threshold to the default value.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

admin-group

Administrative groups, also known as resource classes or link colors, allows the user to assign MPLS-enabled interfaces to various classes. When a device calculates the path for an LSP, it can take into account the administrative group to which a interface belongs; the user can specify which administrative groups the device can include or exclude when making its calculation.

Syntax

admin-group *admin_name admin_group_num*

no admin-group *admin_name admin_group_num*

Command Default

The command is disabled, by default.

Parameters

admin_name

Specifies the selected administrative group name.

admin_group_number

Specifies the selected administrative group number. The number range is 0-31.

Modes

MPLS policy mode.

Usage Guidelines

Up to 32 administrative groups can be configured on the device. The user can see an administrative group either by its name or its number. Before the user can see an administrative group by its name, the user must specify a name for the group at the MPLS policy level and associate the name with that administrative group's number.

After the user associates an administrative group name with a number, the user can see it by name when assigning interfaces to the group or including or excluding the group from LSP calculations.

The **no** form of the command disables specified admin-group.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example establishes three administrative groups.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# admin-group gold 30
device(config-router-mpls-policy)# admin-group silver 20
device(config-router-mpls-policy)# admin-group bronze 10
```

advertise capabilities ac-influenced-df-election

Enables the device to advertise DF Election Extended Community with the AC-DF capability flag set on the ES in the ES route.

Syntax

advertise capabilities ac-influenced-df-election

Parameters

ac-influenced-df-election

Enables the device to advertise DF Election Extended Community with the AC-DF capability flag set on the ES in the ES route.

Modes

Ethernet Segment mode

Usage Guidelines

This configuration can be provisioned only when ESI or LACP Auto is already configured on that Ethernet-Segment. Trying to configure this without setting ESI or LACP Auto configuration will return an error.

This configuration is automatically removed on removing ESI or LACP Auto on that Ethernet-Segment.

The **no** form of the command stops the device from advertising DF election extended community.

By default, DF election extended community is not advertised.

Supported In

SLX 9150, SLX 9250, SLX 9740, Extreme 8520, Extreme 8720, and Extreme 8820.

Examples

The following example shows how to configure and enable AF-influenced-DF-election on an ethernet segment.

```
 SLX# configure terminal
SLX (config)# interface Ethernet 0/3
SLX (conf-if-eth-0/3)# ethernet-segment
SLX (conf-if-eth-0/3-es)# esi 00:11:22:33:44:55:66:77:88:99
SLX (conf-if-eth-0/3-es)# advertise capabilities ac-influenced-df-election
SLX (conf-if-eth-0/3-es)# exit
SLX (conf-if-eth-0/3)# exit
```

```
SLX (config)# exit
SLX#
```

The **no** form of the command stops the device from advertising DF election extended community.

```
 SLX# configure terminal
SLX (config)# interface Ethernet 0/3
SLX (conf-if-eth-0/3)# ethernet-segment
SLX (conf-if-eth-0/3-es)# no advertise capabilities ac-influenced-df-election
SLX (conf-if-eth-0/3-es)# exit
SLX (conf-if-eth-0/3)# exit
SLX (config)# exit
SLX#
```

advertise dot1-tlv

Advertises globally to any attached device IEEE 802.1 organizationally specific Type, Length, Values (TLV) values, or for a specific LLDP profile.

Syntax

advertise dot1-tlv

no advertise dot1-tlv

Command Default

Advertisement is disabled.

Modes

Protocol LLDP and profile configuration modes

Usage Guidelines

Enter **no advertise dot1-tlv** to return to the default setting.

Examples

The following example advertises TLV configuration for IEEE 802.1

```
device# configure terminal
device(config)# protocol lldp
device(conf-lldp)# advertise dot1-tlv
device(conf-lldp)#
```

The following example advertises TLV configuration for IEEE 802.1 for a specific LLDP profile.

```
device(conf-lldp)# profile test1
device(config-profile-test1)# advertise dot1-tlv
device(conf-profile-test1)#
```

advertise dot3-tlv

Advertises to any attached device IEEE 802.3 organizationally specific Type, Length, Values (TLV) values, or for a specific LLDP profile.

Syntax

advertise dot3-tlv

no advertise dot3-tlv

Command Default

Advertisement is disabled.

Modes

Protocol LLDP and profile configuration modes.

Usage Guidelines

Enter **no advertise dot3-tlv** to return to the default setting.

Examples

The following example advertises TLV configuration for IEEE 802.3.

```
device# configure terminal
device(config)# protocol lldp
device(conf-lldp)# advertise dot3-tlv
device(conf-lldp)#
```

The following example advertises TLV configuration for IEEE 802.3 for a specific LLDP profile.

```
device(conf-lldp)# profile test1
device(config-profile-test1)# advertise dot3-tlv
device(conf-profile-test1)#
```

advertise optional-tlv

Advertises the optional Type, Length, and Values (TLV) values, or for a specific LLDP profile.

Syntax

advertise optional-tlv { **management-address** | **port-description** | **system-capabilities** | **system-description** | **system-name** }

no advertise optional-tlv

Command Default

Advertisement is disabled.

Parameters

management-address

Advertises the management address of the system.

port-description

Advertises the user-configured port.

system-capabilities

Advertises the capabilities of the system.

system-description

Advertises the system firmware version and the current image running on the system.

system-name

Advertises the name of the system.

Modes

Protocol LLDP and profile configuration modes

Usage Guidelines

Enter **no advertise optional-tlv** to return to the default setting.

Examples

The following example advertises the management address of the system and the user-configured port.

```
device# configure terminal
device(config)# protocol lldp
device(conf-lldp)# advertise optional-tlv ?
```

```
Possible completions:
  management-address    Management Address TLV
  port-description      Port-Description TLV
  system-capabilities   System Capabilities TLV
  system-description    System Description
  system-name           System Name TLV
device(conf-lldp)# advertise optional-tlv management-address ?
Possible completions:
  port-description      Port-Description TLV
  system-capabilities   System Capabilities TLV
  system-description    System Description
  system-name           System Name TLV
device(conf-lldp)# advertise optional-tlv management-address port-description
device(conf-lldp)#
```

The following example advertises the management address of the system for a specific LLDP profile.

```
device(conf-lldp)# profile test1
device(config-profile-test1)# advertise optional-tlv ?
Possible completions:
  management-address    Management Address TLV
  port-description      Port-Description TLV
  system-capabilities   System Capabilities TLV
  system-description    System Description
  system-name           System Name TLV
device(conf-profile-test1)# advertise optional-tlv management-address
device(conf-profile-test1)#
```

advertise-backup

Enables a backup VRRP router to send advertisement frames to the master VRRP router.

Syntax

advertise-backup

no advertise-backup

Command Default

Advertisement is disabled.

Modes

Virtual-router-group configuration mode

Usage Guidelines

Advertisement packets (or frames) are sent to all members of a VRRP group to indicate that the master router is operational. When the master router is not operational, the backup router becomes the master router. When you run this command, the backup router sends the frames every 60 seconds.

Use this command for VRRP-E, but not for VRRP.

Enter **no advertise backup** to return to the default setting (no periodic transmission).

Examples

This example enables the backup VRRP routers to send advertisement frames to the master VRRP router.

```
device# configure terminal
device(config)# interface ve 25
device(config-ve-25)# vrrp-extended-group 1
device(config-vrrp-extended-group-1)# advertise-backup
```

advertise-best-external

Stores and advertises the best external route for a Border Gateway Protocol (BGP) address family.

Syntax

advertise-best-external

no advertise-best-external

Command Default

The best external route for a BGP address family is not stored or advertised.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command restores the default configuration.

The **advertise-best-external** command enables storing and advertising of the best external route under an address family; the best external route is advertised in addition to the best route.

Examples

The following example shows how to store and advertise the best external route under the IPv4 address family in unicast mode.

```
device# configure terminal
device(bgp)# address-family ipv4 unicast
device(config-bgp)# advertise-best-external
```

advertisement-interval (VRRP)

Configures the interval at which the master VRRP router advertises its existence to the backup routers.

Syntax

advertisement-interval *range*

Command Default

The default is 1 second for version 2, 1000 milliseconds for version 3.

Parameters

range

Interval at which the master VRRP router advertises its existence to the backup routers. Valid values range from 1 through 255 seconds for VRRPv2 and from 1000 through 40900 milliseconds for VRRPv3.

Modes

Virtual-router-group configuration mode

Usage Guidelines

This interval is the length of time, in seconds, between each advertisement sent from the master to its backup VRRP routers. The advertisement notifies the backup routers that the master is still active. If the backup routers do not receive an advertisement from the master in a designated amount of time, the backup with the highest priority can assume the role of master.

This command can be used for either VRRP or VRRP-E and for VRRPv3 and VRRP-Ev3.

Examples

To set the advertisement interval to 30 seconds for VRRP-E group 10:

```
device# configure terminal
device(config)# interface ve 25
device(config-ve-25)# vrrp-extended-group 10
device(config-vrrp-extended-group-10)# advertisement-interval 30
```

To set the advertisement interval to 3000 milliseconds for VRRP-Ev3 group 19:

```
device# configure terminal
device(config)# interface ve 2019
device(config-ve-2019)# ipv6 vrrp-extended-group 19
device(config-vrrp-extended-group-19)# advertisement-interval 3000
```

advertisement-interval-scale

Configures the sub-second intervals at which the master VRRP-Ev3 device advertises its existence to the backup routers.

Syntax

advertisement-interval-scale *scale*

Command Default

The default advertisement interval scale is 1.

Parameters

scale

Number representing the scale of the division of a configured interval at which the master VRRP-Ev3 device advertises its existence to the backup devices. Valid values are 1, 2, 5, and 10.

Modes

Virtual-router-group configuration mode

Usage Guidelines

This command scales the advertisement interval of the master VRRP-Ev3 device as configured by the **advertisement-interval** command. A value of 1, 2, 5, or 10 can be set and the existing advertisement interval value is divided by the scaling value. For example, if the advertisement interval is 1 second and the scaling value is 10, the new advertisement interval is 100 milliseconds.

When all the advertisement intervals in a VRRP-Ev3 session are scaled, sub-second VRRP-Ev3 convergence is possible if a master fails. The advertisement notifies the backup devices that the master is still active. If the backup devices do not receive an advertisement from the master in a designated amount of time, the backup device with the highest priority can assume the role of master. Using sub-second advertising intervals, sub-second device redundancy can be achieved.

Note that the minimum advertisement interval for the **ipv6-vrrp-extended-group** command is 1000 milliseconds, so configure the intervals for the **advertisement-interval** and **advertisement-interval-scale** commands accordingly.

This command is only supported by VRRP-Ev3.

Examples

This example sets the scaling of the advertisement interval to 500 milliseconds for VRRP-Ev3 group 19.

```
device# configure terminal
device(config)# interface ve 2019
device(config-ve-25)# ipv6 vrrp-extended-group 19
device(config-vrrp-extended-group-10)# advertisement-interval 1
device(config-vrrp-extended-group-10)# advertisement-interval-scale 2
```

agent-enable

Enables the Keylime agent on the SLX device. This agent registers itself with remote keylime server(registrar) and listens for queries from the remote Keylime server(verifier).

Syntax

agent-enable

Modes

Remote Attestation mode

Examples

This example shows the complete configuration of Remote Attestation on this SLX device.

```
SLX # configure terminal
SLX (config)# remote-attestation
SLX (config-remote-attestation)# registrar-server 10.1.1.10 use-vrf default-vrf
SLX (config-remote-attestation-10.1.1.10/default-vrf)# registrar-port
SLX (config-remote-attestation-10.1.1.10/default-vrf)# exit
SLX (config-remote-attestation)# agent-enable agent-uuid UUID-F96FCC9E agent-port 3333
SLX (config-remote-attestation)# exit
SLX (config)# exit
SLX #
```

Platform Availability

This command and mode is only available on the Extreme 8720 and Extreme 8520 devices.

agent-port

Assigns the port on which the Keylime agent communicates.

Syntax

agent-port *port-number*

Parameters

port-number

The port number on which the Keylime Remote Attestation agent is communicating.

Command Default

The default port used by the Keylime agent is 9002.

Examples

This example shows the complete configuration of Remote Attestation on this SLX device.

```
SLX # configure terminal
SLX (config)# remote-attestation
SLX (config-remote-attestation)# registrar-server 10.1.1.10 use-vrf default-vrf
SLX (config-remote-attestation-10.1.1.10/default-vrf)# registrar-port
SLX (config-remote-attestation-10.1.1.10/default-vrf)# exit
SLX (config-remote-attestation)# agent-port 3333 agent-uuid UUID-F96FCC9E agent-enable
SLX (config-remote-attestation)# exit
SLX (config)# exit
SLX #
```

Platform Availability

This command and mode is only available on the Extreme 8720 and Extreme 8520 devices.

agent-uuid

Assigns a UUID value to the Keylime agent installed on the SLX device.

Syntax

agent-uuid *UUID*

Parameters

UUID

A unique value assigned to this Keylime agent. If this parameter is not provided, it is automatically generated.

Command Default

When a value is not supplied to the **agent-uuid** command, it is automatically generated and assigned to the Keylime agent.

Modes

Remote Attestation mode

Examples

This example shows the complete configuration of Remote Attestation on this SLX device.

```
SLX # configure terminal
SLX (config)# remote-attestation
SLX (config-remote-attestation)# registrar-server 10.1.1.10 use-vrf default-vrf
SLX (config-remote-attestation-10.1.1.10/default-vrf)# registrar-port
SLX (config-remote-attestation-10.1.1.10/default-vrf)# exit
SLX (config-remote-attestation)# agent-uuid UUID-F96FCC9E agent-port 3333 agent-enable
SLX (config-remote-attestation)# exit
SLX (config)# exit
SLX #
```

Platform Availability

This command and mode is only available on the Extreme 8720 and Extreme 8520 devices.

aggregate-address (BGP)

Configures the device to aggregate routes from a range of networks into a single network prefix.

Syntax

aggregate-address { *ip-addr ip-mask* | *ipv6-addr ipv6-mask* } [**advertise-map** *map-name* | **as-set** | **attribute-map** *map-name* | **summary-only** | **suppress-map** *map-name*]

no aggregate-address { *ip-addr ip-mask* | *ipv6-addr ipv6-mask* } [**advertise-map** *map-name* | **as-set** | **attribute-map** *map-name* | **summary-only** | **suppress-map** *map-name*]

Command Default

The address aggregation feature is disabled. By default, the device advertises individual routes for all networks.

Parameters

ip-addr

IPv4 address.

ip-mask

IPv4 mask.

ipv6-addr

IPv6 address.

ipv6-mask

IPv6 mask.

advertise-map

Causes the device to advertise the more-specific routes in the specified route map.

map-name

Specifies a route map to be consulted. Range is from 1 through 63 ASCII characters.

as-set

Causes the device to aggregate AS-path information for all routes in the aggregate routes from a range of networks into a single network prefix.

attribute-map

Causes the device to set attributes for the aggregate routes according to the specified route map.

map-name

Specifies a route map to be consulted.

summary-only

Prevents the device from advertising more-specific routes contained within the aggregate route.

suppress-map

Prevents the more-specific routes contained in the specified route map from being advertised.

map-name

Specifies a route map to be consulted.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to restore the defaults.

Examples

The following example aggregates routes from a range of networks into a single network prefix under the IPv6 address family and advertises the paths for this route as AS_SET.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# aggregate-address 2001:db8::/32 as-set
```

alias

Configures global or user-level aliases for device commands.

Syntax

alias *alias-name expansion*

no alias *alias-name*

Parameters

alias-name

Specifies the alias name. The number of characters can be from 1 through 255.

expansion

Specifies the CLI command to be triggered when the alias is entered. If the command is more than one word, type double quotes (") around the command. The number of characters can be from 1 through 1023.

Modes

Alias configuration mode

User-alias configuration mode

Usage Guidelines

Global aliases are available to all users.

User-level aliases are available only for a specified user.

In the alias configuration mode, to delete a global alias use the **no** form of his command.

In the user-alias configuration mode, to delete a user alias use the **no** form of his command.

Examples

The following example defines `ck` as a global alias that enters the **show clock** command.

```
device# configure terminal
device(config)# alias-config
device(config-alias-config)# alias ck "show clock"
```

For the user jdoe, the following example defines `sv` as a user-level alias that enters the **show version** command.

```
device# configure terminal
device(config)# alias-config
```

```
device(config-alias-config)# user jdoe
device(config-user-jdoe)# alias sv "show version"
```

alias-config

Launches the alias configuration mode, enabling you to define aliases.

Syntax

alias-config

no alias-config [**alias** | **user** *username*]

Parameters

alias

(For the **no** option) Deletes all global aliases.

user *username*

(For the **no** option) Deletes all aliases defined for the specified user.

Modes

Global configuration mode

Usage Guidelines

From the alias configuration mode—which you access by entering this command—you can manage global aliases. From that mode, you can also access the user-alias configuration mode for a specified user, from which you can manage aliases for that user.

To delete all global aliases, use the **no alias-config alias** form of this command.

To delete all aliases defined for a specified user, use the **no alias-config user** form of this command.

Examples

The following example accesses the alias configuration mode. It then defines `ck` as a global alias for the **show clock** command.

```
device# configure terminal
device(config)# alias-config
device(config-alias-config)# alias ck "show clock"
```

The following example deletes all aliases defined for the user jdoe.

```
device# configure terminal
device(config)# no alias-config user jdoe
```

allow-conflicting-rules

Towards editing ACLs, disables the default restriction on conflicting rules within an ACL. You can then create a conflicting rule before deleting the previous version.

Syntax

allow-conflicting-rules

no allow-conflicting-rules

Command Default

Conflicting rules are not allowed within an ACL.

Modes

ACL policy mode

Usage Guidelines

If the only difference between two rules is that one is a **deny** and the other a **hard-drop**, they are not considered conflicting. However, they are considered duplicates; refer to the **allow-duplicate-rules** topic.

Towards modifying ACL rules, you do not need to first remove ACLs from interfaces. Changes are implemented "on the fly," with no gap in protection.

We recommend that after ACL-editing sessions towards which you enabled **allow-conflicting-rules**, restore the default setting—by entering the **no allow-conflicting-rules** command.

Entering **no allow-conflicting-rules** launches a check of all ACLs for conflicting rules. If you did not immediately restore the default setting, and created ACLs with conflicting rules, you will need to delete conflicting rules before the software accepts **no allow-conflicting-rules**.

Examples

When modifying ACLs by changing a rule from **permit** to **deny** or **hard-drop**—or vice versa—the following flow is typical.

1. Enter the **show running-config** command to display the rules in the ACL that you need to modify.

```
device# show running-config mac access-list extended mac1
mac access-list extended mac1
 seq 10 permit host 0001.0001.0001 any
```

```
 seq 20 deny host 0001.0001.0002 any count
 seq 30 hard-drop host 0001.0001.0003 any mirror
```

2. Enter the **allow-conflicting-rules** command.

```
device# configure terminal
device(config)# acl-policy
device(config-acl-policy)# allow-conflicting-rules
```

3. In the ACL that you need to modify, create the new rule and then delete the old rule.

```
device(config-acl-policy)# exit
device(config)# mac access-list mac1
device(conf-macl-ext)# seq 21 permit host 0001.0001.0002 any count
device(conf-macl-ext)# no seq 20
```

4. Enter the **no allow-conflicting-rules** command to restore the default setting.

```
device(conf-macl-ext)# exit
device(config)# acl-policy
device(config-acl-policy)# no allow-conflicting-rules
```

allow-duplicate-rules

Towards editing ACLs, disables the default restriction on duplicate rules within an ACL. You can then create a duplicate rule at a new sequence before deleting the previous version.

Syntax

allow-duplicate-rules

no allow-duplicate-rules

Command Default

Duplicate rules are not allowed within an ACL.

Modes

ACL policy mode

Usage Guidelines

If the only difference between two rules is that one is a **deny** and the other a **hard-drop**, they are considered duplicates.

Towards modifying ACL rules, you do not need to first remove ACLs from interfaces. Changes are implemented "on the fly," with no gap in protection.

We recommend that after ACL-editing sessions towards which you enabled **allow-duplicate-rules**, restore the default setting—by entering the **no allow-duplicate-rules** command.

Entering **no allow-duplicate-rules** launches a check of all ACLs for duplicate rules. If you did not immediately restore the default setting, and created ACLs with duplicate rules, you will need to delete duplicates before the software accepts **no allow-duplicate-rules**.

Examples

When editing ACLs by duplicating a rule into a new sequence and then deleting the original rule, the following flow is typical.

1. Enter the **show running-config** command to display the rules in the ACL that you need to modify.

```
device# show running-config mac access-list extended mac1
mac access-list extended mac1
 seq 10 permit host 0001.0001.0001 any
```

```
 seq 20 deny host 0001.0001.0002 any count
 seq 30 hard-drop host 0001.0001.0003 any mirror
```

2. Enter the **allow-duplicate-rules** command.

```
device# configure terminal
device(config)# acl-policy
device(config-acl-policy)# allow-duplicate-rules
```

3. In the ACL that you need to modify, create the duplicate rule—specifying the new sequence number—and then delete the old rule.

```
device(config-acl-policy)# exit
device(config)# mac access-list mac1
device(conf-macl-ext)# seq 11 hard-drop host 0001.0001.0003 any mirror
device(conf-macl-ext)# no seq 30
```

4. Enter the **no allow-duplicate-rules** command to restore the default setting.

```
device(conf-macl-ext)# exit
device(config)# acl-policy
device(config-acl-policy)# no allow-duplicate-rules
```

allow multiple-ep-per-port

Enables configuring multiple endpoints on VPLS ports.

Syntax

allow multiple-ep-per-port

no allow multiple-ep-per-port

Command Default

Enables configuring multiple endpoints on VPLS ports.

Modes

Router Interface context

Usage Guidelines

This command enables multiple endpoint on the VPLS ports. Use this command after enabling routing on a BD and binding a router interface to the Bridge Domain. Use this command to enable configuring your Virtual Ethernet interface on a VPLS instance so that VE routing packets can reach remote VPLS endpoints.

Examples

This example turns on support of multiple endpoints on a VE interface.

```
SLX (config-terminal)# interface ve 100
SLX (config-router-interface-ve-100)# allow multi-ep-per-port
```

This example turns off the support of multiple endpoints on a VE interface.

```
SLX (config-terminal)# interface ve 100
SLX (config-router-interface-ve-100)# no allow multi-ep-per-port
```

always-compare-med

Configures the device always to compare the Multi-Exit Discriminators (MEDs), regardless of the autonomous system (AS) information in the paths.

Syntax

always-compare-med

no always-compare-med

Modes

BGP configuration mode

Usage Guidelines

The **no** form of the command disallows the comparison of the MEDs for paths from neighbors in different autonomous systems.

Examples

The following example configures the device always to compare the MEDs.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# always-compare-med
```

always-propagate

Enables the device to advertise BGP routes even though they are not installed in the RIB Manager.

Syntax

always-propagate

no always-propagate

Command Default

This feature is disabled.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

This example configures the device to advertise routes that are not installed in the RIB manager.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# always-propagate
```

This example configures the device to reflect advertise that are not installed in the RIB manager in IPv6 address-family unicast configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# always-propagate
```

This example configures the device to advertise routes that are not installed in the RIB manager in a nondefault VRF instance.

```
device# configure terminal
```

```
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# always-propagate
```

anycast-rp

Configures PIM Anycast rendezvous points (RPs) in IPv4 multicast domains.

Syntax

anycast-rp *rp-address* [*anycast-rp-peer-prefix-list*]

no anycast-rp *rp-address*

Command Default

By default, PIM Anycast RPs are not configured.

Parameters

rp-address

Specifies a shared RP address used among multiple PIM routers.

anycast-rp-peer-prefix-list

Specifies the list of Anycast IPv4 or IPv6 peers that are configured with the same Anycast RP address.

Modes

PIM router configuration mode

Usage Guidelines

PIM Anycast RP provides load balancing and fast convergence to PIM RPs in an IPv4 multicast domain. The RP address of the Anycast RP is a shared address used among multiple PIM routers, known as PIM RP. The PIM RP routers create an Anycast RP set. Each router in the Anycast RP set is configured using two IP addresses: a shared RP address in their loopback address and a separate, unique IP address. The loopback address must be reachable by all PIM routers in the multicast domain. The separate, unique IP address is configured to establish static peering with other PIM routers and communication with the peers.

When the source is activated in a PIM Anycast RP domain, the PIM first hop (FH) registers the source to the closest PIM RP. The PIM RP decapsulates the packet and creates the (s,g) state. If there are external peers in the Anycast RP set, the router re-encapsulates the packet with the local peering address as the source address of the encapsulation. The router distributes the packet to all Anycast RP peers. This re-encapsulation ensures source state distribution to all RPs in a multicast domain.

The **no anycast-rp** form of this command removes the Anycast RP configuration.

Examples

The following example shows how to configure IPv4 PIM Anycast RP.

```
device # configure terminal
device(config)#router-pim
device(config-pim-router)# anycast-rp 101.101.101.101 my-anycast-rps
device(config-pim-router)# exit
device(config)# ip prefix-list my-anycast-rpspermit 1.1.1.1/32
device(config)# ip prefix-list my-anycast-rpspermit 2.2.2.2/32
device(config)# interface loopback 1
device(config-Loopback-1)# ip address 1.1.1.1/32
device(config-Loopback-1)# ip pim-sparse
device(config)#interface loopback 2
device(config-Loopback-2)# ip address 2.2.2.2/32
device(config-Loopback-2)# ip pim-sparse
device(config-Loopback-11)# ip address 101.101.101.101/32
device(config-Loopback-11# ip pim-sparse
```

The following example shows how to configure IPv6 PIM Anycast RP, with 1234::22/128 configured on the other Anycast RP router in the domain.

Note

NOTE Use an IPv6 prefix list only with the **anycast-rp** command in an IPv6 environment. Likewise, only use an IPv6 prefix list when running the command in an IPv6 environment. If you use an IPv4 prefix list in an IPv6 environment, no error is generated and prefixes are ignored.

```
device(config)# ipv6 router pim
device(config-ipv6-router-pim-vrf-default-vrf)# anycast-rp 1234::100 anycast-rp-peer-plist
device(config-ipv6-router-pim-vrf-default-vrfr)# exit
device(config)# ipv6 prefix-list anycast-rp-peer-plist permit 1234::5/128
device(config)# ipv6 prefix-list anycast-rp-peer-plist permit 1234::22/128
device(config)# interface loopback 1
device(config-Loopback-2)# ipv6 address 1234::5/128
device(config-Loopback-1)# ipv6 pim-sparse
device(config)#interface loopback 10
device(config-Loopback-10)# ipv6 address 1234::100/24
device(config-Loopback-10)# ipv6 pim-sparse
```

area authentication (OSPFv3)

Enables authentication for an OSPF Version 3 (OSPFv3) area.

Syntax

area { *A.B.C.D* | *decimal* } **authentication spi** *value* { **ah** | **esp null** } { **hmac-md5** | **hmac-sha1** } **key** *key*

no area { *A.B.C.D* | *decimal* } **authentication spi** *value*

Command Default

Authentication is not enabled on an area.

Parameters

A.B.C.D

Area address in dotted decimal format.

decimal

Area address in decimal format.

spi

Specifies the Security Policy Index (SPI).

value

Specifies the Security Policy Index (SPI) value. Valid values range from decimal numbers 512 through 4294967295

ah

Specifies authentication header (ah) as the protocol to provide packet-level security.

esp

Specifies Encapsulating Security Payload (ESP) as the protocol to provide packet-level security.

null

Specifies that the ESP payload is not encrypted.

hmac-md5

Enables Hashed Message Authentication Code (HMAC) Message Digest 5 (MD5) authentication on the OSPF area.

hmac-sha1

Enables HMAC Secure Hash Algorithm 1 (SHA-1) authentication on the OSPF area.

key

Number used in the calculation of the message digest.

key

The 40 hexadecimal character key.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

Enter **no area authentication spi** to remove an authentication specification for an area from the configuration.

Note
MD5 passwords cannot have ASCII character 32 ('SPACE') as a part of the password string.

Examples

The following example enables ah and MD5 authentication for an OSPF area, setting a SPI value of 750.

```
device# configure termnial
device(config)# ip router-id 10.1.2.3
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# area 0 authentication spi 750 ah hmac-
md5 key abcef12345678901234fedcba098765432109876
```

The following example enables esp and SHA-1 authentication for an OSPF area, setting a SPI value of 900.

```
device# configure terminal
device(config)# ip router-id 10.1.2.3
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# area 0 authentication spi 900 esp null
hmac-md5 sha1 abcef12345678901234fedcba098765432109876
```

area nssa (OSPFv2)

Creates a not-so-stubby area (NSSA) or modifies its parameters.

Syntax

area { *ip-addr* | *decimal* } **nssa** { *metric* [**no-summary**] | **default-information-originate** }

no area nssa

Command Default

No areas are created.

Parameters

ip-addr

Area address in IP address format.

decimal

Area address In decimal format.

metric

Additional cost for using a route to or from this area.

no-summary

When configured on the NSSA area border router (ABR), this parameter prevents any Type 3 and Type 4 summary link-state advertisement (LSA) from being injected into the area. The only exception is that a default route is injected into the NSSA by the ABR, and strictly as a Type 3 LSA (not a Type 7, because that could cause intra-AS traffic to get routed out the AS). This makes the NSSA an NSSA totally stubby area, which can only have Type 1, 2 and 7 LSAs. **Note:** This parameter is disabled by default, which means the default route must use a Type 7 LSA.

default-information-originate

When configured on the ABR, this parameter injects a Type 7 default route into the NSSA area. As a result, the other NSSA routers install the default route through the advertising NSSA ABR. By default the NSSA ABR does not originate a default route to the NSSA.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

NSSAs are typically needed when one-way transmission of Type-5 LSAs (out of the area) is desired but injection of the same LSAs into the area is not acceptable.

Once created, the type of the area cannot be changed. The only exception to this rule is that an NSSA or stub area can be changed to a totally NSSA or a totally stub area, respectively.

The **no** form of the command deletes a NSSA.

Examples

The following example sets an additional cost of 5 on an NSSA identified as 2, includes the no-summary parameter, and prevents the device from importing type 3 and type 4 summary LSAs into the NSSA area.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# area 2 nssa 5 no-summary
```

area nssa (OSPFv3)

Creates a not-so-stubby area (NSSA) or modifies its parameters.

Syntax

area { *ip-addr* | *decimal* } **nssa** [*metric*] [**default-information-originate** [**metric** *num*] [**metric-type** { **type1** | **type2** }]] [**no-redsitribution**] [**no-summary**] [**translator-always**] [**translator-interval** *interval*]

no area nssa

Command Default

No areas are created.

Parameters

ip-addr

Area address in IP address format.

decimal

Area address in decimal format.

metric

Additional cost for using a route to or from this area. Valid values range from 1 through 1048575.

default-information-originate

When configured on the ABR, this parameter injects a Type 7 default route into the NSSA area. As a result, the other NSSA routers install the default route through the advertising NSSA ABR. By default the NSSA ABR does not originate a default route to the NSSA.

metric-type

Specifies how the cost of a neighbor metric is determined.

type1

The metric of a neighbor is the cost between itself and the router plus the cost of using this router for routing to the rest of the world.

type2

The metric of a neighbor is the total cost from the redistributing routing to the rest of the world.

no-redistribution

The no-redistribution parameter prevents an NSSA ABR from generating external (type-7) LSA into a NSSA area. This is used in the case where an ASBR should generate type-5 LSA into normal areas and should not generate type-7 LSA into a NSSA area. By default, redistribution is enabled in a NSSA.

no-summary

When configured on the NSSA area border router (ABR), this parameter prevents any Type 3 and Type 4 summary link-state advertisement (LSA) from being injected into the area. The only exception is that a default route is injected into the NSSA by the ABR, and strictly as a Type 3 LSA (not a Type 7, because that could cause intra-AS traffic to get routed out the AS). This makes the NSSA a NSSA totally stubby area, which can only have Type 1, 2 and 7 LSAs. **Note:** This parameter is disabled by default, which means the default route must use a Type 7 LSA.

translator-always

Configures the translator-role. When configured on an ABR, this causes the router to unconditionally assume the role of a NSSA translator. By default, translator-always is not set, the translator role by default is candidate.

translator-interval *interval*

Configures the time interval for which an elected NSSA translator continues to perform its duties even after its NSSA translator role has been disposed by another router. Valid values range from 10 through 60 seconds. By default the stability-interval is 40 seconds.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

NSSAs are typically needed when one-way transmission of Type-5 LSAs (out of the area) is desired but injection of the same LSAs into the area is not acceptable.

Once created, the type of the area cannot be changed. The only exception to this rule is that a NSSA or stub area can be changed to a totally NSSA or a totally stub area, respectively.

The **no** form of the command deletes a NSSA.

Examples

The following example sets an additional cost of 4 on a NSSA identified as 8 (in decimal format), and prevents any Type 3 or Type 4 summary LSAs from being injected into the area.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# area 8 nssa 4 no-summary
```

area prefix-list (OSPFv2)

Filters prefixes advertised in type 3 link-state advertisements (LSAs) between OSPFv2 areas of an area border router (ABR).

Syntax

area { *ip-addr* | *decimal* } **prefix-list** *name* { **in** | **out** }

no area { *ip-addr* | *decimal* } **prefix-list** *name* { **in** | **out** }

Parameters

ip-addr

Area address in IP address format.

decimal

Area address in decimal format.

prefix-list *name*

Specifies a prefix-list between 1 and 32 characters.

in

Specifies that the prefix list is applied to prefixes advertised to the specified area from other areas.

out

Specifies that the prefix list is applied to prefixes advertised out of the specified area to other areas.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

This command is only applicable to ABRs. The **no** form of the command changes or cancels the configured filter and advertises all type 3 LSAs.

Examples

The following example applies a prefix list to type 3 LSAs advertised out of an area with the area-id 10.1.1.1.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# area 10.1.1.1 prefix-list myprefixlist out
```

The following example applies a prefix list to type 3 LSAs advertised in to an area with the area-id 10.1.1.1.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# area 10.1.1.1 prefix-list myprefixlist in
```

area range (OSPFv2)

Specifies area range parameters on an area border router (ABR).

Syntax

area { *A.B.C.D* | *decimal* } **range** *E.F.G.H I.J.K.L* **advertise** [**cost** *cost_value*]

area { *A.B.C.D* | *decimal* } **range** *E.F.G.H I.J.K.L* **not-advertise** [**cost** *cost_value*]

area { *A.B.C.D* | *decimal* } **range** *E.F.G.H I.J.K.L* **cost** *cost_value*

no area range

Parameters

A.B.C.D

Area address in IP address format.

decimal

Area address in decimal format.

E.F.G.H I.J.K.L

Specifies the IP address and mask portion of the range. All network addresses that match this network are summarized in one route and advertised by the ABR.

advertise

Sets the address range status to *advertise* and generates a Type 3 summary LSA.

cost *cost_value*

Sets the cost value for the area range. This value is used as the generated summary LSA cost. The range for *cost_value* is 1 to 6777214. If this value is not specified, the cost value is the default range metric calculation for the generated summary LSA cost.

not-advertise

Sets the address range status to DoNotAdvertise; the Type 3 LSA is suppressed, and the component networks remain hidden from other networks. This setting temporarily pauses the route summary from the area.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

Use this command only on ABRs to specify a route summary for an existing area. The result is that one summary route is advertised to other areas by the ABR, in the form of

a Type 3 LSA. Routing information is condensed at area boundaries and external to the area, and only one route is advertised for each address range.

For example, use this command is if you have many small networks advertised from area 0 to any other area, or from any non-backbone area into the backbone. This command gives you a summary route instead of many smaller routes. In an area, the OSPF database on each router must be an exact copy of the databases of the other routers. This means that no summary is allowed in the area.

The **no** form of the command disables the specification of range parameters on an ABR.

Examples

The following example advertises to Area 3 all the addresses on the network 10.1.1.0 255.255.255.0 in the ABR you are signed into.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# area 3 range 10.1.1.0 255.255.255.0 advertise
```

area range (OSPFv3)

Specifies area range parameters on an area border router (ABR).

Syntax

area { *ip-addr* | *decimal* } **range** *ipv6 address/mask* [**advertise** | **not-advertise**] [**cost** *cost_value*]

no area range

Parameters

ip-addr

Area address in IP address format.

decimal

Area address in decimal format.

ipv6 address/mask

Specifies the IPv6 address in dotted-decimal notation and the IPv6 mask in CIDR notation. All network addresses that match this network are summarized in a single route and advertised by the ABR.

advertise

Sets the address range status to *advertise* and generates a Type 3 summary LSA.

cost *cost_value*

Sets the cost value for the area range. This value is used as the generated summary LSA cost. The range for *cost_value* is 1 to 6777214. If this value is not specified, the cost value is the default range metric calculation for the generated summary LSA cost.

not-advertise

Sets the address range status to DoNotAdvertise; the Type 3 LSA is suppressed, and the component networks remain hidden from other networks. This setting is used to temporarily pause route summarization from the area.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

Use this command only on ABRs to specify route summarization for an existing area. The result is that a single summary route is advertised to other areas by the ABR, in the form of a Type 3 LSA. Routing information is condensed at area boundaries and external to the area, and only a single route is advertised for each address range.

An example of when you might want to use this command is if you have many small networks advertised from area 0 to any other area, or from any non-backbone area into the backbone. This command gives you a summary route instead of many smaller routes. In an area, the OSPF database on each router must be an exact copy of the databases of the other routers. This means that no summarization is allowed within the area.

The **no** form of the command disables the specification of range parameters on an ABR.

Examples

The following example advertises to Area 3 all the addresses on the network 2001:db8:8::/45 in the ABR you are signed into.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# area 3 range 2001:db8:8::/45 advertise
```

area stub (OSPFv2)

Creates or deletes a stub area or modifies its parameters.

Syntax

area { *ip-addr* | *decimal* } **stub** *metric* [**no-summary**]

no area stub

Command Default

No areas are created.

Parameters

A.B.C.D

Area address in IP address format.

decimal

Area address In decimal format.

metric

Additional cost for using a route to or from this area. Valid values range from 1 through 6777215.

no-summary

When configured on the ABR, this parameter prevents any Type 3 and Type 4 summary LSAs from being injected into the area. The only exception is that a default route is injected into the stub/totally stubby area by the ABR as a Type 3 LSA. Enabling this parameter makes the area a so-called totally stubby area, which can only have Types 1 and 2. This parameter is disabled by default.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

Once created, the type of the area cannot be changed. The only exception to this rule is that a NSSA or stub area can be changed to a totally NSSA or a totally stub area, respectively.

The **no** form of the command deletes a stub area.

Examples

The following example sets an additional cost of 5 on a stub area called 2.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# area 2 stub 5
```

area stub (OSPFv3)

Creates or deletes a stub area or modifies its parameters.

Syntax

area { *ip-addr* | *decimal* } **stub** *metric*

area { *ip-addr* | *decimal* } **stub no-summary** *metric*

no area stub

Command Default

No areas are created.

Parameters

ip-addr

Area address in IP address format.

decimal

Area address In decimal format.

metric

Additional cost for using a route to or from this area. Valid values range from 3 through 1048575.

no-summary

When configured on the ABR, this parameter prevents any Type 3 and Type 4 summary LSAs from being injected into the area. The only exception is that a default route is injected into the stub/totally stubby area by the ABR as a Type 3 LSA. Enabling this parameter makes the area a so-called totally stubby area, which can only have Types 1 and 2. This parameter is disabled by default.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

Once created, the type of the area cannot be changed. The only exception to this rule is that a NSSA or stub area can be changed to a totally NSSA or a totally stub area, respectively.

The **no** form of the command deletes a stub area.

Examples

The following example sets an additional cost of 5 on a stub area called 2.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# area 2 stub 5
```

area virtual-link (OSPFv2)

Creates or modifies virtual links for an area.

Syntax

area { *ip-addr* | *decimal* } **virtual-link** *E.F.G.H* [**authentication-key** *password*] [**dead-interval** *time*] [**hello-interval** *time*] [**md5-authentication** { **key-activation-wait-time** *time* | **key-id** *num key* }] [**retransmit-interval** *time*] [**transmit-delay** *time*]

no area virtual-link

Command Default

No virtual links are created.

Parameters

ip-addr

Area address in IP address format.

decimal

Area address in decimal format.

E.F.G.H

ID of the OSPF router at the remote end of the virtual link.

authentication-key *password*

Sets the password and encryption method. Only one encryption method can be active on an interface at a time. All OSPF packets transmitted on the interface contain this password. All OSPF packets received on the interface are checked for this password. If the password is not present, then the packet is dropped.

dead-interval *time*

How long a neighbor router waits for a hello packet from the current router before declaring the router down. This value must be the same for all routers and access servers that are attached to a common network. Valid values range from 3 through 65535 seconds. The default is 40 seconds.

hello-interval *time*

Time between hello packets that the router sends on an interface. The value must be the same for all routers and access servers that are attached to a common network. Valid values range from 1 through 65535 seconds. The default is 10 seconds.

md5-authentication

Sets either MD5 key-activation wait time or key identifier.
key-activation-wait-time *time*

Time before a newly configured MD5 authentication key is valid. This parameter provides a graceful transition from one MD5 key to another without disturbing

the network. All new packets transmitted after the wait time ends will use the newly configured MD5 Key. OSPF packets that contain the old MD5 key are accepted for up to five minutes (300 seconds) after the new MD5 key is in operation. Valid values range from 0 through 14400 seconds. The default is 300 seconds.

key-id *num key*

The *num* is a number between 1 and 255 which identifies the MD5 key being used. This parameter is required to differentiate among multiple keys defined on a device. When MD5 is enabled, the key is an alphanumeric password of up to 16 characters that is later encrypted and included in each OSPF packet transmitted. You must enter a password in this field when the system is configured to operate with either simple or MD5 authentication. By default, the MD5 authentication key is encrypted.

retransmit-interval *time*

Time between Link State Advertisement (LSA) retransmissions for adjacencies belonging to the interface. Set this interval to a value larger than the expected round-trip delay between any two routers on the attached network. Valid values range from 0 through 3600 seconds. The default is 5 seconds.

transmit-delay *time*

Estimated time required to send an LSA on the interface. This value must be an integer greater than zero. The age of each LSA in the update packet is incremented by the value of this parameter before transmission occurs. Valid values range from 0 through 3600 seconds. The default is 1 second.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

The **no** form of the command removes a virtual link.

Examples

The following example creates a virtual link for an area whose decimal address is 1, and where the ID of the OSPFv2 device at the remote end of the virtual link is 10.1.2.3.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# area 1 virtual-link 10.1.2.3
```

area virtual-link (OSPFv3)

Creates or modifies virtual links for an area.

Syntax

area { *ip-addr* | *decimal* } **virtual-link** *A.B.C.D* [**dead-interval** *time* | **hello-interval** *time* | **hello-jitter** *interval* | **retransmit-interval** *time* | **transmit-delay** *time*]

no area virtual-link

Command Default

No virtual links are created.

Parameters

ip-addr

Area address in IP address format.

decimal

Area address in decimal format.

A.B.C.D

ID of the OSPFv3 device at the remote end of the virtual link.

dead-interval *time*

How long a neighbor device waits for a hello packet from the current device before declaring the device down. This value must be the same for all devices and access servers that are attached to a common network. Valid values range from 3 through 65535 seconds. The default is 40 seconds.

hello-interval *time*

Time between hello packets that the device sends on an interface. The value must be the same for all devices and access servers that are attached to a common network. Valid values range from 1 through 65535 seconds. The default is 10 seconds.

hello-jitter *interval*

Sets the allowed jitter between hello packets. Valid values range from 1 through 50 percent (%). The default value is 10%.

retransmit-interval *time*

Time between Link State Advertisement (LSA) retransmissions for adjacencies belonging to the interface. Set this interval to a value larger than the expected round-trip delay between any two devices on the attached network. Valid values range from 1 through 3600 seconds. The default is 5 seconds.

transmit-delay *time*

Estimated time required to send an LSA on the interface. This value must be an integer greater than zero. The age of each LSA in the update packet is

incremented by the value of this parameter before transmission occurs. Valid values range from 0 through 3600 seconds. The default is 1 second.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The values of the **dead-interval** and **hello-interval** parameters must be the same at both ends of a virtual link. Therefore, if you modify the values of these parameters at one end of a virtual link, you must make the same modifications on the other end of the link. The values of the other virtual link parameters do not require synchronization.

The **no** form of the command removes a virtual link.

Examples

The following example creates a virtual link for an area whose decimal address is 1, and where the ID of the OSPFv3 device at the remote end of the virtual link is 209.157.22.1.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# area 1 virtual-link 209.157.22.1
```

area virtual-link authentication (OSPFv3)

Enables authentication for virtual links in an OSPFv3 area.

Syntax

area { *ip-addr* | *decimal* } **virtual-link** *E.F.G.H* **authentication spi** *spi-value* { **ah** | **esp null** } { **hmac-md5** | **hmac-sha1** } **key** *key*

no area { *A.B.C.D* | *decimal* } **virtual-link** *E.F.G.H* **authentication spi** *spi*

Command Default

Authentication is not enabled on a virtual-link.

Parameters

ip-addr

Area address in IP address format.

decimal

Area address in decimal format.

E.F.G.H

ID of the OSPFv3 device at the remote end of the virtual link.

spi *spi-value*

Specifies the security policy index (SPI) value. Valid values range from decimal numbers 512 through 4294967295

ah

Specifies authentication header (ah) as the protocol to provide packet-level security.

esp

Specifies Encapsulating Security Payload (ESP) as the protocol to provide packet-level security.

null

Specifies that the ESP payload is not encrypted.

hmac-md5

Enables Hashed Message Authentication Code (HMAC) Message Digest 5 (MD5) authentication on the OSPF area.

hmac-sha1

Enables HMAC Secure Hash Algorithm 1 (SHA-1) authentication on the OSPF area.

key *key*

Number used in the calculation of the message digest. 40 hexadecimal character key. The 40 hexadecimal character key is encrypted by default.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

Enter **no area** { *A.B.C.D* | *decimal* } **virtual-link** *E.F.G.H* **authentication spi** *spi* to remove authentication from the virtual-links in the area.

Examples

The following example configures IPsec on a virtual link in an OSPFv3 area.

```
device# configure terminal
device(config)# ip router-id 10.1.2.2
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# area 2 virtual-link 10.1.2.2
authentication spi 600 ah hmac-sha1 key 1134567890223456789012345678901234567890
```

arp

Creates a static Address Resolution Protocol (ARP) entry.

Syntax

arp *A.B.C.D mac-address* **interface** { **ethernet** *slot* **/** *port* | **port-channel** *number* | **ve** *ve_id* }

no arp *A.B.C.D*

Parameters

A.B.C.D

Specifies a valid IP address.

mac-address

Specifies a valid MAC address.

interface

Specifies an interface type.

ethernet

Specifies a physical Ethernet interface.

slot

Specifies a valid slot number. For devices that do not support line cards, specify **0**.

port

Specifies a valid port number.

port-channel *number*

Specifies a port-channel.

ve *ve_id*

Specifies a virtual Ethernet (VE) interface.

Modes

Global configuration mode

VRF configuration mode

Usage Guidelines

The **no** form of the command deletes a static ARP entry.

Examples

The following example creates a static ARP entry that associates an IP address, a MAC address, and a physical port.

```
device# configure terminal
device(config)# arp 10.53.4.2 1245.7654.2348 interface ethernet 2/1
```

The following example configures a static ARP within a user-defined VRF.

```
device# configure terminal
device(config)# vrf test
device(config-vrf-test)# address-family ipv4 unicast
device(vrf-test-ipv4-unicast)# arp 10.6.6.7 0001.0001.0001 interface ethernet 2/1
```

arp access-list

Creates an Address Resolution Protocol (ARP) access control list (ACL), which is one of the steps implementing Dynamic ARP Inspection (DAI) on a VLAN.

Syntax

arp access-list *acl-name*

no arp access-list *acl-name*

Command Default

No ARP ACLs are defined.

Parameters

acl-name

Specifies the name of the ARP ACL. The name can be up to 63 characters in length, and must begin with an alphanumeric character. No special characters are allowed, except for the underscore (_) and hyphen (-).

Modes

Global configuration mode

Interface subtype configuration mode

Usage Guidelines

On untrusted interfaces of DAI-enabled VLANs, incoming ARP packets from permitted IP/MAC addresses are accepted only if all of the following steps were performed:

- Create the ACL, using the **arp access-list** command.
- In the ACL, create one or more rules, using the **permit ip host** command. Each rule specifies an IP/MAC address-pair.
- Apply the ACL to one or more VLANs, using the **ip arp inspection filter** command.
- Enable DAI on such VLANs, using the **ip arp inspection** command.

You can also append the **permit ip host** command to the **arp access-list** command.

You also need ARP ACLs to implement ARP Guard on a physical or port-channel interface.

The **no** form of the command deletes the ARP ACL if the ACL is not applied on any VLAN or port.

Examples

The following example creates an ARP ACL named "host2" and then defines one permit rule in that ACL.

```
device# configure terminal
device(config)# arp access-list host2
device(config-arp-acl)# permit ip host 1.1.1.1 mac host 0000.0011.0022
```

The following example creates an ARP ACL, creates **permit ip host** rules within, applies it to a VLAN, and enables Dynamic ARP Inspection (DAI) on the VLAN.

```
device# configure terminal
device(config)# arp access-list arp_acl_1
device(config-arp-acl)# permit ip host 1.1.1.1 mac host 0020.2222.2222
device(config-arp-acl)# permit ip host 1.1.1.2 mac host 0020.2222.2223
device(config-arp-acl)# exit

device(config)# vlan 200
device(config-vlan-200)# ip arp inspection filter arp_acl_1
device(conf-vlan-200)# ip arp inspection
```

The following example creates an ARP ACL, creates **permit ip host** rules within, and applies it to an interface. This is the first stage of ARP Guard implementation.

```
device# configure terminal
device(config)# arp access-list arp_acl_2
device(config-arp-acl)# permit ip host 1.1.1.1 mac host 0020.2222.2222
device(config-arp-acl)# permit ip host 1.1.1.2 mac host 0020.2222.2223
device(config-arp-acl)# exit

device(config)# interface ethernet 1/2
device(conf-if-eth-1/2)# switchport
device(conf-if-eth-1/2)# ip arp inspection filter arp_acl_2
```

Note
At this point in the flow, ARP Guard is not yet enabled. For enablement details, refer to the "ARP Guard" section of the *Extreme SLX-OS Layer 3 Routing Configuration Guide*.

as-path-ignore

Disables the comparison of the autonomous system (AS) path lengths of otherwise equal paths.

Syntax

as-path-ignore

no as-path-ignore

Command Default

The comparison of the AS path lengths of otherwise equal paths is enabled.

Modes

BGP configuration mode

Usage Guidelines

The **no** form of the command restores default behavior.

Examples

The following example configures the device to always disable the comparison of AS path lengths.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# as-path-ignore
```

auth-check

Disables Intermediate System-to-Intermediate System (IS-IS) authentication checking globally.

Syntax

auth-check { **level-1** | **level-2** } **disable**

no auth-check { **level-1** | **level-2** }

Command Default

IS-IS authentication checking is enabled by default.

Parameters

level-1

Specifies Level 1 packets only.

level-2

Specifies Level 2 packets only.

disable

Disables authentication checking.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command re-enables IS-IS authentication checking globally.

Examples

The following example disables IS-IS authentication checking for Level 1 packets.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# auth-check level-1 disable
```

The following example re-enables IS-IS authentication checking for Level 1 packets.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no auth-check level-1
```

The following example disables IS-IS authentication checking for Level 2 packets.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# auth-check level-2 disable
```

auth-key

Configures an authentication key for Intermediate System-to-Intermediate System (IS-IS) globally.

Syntax

auth-key { **level-1** | **level-2** } *string*

no auth-key { **level-1** | **level-2** }

Command Default

No authentication key is configured.

Parameters

level-1

Specifies Level 1 packets only.

level-2

Specifies Level 2 packets only.

string

Specifies a text string that is used as an authentication password. The string can be from 1 through 63 ASCII characters in length.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The authentication mode must be configured using the **auth-mode** command before an authentication password can be configured. If the authentication mode is reset for the level specified, the authentication key must also be reset. For more information, see auth-mode on page 163.

The **no** form of the command removes the IS-IS authentication key.

Note
MD5 passwords cannot have ASCII character 32 ('SPACE') as a part of the password string.

Examples

The following example configures an authentication key for Level 1 packets.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# auth-key level-1 mykey
```

The following example configures an authentication key for Level 2 packets.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# auth-key level-2 mysecurekey
```

auth-mode

Specifies the type of authentication used in Intermediate System-to-Intermediate System (IS-IS) packets globally.

Syntax

auth-mode md5 { **level-1** | **level-2** }

no auth-mode md5 { **level-1** | **level-2** }

Command Default

Disabled.

Parameters

md5

Specifies Message Digest 5 (MD5) authentication.

level-1

Specifies Level 1 packets only.

level-2

Specifies Level 2 packets only.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command removes the configured authentication mode. The authentication key must be removed using the no auth-key command before removing the configured authentication mode. If the authentication mode is reset for the specified level, the authentication key must also be reset.

Examples

The following example specifies that MD5 authentication is performed on Level 1 packets.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# auth-mode md5 level-1
```

The following example specifies that MD5 authentication is performed on Level 2 packets.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# auth-mode md5 level-2
```

auth-port

Configures a user datagram protocol (UDP) port for Remote Authentication Dial-In User Service (RADIUS) server authentication.

Syntax

auth-port *portnum*

no auth-port

Command Default

By default, port 1812 is used for RADIUS server authentication.

Parameters

portnum

Specifies the UDP port to use for RADIUS server authentication. The valid range is 0 through 65535. The default port is 1812.

Modes

RADIUS server host VRF configuration mode

Usage Guidelines

The **no** form of the command restores the command default value.

Examples

The following example shows how to configure port 1234 as the port used for connection to the RADIUS server for authentication.

```
device# configure terminal
device(config)# radius-server host 10.37.73.180 use-vrf green-vrf
device(config-host-10.37.73.180/green-vrf)# auth-port 1234
```

auto-cost reference-bandwidth (OSPFv2)

Configures reference bandwidth.

Syntax

auto-cost reference-bandwidth { *value* | **use-active-ports** }

no auto-cost reference-bandwidth

Command Default

Reference bandwidth is 100 Mbps.

Parameters

value

Reference bandwidth in Mbps. Valid values range from 1 through 4294967.

use-active-ports

Specifies that any dynamic change in bandwidth immediately affects the cost of OSPF routes. This parameter enables cost calculation for currently active ports only.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

Use this command to configure the cost of an interface that a device advertises to it's OSPF neighbors. OSPF calculates the cost of a route as the ratio of the reference bandwidth to the bandwidth of the egress interface. An increase in the reference bandwidth results in an increased cost. If the resulting cost is less than 1, the software rounds the cost up to 1.

The bandwidth for interfaces that consist of more than one physical port is calculated as follows:

- LAG group — The combined bandwidth of all the ports.
- Virtual interface — The lowest individual bandwidth of all the ports that carry the VLAN for the associated VE.

If a change to the reference bandwidth results in a cost change to an interface, the device sends a link-state update to update the costs of interfaces advertised by the device.

Note
If you specify the cost for an individual interface (by using the **ip ospf cost** command), the cost you specify overrides the cost calculated by the software.

The **no** form of the command disables bandwidth configuration.

Examples

The following example configures a reference bandwidth of 500.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# auto-cost reference-bandwidth 500
```

The reference bandwidth specified in this example results in the following costs:

- 10 Mbps port's cost = 500/10 = 50.
- 100 Mbps port's cost = 500/100 = 5.
- 1000 Mbps port's cost = 500/1000 = 0.5, which is rounded up to 1.

The costs for 10 Mbps and 100 Mbps ports change as a result of the changed reference bandwidth. Costs for higher-speed interfaces remain the same.

auto-cost reference-bandwidth (OSPFv3)

Configures reference bandwidth.

Syntax

auto-cost reference-bandwidth *value*

no auto-cost reference-bandwidth

Command Default

Reference bandwidth is 100 Mbps.

Parameters

value

Reference bandwidth in Mbps. Valid values range from 1 through 4294967. The default is 100 Mbps.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

Use this command to configure the cost of an interface that a device advertises to it's OSPF neighbors. OSPFv3 calculates the cost of a route as the ratio of the reference bandwidth to the bandwidth of the egress interface. An increase in the reference bandwidth results in an increased cost. If the resulting cost is less than 1, the software rounds the cost up to 1.

The bandwidth for interfaces that consist of more than one physical port is calculated as follows:

- LAG group — The combined bandwidth of all the ports.
- Virtual interface — The lowest individual bandwidth of all the ports that carry the VLAN for the associated VE.

If a change to the reference bandwidth results in a cost change to an interface, the device sends a link-state update to update the costs of interfaces advertised by the device.

Note
If you specify the cost for an individual interface using the **ipv6 ospf cost** command, the cost you specify overrides the cost calculated by the software.

The **no** form of the command restores the reference bandwidth to its default value and, thus, restores the default costs of the interfaces to their default values.

Examples

The following example configures a reference bandwidth of 500.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# auto-cost reference-bandwidth 500
```

The reference bandwidth specified in this example results in the following costs:

- 10 Mbps port's cost = 500/10 = 50.
- 100 Mbps port's cost = 500/100 = 5.
- 1000 Mbps port's cost = 500/1000 = 0.5, which is rounded up to 1.
- 155 Mbps port cost = 500/155 = 3.23, which is rounded up to 4
- 622 Mbps port cost = 500/622 = 0.80, which is rounded up to 1
- 2488 Mbps port cost = 500/2488 = 0.20, which is rounded up to 1

The costs for 10 Mbps, 100 Mbps, and 155 Mbps ports change as a result of the changed reference bandwidth. Costs for higher-speed interfaces remain the same.

auto-shutdown-new-neighbors

Disables the establishment of BGP connections with a remote peer when the peer is first configured.

Syntax

auto-shutdown-new-neighbors

no auto-shutdown-new-neighbors

Command Default

This feature is disabled.

Modes

BGP configuration mode

Usage Guidelines

The **auto-shutdown-new-neighbors** command applies to all neighbors configured under each VRF. When the **auto-shutdown-new-neighbors** command is used, any new neighbor configured will have the shutdown flag enabled for them by default. Once all the neighbor parameters are configured and it is ready to start the establishment of BGP session with the remote peer, the BGP neighbor's shutdown parameter has to disabled by removing the shutdown command for the neighbor.

The **no** form of the command restores the default.

Examples

The following example enables auto shutdown of BGP neighbors on initial configuration.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# auto-shutdown-new-neighbors
```

The following example disables the peer shutdown state and begins the BGP4 session establishment process.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 65520
device(config-bgp-router)# no neighbor 10.1.1.1 shutdown
```

autobw-threshold table

Changes the parser mode to the config-router-mpls-autobw-threshold-table mode, allowing the user to change the absolute adjustment threshold values.

Syntax

autobw-threshold-table

no autobw-threshold-table

Command Default

There are no entries in the adjustment-threshold table.

Modes

MPLS configuration mode

Usage Guidelines

The **no** form of the command clears all entries in adjustment-threshold table.

Examples

The following example configures the autobw-threshold table

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# autobw-threshold-table
device(config-mpls-autobw-threshold-table)# bandwidth-ceiling 10 threshold 2000
device(config-mpls-autobw-threshold-table)# bandwidth-ceiling 1000 threshold 3000
device(config-mpls-autobw-threshold-table)# bandwidth-ceiling 10000 threshold 5000
```

backup-advertisement-interval

Configures the interval at which backup VRRP routers advertise their existence to the master router.

Syntax

backup-advertisement-interval *interval*

Command Default

The default backup advertisement-interval is 60 seconds.

Parameters

interval

Interval at which a backup VRRP router advertises its existence to the master router. Valid values range from 60 through 3600 seconds.

Modes

Virtual-router-group configuration mode

Usage Guidelines

The interval is the length of time, in seconds, between each advertisement sent from the backup routers to the master router. The advertisement notifies the master router that the backup is still active. If the master router does not receive an advertisement from the backup in a designated amount of time, the backup with the highest priority can assume the role of master.

This command can be used for either VRRP or VRRP-E.

Examples

To set the backup advertisement interval to 120 seconds for VRRP-E group 10:

```
device# configure terminal
device(config)# interface ve 25
device(config-ve-25)# vrrp-extended-group 10
device(config-vrrp-extended-group-10)# backup-advertisement-interval 120
```

bandwidth-ceiling

This command adds a new threshold change point to the autobw-threshold table. When the change point is already there, the threshold value updates to the new value.

Syntax

bandwidth-ceiling [*bw in kbps* | **max-bw-threshold** [*threshold _n_kbps* | [**percentage** *threshold_percentage*]]

no bandwidth-ceiling

Command Default

There are no bandwidth ceiling entry.

Parameters

bw_in_kbps

The bandwidth in kilobytes per second. 0 - 0x7FFFFFFF. Range of bandwidth in kbps.

max-bw-threshold *theshold _in_kbps*

The threshold in kilobytes per second. 0 - 0x7FFFFFFF. Rangeof bandwidthin kbps.

threshold *threshold_percentage*

The threshold percentage per second. 0 - 100%. By default, the last ceiling is used.

Note
The first parameter indicates that any rate above the maximum ceiling configured. The second parameter is the threshold in kbps. for those rates.

Modes

MPLS global adjustment threshold configuration mode.

Usage Guidelines

Review the updated global adjustment-threshold table after executing this command.

The max keyword sets the threshold for any traffic-rate above the maximum bandwidth-ceiling configured in the table.

The **no** function of the command remove the bandwidth ceiling entry from the table.

MPLS is supported on Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices.

Examples

The following example configures the bandwidth ceiling maximum threshold percentage to 10.

```
device>configure
device(config)# router mpls
device(config-router-mpls)# autobw-threshold-table
device(config-router-mpls-autobw-threshold-table)# max threshold percentage 10
```

banner

Defines an incoming, login, or message of the day banner.

Syntax

banner { **incoming** | **login** | **motd** } *string*

no banner incoming | **login** | **motd**

Parameters

incoming

Sets the incoming terminal line banner that is displayed on the console when a user establishes a Telnet session.

login

Sets the login banner that is displayed on the user terminal when the user logs into the device.

motd

Sets the message of the day (MOTD) that is displayed on the user terminal when a Telnet CLI session is established.

string

Specifies a text string from 1 through 2048 characters in length including spaces.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of the command to delete the banner.

The banner can appear on multiple lines if you enter multiline mode by using **Esc-M** and exit by using **CTRL-D**.

Examples

To create a login banner with a single line:

```
device # configure terminal
device(config)# banner login "Please do not disturb the setup on this switch"
```

beacon enable

Configures LED beacons at device or interface level.

Syntax

beacon enable chassis [**length** *length* | **start** *start-time*]

beacon enable interface { **ethernet** {*slot/port* [**length** *length* **start** *start-time*] } | { **port-channel** *port-channel* } }

Parameters

length

Specifies the duration in minutes. The range can be an integer in the range 1 to 1440.

start-time

Specifies the start time in the format (CCYY-MM-DD**T**HH:MM:SS). Date and time are separated by a delimiter **T**.

port-channel

Specifies the port channel ID.

Modes

Privileged EXEC mode

Usage Guidelines

The **chassis** option affects all device interfaces.

Blink rate is one blink per second.

RASLOG messages are generated for chassis beacon enable and disable.

Examples

The following example configures beacon LEDs at device level.

```
device# beacon enable chassis ?
Possible completions:
  length   Duration in minutes
  start    Start time
  |        Output modifiers
  <cr>

device# beacon enable chassis length ?
Possible completions:
  <Enter a valid integer, 1 .. 1440>
device# beacon enable chassis length 1 ?
Possible completions:
  start   Start time
```

```
  |       Output modifiers
  <cr>

device# beacon enable chassis length 1 start ?
Possible completions:
  <dateTime (CCYY-MM-DDTHH:MM:SS)>
 Please note the delimiter T which is used to separate date and time
```

The following example configures beacon LEDs based at interface or port-channel level.

```
device# beacon enable interface ?
Possible completions:
  ethernet       Ethernet interface
  port-channel   Port-channel interface

device# beacon enable interface ethernet 0/1 ?
Possible completions:
  length   Duration in minutes
  start    Start time
  |        Output modifiers
<cr>

device# beacon enable interface port-channel ?
Possible completions:
  <port channel id>
```

The following example shows RASLOG messages for chassis beacon enable and disable.

```
device# 2017/01/09-19:32:00, [NSM-2071], 7549, DCE, INFO, SLX9540, Chassis beaconing is
enabled
device# 2017/01/09-19:33:00, [NSM-2072], 7550, DCE, INFO, SLX9540, Chassis beaconing is
disabled
```

bestpath prefix-validation disable

This command disables the validation of prefixes that are received from BGP peers when calculating best path. The default behavior is to allow using all prefixes for best path calculation.

Syntax

bestpath prefix-validation disable

[no] bestpath prefix-validation disable

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The default behavior is to allow the use of all prefixes for best path calculation.

The [no] format of this command enables the default behavior.

Examples

This example shows the commands to disable validation of prefixes while calculating best path, irrespective of the prefix validation state received from the RPKI cache server.

```
SLX(config)#router bgp
SLX(config-bgp-router)# address-family ipv4 unicast
SLX(config-bgp-ipv4u)# bestpath prefix-validation disable
SLX(config-bgp-ipv4u)#
```

bestpath prefix-validation disallow-invalid

This command prevents the use of invalid prefixes for calculating bestpaths. The default behavior is to allow invalid prefixes to be used in bestpath calculation.

Syntax

bestpath prefix-validation disallow-invalid

[no] bestpath prefix-validation disallow-invalid

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The [no] form of this command enables the default behavior of allowing all prefixes (including invalid prefixes) to be used for bestpath calculation.

Examples

This example shows the commands to prevent invalid prefixes being used when calculating bestpath. This is irrespective of the prefix validation state received from the RPKI cache server.

```
SLX(config)#router bgp
SLX(config-bgp-router)# address-family ipv4 unicast
SLX(config-bgp-ipv4u)# bestpath prefix-validation disallow-invalid
SLX(config-bgp-ipv4u)#
```

bfd

Enables Bidirectional Forwarding Detection (BFD).

Syntax

bfd

no bfd

Modes

IS-IS router configuration mode

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

Use the **bfd** command in IS-IS router configuration mode to enable BFD sessions on all IS-IS interfaces on which BFD has been configured using the **isis bfd** command.

Use the **bfd** command in OSPF router configuration mode to enable BFD sessions on all OSPFv2 interfaces on which BFD has been configured using the **ip ospf bfd** command. Use the **bfd** command in OSPFv3 router configuration mode to enable BFD sessions on all OSPFv3 interfaces on which BFD has been configured using the **ipv6 ospf bfd** command.

The **no** form of the command disables BFD globally.

Examples

The following example enables BFD globally in IS-IS router configuration mode.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# bfd
```

The following example enables BFD globally in OSPF router configuration mode.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# bfd
```

The following example disables BFD globally in OSPFv3 router configuration mode.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# no bfd
```

bfd holdover-interval

Sets the time interval for which Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), or Border Gateway Protocol (BGP) routes are withdrawn after a Bidirectional Forwarding Detection (BFD) session is declared down.

Syntax

bfd holdover-interval *time*

no bfd holdover-interval *time*

Command Default

The BFD holdover interval is set to 0 by default.

Parameters

time

Specifies the BFD holdover interval in seconds. In BGP configuration mode, valid values range from 0 through 30 and the default is 0. In IS-IS router configuration mode, OSPF router VRF and OSPFv3 router VRF configuration mode, valid values range from 0 through 20 and the default is 0.

Modes

BGP configuration mode

IS-IS router configuration mode

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The BFD holdover interval is supported for both single-hop and multihop sessions.

In BGP configuration mode, use this command to set the BFD holdover interval globally for BGP. In OSPF router configuration mode or OSPF router VRF configuration mode, use this command to set the BFD holdover interval globally for OSPFv2. In OSPFv3 router or OSPFv3 router VRF configuration mode, use this command to set the BFD holdover interval globally for OSPFv3. In IS-IS router configuration mode, use this command to set the BFD holdover interval globally for IS-IS.

The IS-IS options are supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540devices only.

The **no** form of the command removes the configured BFD holdover interval from the configuration, and reverts to the default value of 0.

Examples

The following example sets the BFD holdover interval globally to 15 in BGP configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# bfd holdover-interval 15
```

The following example sets the BFD holdover interval globally to 12 in OSPF router configuration mode.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# bfd holdover-interval 12
```

The following example sets the BFD holdover interval globally to 20 in OSPFv3 router configuration mode.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# bfd holdover-interval 20
```

The following example sets the BFD holdover interval globally to12 in IS-IS router configuration mode.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# bfd holdover-interval 12
```

bfd interval

Configures Bidirectional Forwarding Detection (BFD) session parameters on an interface.

Syntax

bfd interval *transmit-time* **min-rx** *receive-time* **multiplier** *number*

no bfd interval *transmit-time* **min-rx** *receive-time* **multiplier** *number*

Parameters

transmit-time

Specifies the interval, in milliseconds, that a device waits to send a control packet to BFD peers. Valid values range from 50 through 30000. The default is 300.

min-rx *receive-time*

Specifies the interval, in milliseconds, that a device waits to receive a control packet from BFD peers. Valid values range from 50 through 30000. The default is 300.

multiplier *number*

Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD determines that the connection to that peer is not operational. Valid values range from 3 through 50. The default is 3.

Modes

BGP configuration mode

Interface subtype configuration mode

Usage Guidelines

The *transmit-time* and **min-rx** *receive-time* parameters are the intervals desired by the local device. The actual values in use are the negotiated values.

Use the **bfd interval** command in BGP configuration mode for multihop sessions only. Single-hop sessions in BGP use the values that are configured at the interface level with the **bfd interval** command. Otherwise, the default BFD interfal is used.

The **no** form of the command reverts to the default parameters.

Examples

The following example sets the BFD session parameters for an Ethernet interface.

```
device# configure terminal
```

```
device(config)# interface ethernet 0/4
device(conf-if-eth-0/4)# bfd interval 100 min-rx 100 multiplier 10
```

The following example sets the BFD session parameters for a virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 24
device(config-if-ve-24)# bfd interval 120 min-rx 150 multiplier 8
```

The following example sets the BFD session parameters globally for BGP.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# bfd interval 140 min-rx 125 multiplier 44
```

bfd max-session-support

Defines the maximum number of Bidirectional Forwarding Detection sessions that can be created.

Syntax

bfd max-session-support *number-of-sessions*

no bfd max-session-support

Command Default

By default, 250 BFD sessions are supported.

Parameters

number-of-sessions

Defines the maximum number of BFD sessions that can be created. Valid values range from 251 through 1000.

Modes

Global configuration mode

Usage Guidelines

If the maximum session count is changed to a higher value, notification is sent to the static protocol. The static protocol sends a session-creation request to BFD for any previous sessions that failed because the maximum session count was exceeded.

If the maximum session count is changed to a lower value, then *x* number of current sessions are brought down until the number of sessions does not exceed the maximum session count.

Use the **no** form of the command to revert to the default of 250 sessions.

Examples

This example sets the maximum at 300 sessions.

```
device# configure terminal
device(config)# bfd max-session-support 300
```

This example restores the default of 250 sessions.

```
device# configure terminal
device(config)# no bfd max-session support
```

bfd shutdown

Disables Bidirectional Forwarding Detection (BFD) on an interface.

Syntax

bfd shutdown

no bfd shutdown

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command re-enables BFD sessions on an interface.

Examples

The following example disables BFD sessions on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/4
device(conf-if-eth-1/4)# bfd shutdown
```

The following example disables BFD sessions on a virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 24
device(config-if-ve-24)# bfd shutdown
```

bgp-redistribute-internal

Causes the device to allow the redistribution of IBGP routes from BGP into OSPF for non-default VRF instances.

Syntax

bgp-redistribute-internal

no bgp-redistribute-internal

Command Default

This feature is disabled.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of the command to restore the defaults.

By default, with default VRF instances, the device does not allow the redistribution of IBGP routes from BGP4 and BGP4+ into OSPF. This helps to eliminate routing loops. In non-default VRF instances, use this command to allow the redistribution of IBGP routes from BGP into OSPF. This command is enabled only if a non-default VRF instance has been specified.

Examples

This example enables BGP4 route redistribution.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# bgp-redistribute-internal
```

This example enables BGP4+ route redistribution for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# bgp-redistribute-internal
```

bmc

Enters the BMC configuration mode from where all BMC related commands are executed.

Syntax

bmc

no bmc

Parameters

None

Modes

Global Configuration Mode

Usage Guidelines

The **no** format of this command does the following actions:

1. Deletes the complete BMC interface. SLX-OS sets the default value for the BMC interface as *192.168.11.1/24* and its gateway as *0.0.0.0*.
2. Deletes all BMC user configurations.
3. Shuts down the BMC interface (SoHo Port).

Examples

This example shows how to enter into the BMC mode for further configuration of the BMC parameters.

```
SLX # configure terminal
SLX (config)# bmc ?
<CR>
SLX (config)# bmc
SLX (config-bmc)# ?
Possible completions:
  describe    Display transparent command information
  do          Run an operational-mode command
  exit        Exit from current mode
  help        Provide help information
  interface   BMC network configuration
  no          Negate a command or set its defaults
  pwd         Display current mode path
  top         Exit to top level and optionally run command
  user-id     BMC users configuration
SLX (config-bmc)#
```

This example shows the usage of the **no bmc** command to reset the BMC parameters.

```
SLX (config-bmc)# exit
SLX (config)# no bmc
```

bmc factory reset

Resets the BMC configuration to the factory default settings.

Syntax

bmc factory reset

Parameters

reset

Resets the existing BMC configuration to its default configuration. Use `y` to reset the configuration. Use `n` to exit without changing the configuration.

Modes

Privileged EXEC Mode

Usage Guidelines

This CLI resets the BMC configurations to the factory settings including user accounts, LAN, and field replaceable unit (FRU) sensor settings.

Since the sensor data are reset, you must use the SLX-OS **reload** command to reboot the device for these changes to take effect.

Examples

The following examples resets the BMC configuration to its default settings. A reboot of the device is also shown.

```
SLX# bmc factory reset
SLXOS needs to be restarted for normal operations, after bmc factory reset.
Do you want to continue? (y/n): y
SLX# reload
SLX#
```

bpdu-drop-enable

Enables dropping Layer 2 (L2) bridge protocol data units (BPDUs) on endpoints in L2 interfaces.

Syntax

bpdu-drop-enable

no bpdu-drop-enable

Command Default

Dropping of L2 BPDUs is disabled. L2 BPDUs are allowed on endpoints in L2 interfaces.

Modes

Global Configuration Mode

Physical Interface Configuration Mode

Port-Channel Interface Configuration Mode

Usage Guidelines

The **no** form of the command disables dropping of Layer 2 (L2) bridge protocol data units (BPDUs) in Layer 2 interfaces.

Examples

The following example shows how to enable dropping of L2 BPDUs for all L2 Interfaces.

```
device# configure terminal
device(config)# bpdu-drop-enable
```

The following example shows how to enable dropping of L2 BPDUs for L2 Physical Interface.

```
device# configure terminal
device(config)# interface Ethernet 0/40
device(conf-if-eth-0/40)# bpdu-drop-enable
```

The following example shows how to enable dropping of L2 BPDUs for L2 Port-Channel Interface.

```
device# configure terminal
device(config)# interface Port-channel 30
device(conf-Port-channel-30)# bpdu-drop-enable
```

breakout mode

Configures breakout mode for the supported connectors.

Syntax

breakout mode { **4x10g** | **4x25g** | **4x1g** }

no breakout

Command Default

By default, breakout mode is not configured.

Parameters

4x10g

Configures four 10g breakout interfaces on a port.

4x25g

Configures four 25g breakout interfaces on a port.

4x1g

(SLX 9250 only) Configures four 1g breakout interfaces on a port.

Modes

Hardware connector configuration mode

Usage Guidelines

You do not need to reboot a device for the breakout configuration change to take effect.

When you configure a breakout mode on an Ethernet port, the original interface is de-configured and deleted. The new breakout interfaces in the default configuration are created automatically. These new interfaces are identified with the name of the original interface followed by a suffix. For example, the breakout interfaces of connector 0/25 have the following naming convention:

```
interface ethernet 0/25:1
interface ethernet 0/25:2
interface ethernet 0/25:3
interface ethernet 0/25:4
```

Use the **no** form of the command to reset the port to non-breakout mode. When you run the no form of the command, the breakout interfaces are de-configured and deleted. The original Ethernet interface in the default configuration is created automatically.

To switch from one breakout mode to another, set the port to non-breakout mode and then run the command to configure the new breakout mode.

(SLX 9250) This platform supports only the 4x1g breakout mode, which supports the redundant management interface feature. This feature is used with Mellanox network adapters and 1GB copper SFPs.

(SLX 9150, SLX 9540, SLX 9640, and Extreme 8520) These platforms support the 4x10g and 4x25g breakout modes. The number of connectors and connector IDs that support the breakout function varies by platform. For more information, see the *Technical Specifications* guide for your platform.

(Extreme 8720) This platform supports the 4x10g and 4x25g breakout modes on all ports.

(SLX 9740/Extreme 8820) These platforms have breakout restrictions related to port macros (PM). A PM is a port group. Each PM has four ports, which are contiguous. PM0 has ports 0/1 – 0/4, PM1 has ports 0/5 – 0/8, PM2 has ports 0/9 – 0/12, and so on. In any PM, 40g and 10g ports cannot coexist with 25g ports. The following configurations are not supported.

- If any port in a PM is configured as 40g or 4x10g breakout, no 4x25g breakout is allowed in the PM unless the 40g ports will be removed as part of the breakout operation. For example:
  - If 0/1 or 0/2 is 40g, you cannot configure 0/3 as 4x25g breakout.
  - If 0/1 or 0/2 is 40g, you can configure 0/1 as 4x25g breakout because 0/1 and 0/2 will be removed.
- If 4x25g breakout is configured in a PM, no 40g or 4x10g is allowed in the PM. For example:
  - If 0/1 is configured as 4x25g breakout, you cannot configure 0/3 or 0/4 as 40g.
  - If 0/3 is configured as 4x25g breakout, you cannot configure 0/1 as 4x10g breakout.
- Breakout is allowed only on odd ports. Breakout is not allowed on the following ports:
  - 0/5, 0/7 - on SLX 9740-40C/Extreme 8820-40C devices
  - 0/5, 0/7, 0/45, 0/47 - on SLX 9740-80C/Extreme 8820-80C devices
- Only 100G is allowed on the following ports:
  - 0/5, 0/6, 0/7, 0/8 - on SLX 9740-40C/Extreme 8820-40C devices
  - 0/5, 0/6, 0/7, 0/8, 0/45, 0/46, 0/47, 0/48 - on SLX 9740-80C/Extreme 8820-80C devices

Examples

This example configures 4x25g breakout mode on connector 0/25 on SLX 9640.

```
device(config)# hardware
device(config-hardware)# connector 0/25
device(config-connector-0/25)# breakout mode 4x25g
```

This example reverts a port to non-breakout mode on SLX 9640.

```
device(config)# hardware
device(config-hardware)# connector 0/25
device(config-connector-0/25)# no breakout
```

This example configures 4x10g breakout mode on connector 0/25 on SLX 9640.

```
device(config)# hardware
device(config-hardware)# connector 0/25
device(config-connector-0/25)# breakout mode 4x10g
```

This example configures 4x1g breakout mode on connector 0/15 on SLX 9250.

```
device(config)# hardware
device(config-hardware)# connector 0/21
device(config-connector-0/15)# breakout mode 4x1g
```

bridge-domain

Creates a bridge domain, which represents a switching or inter-connection domain for a wide range of service end-point types.

Syntax

bridge-domain *bd-id* [**p2mp** | **p2p**]

no bridge-domain *bd-id* [**p2mp** | **p2p**]

Command Default

No bridge domain is configured.

Parameters

bd-id

Specifies a unique numeric bridge-domain identifier. For supported values, see the Usage Guidelines.

p2mp

Specifies a multipoint service type. This is the default service type.

p2p

Specifies a point-to-point cross-connect service type.

Modes

Global configuration mode.

Usage Guidelines

The range of supported bridge-domain ID values varies with device:

- For Extreme 8720, Extreme 8520, SLX 9250, and SLX 9150 devices - From 1 through 1024.
- For Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices - From 1 through 4096.

(For Extreme 8820, SLX 9740, SLX 9640, and SLX 9540) VPLS performs any-to-any switching between Ethernet attachment circuits (ACs) and MPLS pseudowires (PWs). VLL performs one-to-one switching between Ethernet AC and MPLS PWs. Use the bridge-domain to specify the related configuration for both VPLS and VLL.

The **no** version of this command removes the bridge-domain configuration.

Examples

The following example shows how to configure bridge domain 1 and specifies a point-to-point cross-connect service for the domain.

```
device# configure terminal
device(config)# bridge-domain 1 p2p
```

The following example shows the error message that is displayed when the specified bridge-domain ID is out of range.

```
device# configure terminal
device(config)# bridge-domain 10000000
Error: syntax error: "10000000" is out of range.
```

The following example shows the error message that is displayed when the bridge-domain creation is not successful in the back-end.

```
device# configure terminal
device(config)# bridge-domain 110
Error: bridge-domain: connection instance creation failed.
```

bridge-domain (EVPN)

Specifies a bridge domain (BD), or adds or removes a range VLANs from the BD, for an Ethernet Virtual Private Network (EVPN) instance.

Syntax

bridge-domain *BD-ID*

no bridge-domain *BD-ID*

bridge-domain { **add** | **remove** } {*VLAN-range* }

Command Default

Disabled

Parameters

BD-ID

Specifies a BD.

add

Adds a range of VLANs to the BD for default EVPN instance.

remove

Removes a range of VLANs from the BD for the default EVPN instance.

VLAN-range

Specifies a hyphen-delimited VLAN range to be added to or removed from BD for the EVPN instance.

Modes

EVPN configuration mode

Usage Guidelines

Each VLAN/BD added to an EVPN configuration is considered as an EVPN instance and is assigned a unique EVPN instance ID (EVI) internally. The EVI is calculated as shown in the following table.

When adding a bridge domain, use the **clear bgp evpn neighbor all soft in** command for the change to take effect.

Table 6: Calculating EVI values from VLAN/BD values

VLAN/BD	EVI value
VLAN: 1–4096	VLAN ID
BD: 1–4096	BD ID + 4096

Important
To interoperate with third-party vendors, the RTs across the interoperating devices must be the same. If third-party devices do not support automatic RT assigment, or the EVIs are not calculated as shown in the above table, the VLAN/BD instances must be configured manually to ensure that RTs across the devices are compatible.

Examples

To specify a BD and enter EVPN BD configuration mode:

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# bridge-domain 100
device(evpn-bridge-domain-100)#
```

To add BDs 100 through 200 to the default EVPN instance:

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# bridge-domain add 100-200
device(config-evpn-default)#
```

To remove BDs 150 through 180 from the default EVPN instance:

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# bridge-domain remove 150-180
device(config-evpn-default)#
```

bridge-priority

Specifies the bridge priority for the common instance.

Syntax

bridge-priority *priority*

no bridge-priority

Command Default

The default priority is 32768.

Parameters

priority

Specifies the bridge priority. Valid values range from 0 through 61440 in increments of 4096.

Modes

Protocol Spanning Tree mode

Usage Guidelines

The priority values can be set only in increments of 4096.

Using a lower priority value indicates that the bridge might become root.

Enter **no bridge-priority** to return to the default priority.

Examples

To specify the bridge priority:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# bridge-priority 8192

device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# bridge-priority 8192

device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# bridge-priority 8192
```

bsr-candidate

Configures a bootstrap router (BSR) as a candidate to distribute rendezvous point (RP) information to the other PIM-SM (Sparse Mode) devices in a PIM-SM domain.

Syntax

bsr-candidate interface {*ethernet* | *loopback* | *port-channel* | *ve* } *num*
mask *length* [**priority** *value*]

no bsr-candidate

Command Default

By default, the PIM router is not part of the BSR election process.

Parameters

ethernet *num*

Specifies the Ethernet interface for the candidate BSR.

loopback *num*

Specifies the loopback interface for the candidate BSR.

ve *num*

Specifies the virtual interface for the candidate BSR.

port-channel *num*

Specifies the port-channel number for the candidate BSR.

mask

Specifies the mask for the candidate BSR.
length

Specifies the hash mask length. Valid values range from 1-32 for IPv4 PIM.

priority *value*

Specifies the BSR priority. Valid values range from 0-255.

Modes

PIM Router configuration mode

Usage Guidelines

Each PIM-SM domain has one active BSR. For redundancy, you can configure ports on multiple devices as candidate BSRs. PIM-SM uses an election process to select one of the candidate BSRs as the BSR for the domain. The BSR with the highest BSR priority is elected. If the priorities result in a tie, the candidate BSR interface with the highest IP address is elected.

Although you can configure the device as only a candidate BSR or an RP, a best practice is to configure the same interface on the same device as both a BSR and an RP.

The **no bsr-candidate** form of this command makes the PIM router cease to act as a candidate BSR.

Examples

The following example configures a physical interface as a candidate BSR.

```
device(config)# router pim
device(config-pim-router)# bsr-candidate ethernet 2/2 30 255
```

The following example configures a loopback interface as a candidate BSR.

```
device(config)# router pim
device(config-pim-router)# bsr-candidate interface loopback 11 mask 32
```

The following example configures a virtual interface as a candidate BSR.

```
device(config)# router pim
device(config-pim-router)# bsr-candidate ve 120 30 250
```

The following example configures an IPv6 virtual interface as a candidate BSR.

```
device(config)# ipv6 router pim
device(config-ipv6-router-pim-vrf-default-vrf)# bsr-candidate interface ve 30 mask 126
priority 10
```

The following example configures an IPv6 physical interface as a candidate BSR.

```
device(config)# ipv6 router pim
device(config-ipv6-router-pim-vrf-default-vrf)# bsr-candidate interface ethernet 2/2 mask
64
```

The following example configures an IPv6 loopback interface as a candidate BSR.

```
device(config)# ipv6 router pim
device(config-ipv6-router-pim-vrf-default-vrf)# bsr-candidate interface loopback 11 mask
96 priority 20
```

bypass-lsp

Creates a bypass LSP by using the **bypass-lsp** command. Thereafter, in the bypass LSP context, you must specify at least one interface as an excluded or protected interface.

Syntax

bypass-lsp *name*

no bypass-lsp *name*

Parameters

name

Specifies the name of the target LSP.

Modes

MPLS router configuration mode

Usage Guidelines

The *name* variable must be unique among all regular LSPs and bypass LSPs.

The **no** form of the command deletes the bypass LSP from the system.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example selects the *xm4-by* LSP as a bypass LSP.

```
device>configure
device(config)# router mpls
device(config-router-mpls)# bypass-lsp xm4-by
device(config-router-mpls-bypasslsp-xm4-by)#
```

bypass-lsp (Telemetry)

Indicates the MPLS Bypass-LSP to be used for the mpls-traffic-bypass profile.

Syntax

bypass-lsp { *bypass-lsp-name* }

no bypass-lsp { *bypass-lsp-name* }

Parameters

bypass-lsp-name

Specifies the name of the target LSP for the profile.

Modes

Telemetry profile configuration mode

Usage Guidelines

The *bypass-lsp-name* variable must be unique among all regular LSPs and bypass LSPs.

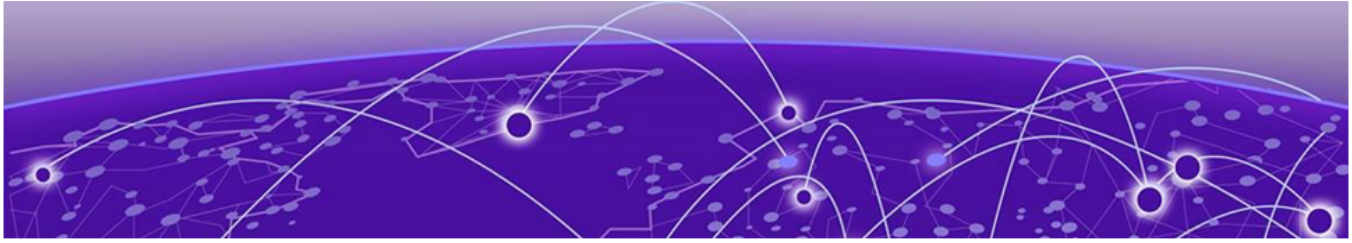
The **no** form of the command deletes the bypass LSP from the profile.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example selects the *xm2by* LSP as the bypass LSP for the profile.

```
device(config)# telemetry profile mpls-traffic-bypass
default_mpls_traffic_bypass_statistics
device(config-telemetry-profile)# bypass-lsp xm2by
```



Commands C - D

capability as4-enable on page 210
ccm-interval on page 211
cee-map on page 212
certutil import sshkey on page 213
certutil sshkey on page 215
certutil sshx509v3 on page 217
cfm linktrace on page 219
cfm loopback on page 221
cfm y1731 domain on page 223
channel-group on page 224
chassis on page 227
cipherset on page 228
cisco-interoperability on page 230
class on page 231
class-map on page 233
clear arp on page 234
clear bfd neighbors on page 235
clear bgp evpn l2routes on page 236
clear bgp evpn local routes on page 237
clear bgp evpn neighbor on page 238
clear bgp evpn neighbor dynamic all on page 240
clear bgp evpn routes on page 241
clear bgp ip flowspec local on page 243
clear bgp ip flowspec neighbor on page 244
clear bgp ip flowspec routes on page 246
clear bgp ip neighbor ipv6 on page 247
clear cfm y1731 client-signal-fail statistics on page 249
clear cfm y1731 statistics on page 250
clear cfm y1731 statistics delay-measurement on page 251
clear cfm y1731 statistics synthetic-loss-measurement on page 252
clear counters on page 253
clear counters access-list on page 254
clear counters access-list overlay type vxlan on page 257
clear counters storm-control on page 258

clear dot1x statistics on page 260
clear erp statistics on page 261
clear erp wtb-time on page 262
clear erp wtr-time on page 263
clear filter-change-update on page 264
clear ip arp inspection statistics on page 265
clear ip arp suppression-cache on page 266
clear ip arp suppression-statistics on page 267
clear ip bgp dampening on page 268
clear ip bgp flap-statistics on page 269
clear ip bgp local routes on page 270
clear ip bgp neighbor on page 271
clear ip bgp neighbor dynamic on page 273
clear ip bgp routes on page 274
clear ip bgp rpki server on page 275
clear ip bgp traffic on page 276
clear ip dhcp relay statistics on page 277
clear ip dhcp snooping binding on page 278
clear ip flowspec rules statistics on page 279
clear ip igmp groups on page 280
clear ip igmp statistics on page 281
clear ip multicast snooping mcache on page 282
clear ip pim mdt on page 283
clear ip ospf on page 284
clear ip route on page 286
clear ipv6 bgp dampening on page 287
clear ipv6 bgp flap-statistics on page 288
clear ipv6 bgp local routes on page 289
clear ipv6 bgp neighbor on page 290
clear ipv6 bgp neighbor dynamic on page 292
clear ipv6 bgp routes on page 293
clear ipv6 bgp traffic on page 294
clear ipv6 counters on page 295
clear ipv6 dhcp relay delegated-prefixes on page 296
clear ipv6 dhcp relay statistics on page 298
clear ipv6 mld groups on page 299
clear ipv6 mld snooping on page 301
clear ipv6 mld statistics on page 302
clear ipv6 multicast snooping mcache on page 303
clear ipv6 nd suppression-cache on page 304
clear ipv6 nd suppression-statistics on page 305
clear ipv6 neighbor on page 306

clear ipv6 ospf on page 307
clear ipv6 pim mcache on page 309
clear ipv6 pim rp-map on page 310
clear ipv6 pim traffic on page 311
clear ipv6 route on page 312
clear ipv6 vrrp statistics on page 313
clear isis all on page 315
clear isis counts on page 316
clear isis database on page 317
clear isis force-spf on page 318
clear isis force-v6spf on page 319
clear isis ipv6 spf-log on page 320
clear isis neighbor on page 321
clear isis route on page 322
clear isis spf-log on page 323
clear isis traffic on page 324
clear lacp on page 325
clear lacp counters on page 326
clear link-oam statistics on page 327
clear lldp neighbors on page 328
clear lldp statistics on page 330
clear logging raslog on page 332
clear loop-detection on page 334
clear loop-detection bridge-domain on page 335
clear mac-address-table on page 336
clear mpls auto-bandwidth-samples on page 338
clear mpls lsp on page 339
clear mpls statistics on page 340
clear mvrp statistics on page 342
clear overlay-gateway on page 343
clear policy-map-counters on page 344
clear qos flowcontrol statistics on page 345
clear spanning-tree counter on page 346
clear spanning-tree detected-protocols on page 347
clear statistics bridge-domain on page 348
clear statistics vlan on page 349
clear tm voq-stat ingress-device on page 350
clear tm voq-stat slot on page 351
clear tunnel statistics on page 352
clear udld statistics on page 353
clear vrrp statistics on page 354
CLI on page 356

client on page 359
client-interface on page 360
client-interface (Y1731) on page 361
client-interfaces-shutdown on page 363
client-pw on page 364
client-to-client-reflection on page 365
clock set on page 367
clock timezone on page 368
cluster on page 369
cluster-client auto on page 370
cluster-track on page 372
commit on page 374
compare-med-empty-aspath on page 375
compare-routerid on page 376
confederation identifier on page 377
confederation peers on page 378
configure terminal on page 379
config-drift-track on page 380
connector on page 381
control-word on page 382
console on page 384
copy on page 386
core-isolation-disable on page 389
core-isolation-track on page 390
cos (MPLS) on page 392
cos (Y1731) on page 394
convergence-time on page 395
crypto ca authenticate on page 396
crypto ca enroll on page 398
crypto ca import on page 400
crypto ca import-pkcs on page 402
crypto ca trustpoint on page 405
crypto cert expiry-level on page 406
crypto import on page 408
crypto key on page 410
csnp-interval on page 412
cspf-computation-mode on page 413
cspf-interface-constraint on page 415
cspf-group on page 416
cspf-group-computation on page 417
dampening on page 419
database-overflow-interval (OSPFv2) on page 421

database-overflow-interval (OSPFv3) on page 423
debug access-list-log buffer on page 425
debug arp packet buffer on page 426
debug dhcp packet buffer on page 428
debug dot1x packet on page 430
debug ip bgp on page 432
debug ip bgp neighbor on page 435
debug ip igmp on page 437
debug ip ospf shortcuts on page 439
debug ip pim on page 440
debug ipv6 bgp on page 442
debug ipv6 bgp neighbor on page 444
debug ipv6 dhcp pd on page 446
debug ipv6 mld on page 447
debug ipv6 ospf graceful-restart on page 449
debug ipv6 pim on page 450
debug lacp on page 452
debug lldp dump on page 454
debug lldp packet on page 455
debug spanning-tree on page 457
debug udld packet on page 459
default-information-originate (BGP) on page 461
default-information-originate (IS-IS) on page 462
default-information-originate (OSPFv2) on page 463
default-information-originate (OSPFv3) on page 465
default-ipv6-gateway on page 467
default-link-metric on page 469
default-local-preference on page 471
default-metric (BGP) on page 472
default-metric (IS-IS) on page 473
default-metric (OSPF) on page 474
default-passive-interface on page 475
delay on page 476
delay-link-event on page 477
delete on page 479
delete-packet on page 480
deploy on page 482
description (BD) on page 484
description (event-handler) on page 485
description (interfaces) on page 486
description (LLDP) on page 487
description (STP) on page 488

description (VRRP) on page 489
designated-forwarder-hold-time on page 490
destination on page 491
dhcp ztp cancel on page 492
dhcp ztp log on page 493
dir on page 495
default-metric (IS-IS) on page 496
disable-adjacency-check on page 497
disable-incremental-spf-opt on page 498
disable-inc-stct-spf-opt on page 499
disable-partial-spf-opt on page 500
disallow-oar-ac on page 501
discard-packet on page 502
discard-voq-packet on page 504
distance (BGP) on page 506
distance (IS-IS) on page 507
distance (OSPF) on page 508
distribute on page 510
distribute-list prefix-list (OSPFv3) on page 511
distribute-list route-map on page 512
domain-name on page 513
dot1ag-compliance on page 514
dot1x authentication on page 515
dot1x enable on page 516
dot1x filter-strict-security on page 517
dot1x max-req on page 519
dot1x port-control on page 520
dot1x quiet-period on page 522
dot1x reauthenticate on page 523
dot1x reauthentication on page 524
dot1x reauthMax on page 525
dot1x test eapol-capable on page 526
dot1x test timeout on page 527
dot1x timeout on page 528
dpod on page 530
dscp (QoS) on page 532
dscp (Tunnel) on page 534
dscp-ttl-mode on page 535
duplicate-mac-timer (EVPN default instance) on page 536
dynamic-bypass on page 537

capability as4-enable

Enables 4-byte autonomous system number (ASN) capability at the BGP global level.

Syntax

capability as4-enable

no capability

Command Default

This feature is disabled.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to disable this functionality.

Examples

The following example enables 4-byte ASN capability.

```
device#configure terminal
device(config)# router bgp
device(config-bgp-router)# capability as4-enable
```

ccm-interval

Sets the time interval between two successive Continuity Check Messages (CCMs) that are sent by Maintenance End Points (MEP) in the specified Maintenance Association (MA).

Syntax

ccm-interval [1-second | 10-second | 3.3-ms | 10-ms | 100-ms]

Parameters

1-second

Sets the time interval between two successive CCM packets to 1 second.

10-second

Sets the time interval between two successive CCM packets to 10 seconds.

3.3-ms

Ssets the time interval between two successive CCM packets to 3.3 milliseconds.

10-ms

Sets the time interval between two successive CCM packets to 10 milliseconds.

100-ms

Sets the time interval between two successive CCM packets to 100 milliseconds.

Modes

CFM protocol configuration mode

Usage Guidelines

The default value is 10 seconds.

Examples

```
device# configure terminal
device(config)# protocol cfm
device(config-cfm)# domain name md1 level 4
device(config-cfm-md-md1)# ma-name ma1 id 1 vlan-id 30 priority 4
device(config-cfm-md-ma-ma1)#ccm-interval 10-second
```

cee-map

Converged Enhanced Ethernet (CEE) enables you to configure the ETS/CEE parameters including mapping of incoming priorities (traffic with different CoS) to traffic-classes, assigning weights and corresponding bandwidths to those priorities, and scheduling of all occupied traffic-class traffic to egress wire.

Syntax

cee-map *<cee map name>*

Parameters

<cee map name>

Sets the name of the CEE policy being created.

Modes

Priv EXEC Mode

Usage Guidelines

You can define only one CEE map and the name that must be assigned to this policy should always be *default*. All other names will result in an error. Attempts to create more than one CEE map will also result in an error.

Examples

```
device# configure terminal
device(config)# cee-map default
device(config-cee-map-default)#
```

certutil import sshkey

Imports an SSH public key for a local SSH user from a remote host using the login credentials and path name.

Syntax

certutil import sshkey directory *ssh_public_key_path* **file** *file-name* **host** *remote_ip_address* **login** *login_id* **password** *password* **source-ip** *source-ip* **user** *user_acct*

Parameters

directory *path*

Specifies the path to the certificate on the remote host.

file *filename*

Specifies the SSH public key with a .pub extension.

host *remote_ip*

Specifies the IP address of the remote host.

login *login_id*

Specifies the login name in the remote host.

password *password*

Specifies the password to access the remote host.

source-ip *source-ip*

(SCP only) Specifies the source IP address to use in the header.

user *user_acct*

Specifies a local user name.

Modes

Privileged EXEC mode

Usage Guidelines

When using the **password** parameter with special characters (such as #$@`) use single or double-quotes around the password. Alternatively, precede the special characters by a backslash (\) character.

To delete a public key for a specific user, use to the **no cerutil sshkey** command.

Examples

The following example shows how to import an SSH public key for an SSH user named admin from a remote host (10.70.4.106). The command specifies the SSH public key directory on the remote host as well as login credentials to the remote host.

```
device# certutil import sshkey user admin host 10.70.4.106 directory /users/home40/
bmeenaks/.ssh file id_rsa.pub login fvt password pass1
```

The following example demonstrates the use of special characters in a password.

```
device# certutil import ssh host 192.168.10.10 dir /home/brcd1/.ssh file id_rsa.pub user
admin login brcd1 pass Abcde\! login brcd1 pass "Abcde!"
```

certutil sshkey

Enters an SSH public key for a specific user by using the command line interface (CLI).

Syntax

certutil sshkey user *user-acct* **pubkey** *public-key*

no certutil sshkey user *user-acct*

Parameters

user *user-acct*

Specifies a user name. The user must be a pre-existing user on the device. By default there are two users: “admin” and “user”.

pubkey *public-key*

Specifies a public key.

Modes

Privileged EXEC mode

Usage Guidelines

After an SSH public key is configured, the SSH server restarts on all VRF instances and all existing SSH connections are disconnected.

The user for whom a public key is to be configured by using the **certutil sshkey** command must already be configured on the device. By default, two users (admin and user) are configured on the device. Additional users are configured by using the **username** command in global configuration mode.

The public key must be entered within double quotes (" ").

To generate a public key, run the **ssh-keygen -t rsa** command on any server from which you want to start an SSH session to the device. Once you run this command, and have not entered any other path while generating the key, the public key is generated at /root/.ssh/id_rsa.pub by default. Open this file and copy all its contents after the **pubkey** option in the CLI.

The **no** form of the command removes the public key configuration for the specified user.

Examples

The following example shows how to enter an SSH public key directly into the CLI under the username admin.

```
device# certutil sshkey user admin pubkey “ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDnim+Ofjx/id3z2jDxXu9DcMuQqVq/
NKi2Lms+q7dA5Dqww8jlrOGawG8tMySOvnB1ZEvJt1kqNneRi4l6Ot4/7hfd99rIOPGBP/
NJs6xTLUrQhDgxB78ddTg+6euBtkYLTAaTC7kbXGXcO8VVB9+4xrH+0bkvjU9RRvGJguUfdiFKEfIGVOyt0atdHi1d
mgQ9BE0cO65nc/i9MjMJedBe174/QT4TxeGeEgaQ57c2AL5It2V4CzrZBDtnixdnHUO5w2vmBR61LZIDVT1fuX/
xYxDAm9H8SDpDX8pZlfFpQBy/wrkIYPZ/p4OLrUApB/XAJGujrlNlZLEu9U9MPVM/ root@ldap.hc-fusion.in”
```

certutil sshx509v3

Configures the SSH user certificate Distinguished Name (DN).

Syntax

certutil sshx509v3 { **user** *user-name* **DN** *DN-attributes* }

no certutil sshx509v3 { **user** *user-name* }

Command Default

By default, a DN is not configured.

Parameters

user *user-name*

Specifies the user name associated with the DN.

DN *DN-attributes*

Specifies the attributes of the DN, which can include any of the following:

- SERIALNUMBER: Certificate serial number
- emailAddress: Email address
- UID, USERID: User ID
- CN: Common name
- T: Title
- OU: Organizational Unit
- DC: Domain component
- O: Organization
- STREET: Street or street address
- L: Locality
- ST, SP, S: State or Province
- PC: Postal or zip code
- C: Country

Modes

Privileged EXEC mode

Usage Guidelines

Use the **no** form of the command to remove the DN.

Examples

This following is a typical example.

```
device# certutil sshx509v3 user user1 DN “C=US, ST=California, L=SJC,
O=ExtrNet Inc, OU=DCIP EMIS, CN=user1/emailAddress=myname@mycompany.com”
```

cfm linktrace

Transmits a linktrace message to a Maintenance End Point (MEP) in the domain

Syntax

cfm linktrace { **domain** *name* | **ma** *ma-name* | **src-mep** *mep-id* { **target-mip** *HH:HH:HH:HH:HH:HH* | **target-mep** *mep-id* }| **timeout** *time* | **ttl** *ttl-value*

Parameters

domain *name*

Specifies the maintenance domain to be used for a linktrace message. The name attribute is case-sensitive.

ma *ma-name*

Specifies the maintenance association to be used for a linktrace message. The ma-name attribute is case-sensitive.

src-mep *mep-id*

Specifies the Source ID. The range of valid values is from 1 through 8192.

target-mip *HH:HH:HH:HH:HH:HH*

Specifies the MAC address of the MIP linktrace destination.

target-mep *mep-id*

Specifies the destination ID. The range of valid values is from 1 through 8192.

ttl *ttl-value*

specifies the initial TTL field value. The range of valid values is from 1 through 64.

timeout *time*

Specifies the timeout used to wait for linktrace reply in seconds.

Modes

Privileged EXEC mode .

Usage Guidelines

The **cfm linktrace** command sends a trace message to a specified MEP in the domain to diagnose the path of the MEP link.

Examples

The following example transmits a successful trace from MEP 21 to MEP 1.

```
device# cfm linktrace domain md1 ma ma1 src-mep 21 target-mep 1 timeout 10

Linktrace to 000c.dbfb.5378 on Domain md1, level 4: timeout 10ms, 4 hops
------------------------------------------------------------------
Hops            MAC         Ingress     Ingress Action     Relay Action
```

```
Forwarded         Egress     Egress Action     Nexthop
-------------------------------------------------------------
1         000c.dbe2.6ea0                         RLY_FDB
Forwarded         5/4         EgrOK
2         000c.dbfb.5378     7/2         IgrOK         RLY_HIT
Not Forwarded
Destination 000c.dbfb.5378 reached
```

cfm loopback

Transmits a loopback message to a specific Maintenance End Point (MEP) or Maintenance Intermediate Point (MIP) in a specified domain.

Syntax

cfm loopback { **domain** *name* | **ma** *ma-name* | **src-mep** *mep-id* { **target-mip** *HH:HH:HH:HH:HH:HH* | **target-mep** *mep-id* }| **number** *value* | **timeout** *time*

Parameters

domain *name*

Specifies the maintenance domain to be used for a loopback message. The name attribute is case sensitive.

ma *ma-name*

Specifies the maintenance association to be used for a loopback message. The ma-name attribute is case-sensitive.

src-mep *mep-id*

Specifies the Source ID. The range of valid values is from 1 through 8192.

target-mip *HH:HH:HH:HH:HH:HH*

Specifies the MAC address of the MIP loopback destination.

target-mep *mep-id*

Specifies the destination ID. The range of valid values is from 1 through 8192.

number *value*

Specifies the number of loopback messages to be sent.

timeout *time*

Specifies the timeout used to wait for loopback reply in seconds.

Modes

Privileged EXEC mode

Usage Guidelines

The cfm loopback command sends a loopback message to a specific MEP or MIP in a specified domain for testing purposes.

Examples

Command example sending a message from MEP 2 to MEP 1 a total of ten times.

```
device# cfm loopback domain md1 ma ma1 src-mep 2 target-mep 1 timeout 10 number 10

cfm: Sending 10 Loopback to 000c.dbfb.5378, timeout 10 msec
Type Control-c to abort
```

```
Reply from 000c.dbfb.5378: time=1ms
Reply from 000c.dbfb.5378: time<1ms
Reply from 000c.dbfb.5378: time<1ms
Reply from 000c.dbfb.5378: time<1ms
Reply from 000c.dbfb.5378: time<1ms
Reply from 000c.dbfb.5378: time<1ms
Reply from 000c.dbfb.5378: time<1ms
Reply from 000c.dbfb.5378: time<1ms
Reply from 000c.dbfb.5378: time<1ms
A total of 10 loopback replies received.
Success rate is 100 percent (10/10), round-trip min/avg/max=0/0/1 ms.
```

cfm y1731 domain

Sets the on-demand two-way delay measurement or two-way synthetic loss measurement parameters.

Syntax

cfm y1731 domain *domain-name* **ma** *ma-name* **src-mep** *mep-id* **target-mep** *mep-id* **test-profile** *profile-name*

Parameters:

domain-name

Specifies the domain name.

ma

Specifies the maintenance association (MA).

ma-name

Specifies the MA name.

src-mep *mep-id*

Specifies the source mep-id.

target *mep-id*

Specifies the taraget mep-id.

profile

Specifies the default or configured test profile.

profile-name

Specifies the profile name.

Modes

Privilieged EXEC mode

Examples

This example shows how to run on-demand two-way delay measurement or two-way synthetic loss measurement parameters.

```
device# cfm y1731 domain md1 ma ma1 src-mep 1 target-mep 2 test-profile
2dm_default_profile
device# cfm y1731 domain md1 ma ma1 src-mep 1 target-mep 2 test-profile
2slm_default_profile
```

channel-group

Enables link aggregation on an interface.

Syntax

channel-group *number* **mode** { **active** | **passive** | **on** } [**type standard**]

no channel-group

Command Default

The value for **type** is set to **standard** .

Parameters

number

Specifies the port-channel to which you are assigning the interface.

mode

Specifies the mode of Link Aggregation.

active

Enables the initiation of LACP negotiation on an interface.

passive

Disables LACP on an interface.

on

Enables static link aggregation on an interface.

type standard

Specifies the 802.3ad standard-based LAG.

Modes

Interface subtype configuration mode

Usage Guidelines

Port channel scale and support for SLX 9740 and Extreme 8820 devices:

Table 7: Port-channel scale for SLX 9740/Extreme 8820 devices.

Device	LAG Profile	Supported port-channel IDs	Maximum links per port-channel
SLX 9740-40/ Extreme 8820-40	default	1-256; Only 77 portchannels may be created at any one time	64
SLX 9740-80/ Extreme 8820-80	default	Only 153 portchannels may be created at any one time.	64

Note

- For the 1U SLX 9740-40/Extreme 8820-40 devices, the number of LAGs will be 77, where:
  - 76 are the front end ports (all breakouts)
  - 1 (insight port)
- For the 2U SLX 9740-80/Extreme 8820-80 devices, the number of LAGs will be 153. where:
  - 152 are the front end ports (all breakouts)
  - 1 (insight port)

(For SLX 9540 and SLX 9640) Maximum numbers of port-channel IDs and links per port-channel vary with device and LAG profile, as follows:

Table 8: Port-channel scale for SLX 9540 and SLX 9640 devices

Device or series	LAG profile	Supported port-channel IDs	Maximum links per port-channel
SLX 9540 SLX 9640	default	1–256; Only 64 port-channels may be created at any one time.	64
SLX 9540, SLX 9640	lag-profile-1	1–256; Only 64 port-channels may be created at any one time.	32

(SLX 9150, SLX 9250, Extreme 8520, and Extreme 8720) Maximum numbers of port-channel IDs and links per port-channel vary only with device, as follows:

Table 9: Port-channel support for SLX 9150, SLX 9250, Extreme 8520, and Extreme 8720 devices

Device or series	Supported port-channel IDs	Maximum links per port-channel
SLX 9150, SLX 9250, Extreme 8520, and Extreme 8720	1–256; Only 128 port-channels may be created at any one time.	64

Note
Non-default LAG profiles are not supported for the SLX 9150, SLX 9250, Extreme 8520, and Extreme 8720 devices.

To remove the interface from a port-channel, enter the **no** form of this command.

Examples

The following example associates interface 0/9 with port-channel 4 and activates LACP.

```
device# configure terminal
device(config)# interface ethernet 0/9
device(conf-if-eth-0/9)# channel-group 4 mode active
```

chassis

Sets the IPv4 or IPv6 address of a device.

Syntax

chassis { **virtual-ip** *IPv4-address* | **virtual-ipv6** *IPv6-address* }

no chassis

Command Default

The default is the initial device address.

Parameters

virtual-ip *IPv4-address*

Sets an IPv4 address in dotted-decimal notation with a CIDR prefix (mask).

virtual-ipv6 *IPv6-address*

Sets an IPv6 address in colon-separated hexadecimal notation with a CIDR prefix.

Modes

Global configuration mode

Usage Guidelines

This command changes the current IPv4 or IPv6 address.

Use this command to change the IP address to facilitate management, for example, if a device is moved to a different subnet. The IP address of the management platform should be in the same subnet as the devices it manages.

Use the **no** form of this command to revert to the default address.

Examples

IPv4:

```
device# configure terminal
device(config)# chassis virtual-ip 10.11.12.13/20
```

IPv6:

```
device# configure terminal
device(config)# chassis virtual-ipv6 2001:db8:8086:6502/64
```

cipherset

Configures FIPS-compliant ciphers for the Lightweight Directory Access Protocol (LDAP).

Syntax

cipherset { **ldap** | **radius** }

Command Default

There are no restrictions on LDAP ciphers.

Parameters

radius

Specifies secure RADIUS ciphers.

ldap

Specifies secure LDAP ciphers.

Modes

Privileged EXEC mode

Usage Guidelines

A device must be configured with secure ciphers for SSH before that device can be FIPS compliant. If LDAP authentication is to be used, the LDAP ciphers are also required before a device can be FIPS compliant.

The secure LDAP ciphers are EAS128-SHA and DES-CBC3-SHA.

This command can be used only from a user account to which an administrative role is assigned.

Note
Use the **ssh client cipher** or the **ssh server cipher** commands to set the SSH client's cipher lists for SSH clients and servers.

Examples

This example configures secure RADIUS ciphers.

```
device# cipherset radius

RADIUS cipher list configured successfully.
RADIUS Cipher List(FIPS 140-2 Approved) : AES256-SHA256 AES256-SHA AES128-SHA256 AES128-
SHA
```

This example configures secure LDAP ciphers.

```
device# cipherset ldap

ldap cipher list configured successfully.
LDAP Cipher List(FIPS 140-2 Approved) : AES256-SHA256 AES256-SHA AES128-SHA256 AES128-SHA
```

cisco-interoperability

Configures the device to interoperate with some legacy Cisco switches.

Syntax

cisco-interoperability { **disable** | **enable** }

Command Default

Cisco interoperability is disabled.

Parameters

disable

Disables Cisco interoperability for the Multiple Spanning Tree Protocol (MSTP) device.

enable

Enables Cisco interoperability for the MSTP enabled device.

Modes

Protocol Spanning Tree MSTP mode

Usage Guidelines

For some devices, the MSTP field, Version 3 Length, does not adhere to the current standards.

If Cisco interoperability is required on any device in the network, then all devices in the network must be compatible, and therefore enabled using this command for interoperability with a Cisco switch.

Examples

To enable Cisco interoperability on a device:

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# cisco-interoperability enable
```

To disable Cisco interoperability on a device:

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# cisco-interoperability disable
```

class

Creates a class map in a policy map and enters the class map configuration mode.

Syntax

class *class-mapname*

no class *class-mapname*

Command Default

A policy map is not created.

Parameters

class-mapname

The designated name for the class map.

Modes

Policy map configuration mode

Usage Guidelines

Use this command to configure a class map for a police policy map with QoS and policing parameters for inbound or outbound traffic. The class map must be previously created and associated with match criteria using the **class-map** command. (Refer to the **qos cos** command.)

When you enter the **class** command and access policy-map class configuration mode, you can configure QoS and policing parameters for the class map using the commands for the specific parameters.

Each policy map can contain one class map.

The **police cir** command is mandatory for configuring a class map.

Enter **no police** while in config-policymap-class mode to remove all policing parameters for the class map.

Enter **no police** command followed by a policing parameter name to remove a specific parameter.

Note
The **cir** is mandatory for configuring a class map. Other parameters are optional. If optional parameters are not set then they will be treated as disabled. To delete the mandatory CIR parameter, you must delete all policer parameters while in the policy map class configuration mode using the **no police** command.

Examples

This example configures a class-map called "default" within a policy-map.

```
device# configure terminal
device(config)# policy-map policymap1
device(config-policymap)# class default
device(config-policymap-class)# police cir 40000
```

class-map

Enters class (classification) map configuration mode.

Syntax

class-map *class-map-name*

no class-map *class-map-name*

Command Default

The class map name "default" is reserved and cannot be created by users.

Parameters

class-map-name

Name of classification map. The map name is restricted to 64 characters.

Modes

Global configuration mode.

Usage Guidelines

Enter **no map class-map** *class-map-name* while in global configuration mode to remove the classification map.

Examples

The following example accesses class map configuration mode for the default class map:

```
device(config)# class-map default
device(config-classmap)#
```

The following example creates a class map, accesses class map configuration mode, and adds a match statement to a VLAN:

```
device(config)# class-map c1
device(config-classmap)# match vlan 500
```

The following example creates a class map, accesses class map configuration mode, and adds a match statement to a bridge domain:

```
device(config)# class-map BD-1000
device(config-classmap)# match bridge-domain 1000
```

clear arp

Clears some or all Address Resolution Protocol (ARP) entries.

Syntax

clear arp [**ethernet** *slot* **/** *port* | **ip** *ip-address* | **ve** *ve-id*] [**no-refresh**] [**vrf** *vrf-name*]

Parameters

ethernet

Specifies a physical Ethernet interface.

slot

Specifies a valid slot number. For devices that do not support line cards, specify **0**.

port

Specifies a valid port number.

ip *ip-address*

Specifies a next-hop IP address.

ve *ve-id*

Specifies a virtual Ethernet (VE) interface.

no-refresh

Clears the ARP cache without resending ARP requests to the local hosts.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

If the **no-refresh** keyword is not included, ARP requests are automatically triggered for the cleared entries. To avoid this triggering, include the **no-refresh** keyword. It is required to include the **no-refresh** keyword, in case the number of ARP entries reaches the system threshold

Examples

The following example clears all ARP entries on the device.

```
device# clear arp
```

clear bfd neighbors

Clears Bidirectional Forwarding Detection (BFD) neighbors.

Syntax

clear bfd neighbors [*ipv4-addr* | *ipv6-addr*]

Parameters

ipv4-addr

Specifies an IPv4 address.

ipv6-addr

Specifies an IPv6 address.

Modes

Privileged EXEC mode

Examples

The following example clears a specified IPv4 BFD neighbor.

```
device# clear bfd neighbors 10.1.1.1
```

The following example clears all BFD neighbor.

```
device# clear bfd neighbors
```

clear bgp evpn l2routes

Clears routes from the BGP EVPN Layer 2 route table.

Syntax

```
clear bgp evpn l2routes type { arp |igmp-join-sync | igmp-leave-sync |
   inclusive-multicast | mac | nd}
```

Parameters

type

Specifies the type of route.

arp

Specifies Address Resolution Protocol routes.

igmp-join-sync

Specifies Join Sync routes.

igmp-leave-sync

Specifies Leave Sync routes.

inclusive-multicast

Specifies inclusive multicast routes.

mac

Specifies MAC routes.

nc

Specifies neighbor discovery routes.

Modes

Privileged EXEC mode

Examples

This example clears all routes from the BGP EVPN route table.

```
device# clear bgp evpn l2routes
```

This example clears all Leave Sync routes from the BGP EVPN route table.

```
device# clear bgp evpn l2 routes type igmp-leave-sync
```

clear bgp evpn local routes

Clears routes from the BGP EVPN local route table.

Syntax

```
show bgp evpn local routestype { arp |igmp-join-sync | igmp-leave-sync |
   ipv4-prefix | ipv6-prefix |mac | nd}
```

Parameters

type

Specifies the type of route.

arp

Specifies Address Resolution Protocol routes.

igmp-join-sync

Specifies Join Sync routes.

igmp-leave-sync

Specifies Leave Sync routes.

ipv4-prefix

Specifies IPv4 routes.

ipv6-prefix

Specifies IPv6 routes.

mac

Specifies MAC routes.

nc

Specifies neighbor discovery routes.

Modes

Privileged EXEC mode

Examples

The following example clears all Leave Sync routes from the BGP EVPN local route table.

```
device# clear bgp evpn local routes type igmp-leave-sync
```

clear bgp evpn neighbor

Requests a dynamic refresh of BGP EVPN connections or routes from a neighbor, with a variety of options.

Syntax

clear bgp evpn neighbor { **all** | *ipv4-addr* | *ipv6-addr* } [**soft** [**in** | **out**]]

clear bgp evpn neighbor { **all** | *ipv4-addr* | *ipv6-addr* } [**soft-outbound**]

Parameters

all

Resets and clears all BGP EVPN connections to all neighbors.

ipv4-addr

Specifies an IPv4 address.

ipv6-addr

Specifies an IPv6 address.

soft

Refreshes routes received from or sent to the neighbor.

in

Refreshes received routes.

out

Refreshes sent routes.

soft-outbound

Refreshes all outbound routes by applying new or changed filters, but sends only the existing routes affected by the new or changed filters to the neighbor.

Note

Use **soft-outbound** only if the outbound policy is changed. This operand updates all outbound routes by applying the new or changed filters. However, the device sends to the neighbor only the existing routes that are affected by the new or changed filters. The **soft out** operand updates all outbound routes and then sends the entire route table on the device to the neighbor after the device changes or excludes the routes affected by the filters.

dynamic all

Clears all dynamic neighbors in the EVPN address family.

Modes

Privileged EXEC mode

Examples

This example refreshes all BGP EVPN neighbor connections.

```
device# clear bgp evpn neighbor all
```

This example clears BGP EVPN connections with a specified IPv6 address.

```
device# clear bgp evpn neighbor 2001::1
```

This example refreshes routes received from a neighbor with the IP address 10.0.0.1.

```
device# clear bgp evpn neighbor 10.0.0.1 soft in
```

clear bgp evpn neighbor dynamic all

Clears all BGP dynamic neighbors in an EVPN address family.

Syntax

clear bgp evpn neighbor dynamic all

Modes

Privileged EXEC mode

Examples

This example clears all dynamic neighbors in an EVPN address family.

```
device# configure terminal
device(config)# clear bgp evpn neighbor dynamic all
```

clear bgp evpn routes

Clears routes from the BGP EVPN route table and resets the routes.

Syntax

clear bgp evpn routes

clear bgp evpn routes type arp *ip address* **mac** *mac address* **ethernet-tag** *tag-id*

clear bgp evpn routes type ipv4-prefix *ip address/mask*

clear bgp evpn routes type ipv6-prefix *ipv6 address/mask*

clear bgp evpn routes type mac *mac address***ethernet-tag** *tag-id*

clear bgp evpn routes type nd *IPv6 address* **mac** *mac address* **ethernet-tag** *tag-id*

clear bgp evpn routes type [**igmp-join-sync**| **igmp-leave-sync**]

Parameters

arp

Specifies address-resolution protocol (ARP) routes.

ip address

Specifies an IP address.

mac *mac address*

Specifies Media Access Control (MAC) routes and a MAC address. The valid format is HHHH.HHHH.HHHH.

ethernet-tag *tag-id*

Specifies an Ethenet tag. Valid values range from 1 through 4294967295.

ipv4-prefix

Specifies IPv4 prefix routes.

IPv4 address/mask

Specifies an IPv4 address and mask.

ipv6-prefix

Specifies IPv6 prefix routes.

IPv6 address/mask

Specifies an IPv6 address and mask.

mac

Specifies MAC routes.

nd

Specifies neighbor-discovery (ND) routes.

igmp-join-sync

Specifies Join Sync routes.

igmp-leave-sync

Specifies Leave Sync routes.

Modes

Privileged EXEC mode

Examples

This example clears all routes from the BGP EVPN route table.

```
device# clear bgp evpn routes
```

This example clears all ARP routes from the BGP EVPN route table.

```
device# clear bgp evpn routes type arp
```

This example clears a specified MAC route from the BGP EVPN route table.

```
device# clear bgp evpn routes type mac 000.abba.baba ethernet-tag 0
```

This example clears all Leave Sync routes from the BGP EVPN route table.

```
device# clear bgp evpn routes type igmp-leave-sync
```

clear bgp ip flowspec local

Removes and re-installs local routes for Border Gateway Protocol flow specification (BGP flowspec).

Syntax

clear bgp ip flowspec local routes vrf *vrf-name*

Parameters

routes

Specifies clearing BGP route information.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example shows how to remove and re-install local routes for BGP flowspec in a VRF named red.

```
device# clear bgp ip flowspec local routes vrf red
```

clear bgp ip flowspec neighbor

Removes and re-installs Border Gateway Protocol flow specification (BGP flowspec) information for BGP neighbors.

Syntax

clear bgp ip flowspec neighbor { *asn-number* | *ip-address* | **peer-group** | **dynamic** |**all** } [**soft**] [**soft-outbound**] [**vrf** *vrf-name*]

Parameters

asn-number

Specifies the autonomous system number of the neighbors.

ip-address

Specifies a neighbor IP address in IPv4 format.

peer-group

Specifies a neighbor peer group.

dynamic

Specifies dynamic BGP flowspec neighbors.

all

Clears all BGP flowspec neighbors.

soft

Causes a soft reconfiguration.

soft-outbound

Causes a soft reconfiguration and advertisement only of updated routes.

vrf *vrf-name*

Specifies a neighbor VRF instance.

Modes

Privileged EXEC mode

Examples

This example shows how to refresh BGP flowspec information for all BGP flowspec neighbors.

```
device# clear bgp ip flowspec neighbor all

2018/10/12-00:37:02, [BGP-1006], 96176,, INFO, Avalanche-P6,  BGP: 10.50.50.254 DOWN
(User Reset Peer Session).
2018/10/12-00:37:02, [BGP-1006], 96177,, INFO, Avalanche-P6,  BGP: 10.51.51.254 DOWN
(User Reset Peer Session).
2018/10/12-00:37:13, [BGP-1005], 96178,, INFO, Avalanche-P6,  BGP: 10.50.50.254 UP
(ESTABLISHED).
```

```
2018/10/12-00:37:13, [BGP-1005], 96179,, INFO, Avalanche-P6,  BGP: 10.51.51.254 UP
(ESTABLISHED).
```

This example shows how to clear all dynamic BGP flowspec neighbors.

```
device# clear bgp ip flowspec neighbor dynamic all
```

clear bgp ip flowspec routes

Removes and re-installs Border Gateway Protocol flow specification (BGP flowspec) routes into the hardware.

Syntax

clear bgp ip flowspec routes [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example shows how to uninstall and re-install BGP flowspec rules into the hardware.

```
device# clear bgp ip flowspec routes
```

clear bgp ip neighbor ipv6

Requests a dynamic refresh of Border Gateway Protocol (BGP) connections to IPv4 over IPv6 neighbors.

Syntax

clear bgp ip neighbor ipv6 {*as-num* | *ipv6-addr* [**last-packet-with-error** | **notification-errors** | **soft** [**in** | **out**] | **soft-outbound** | **traffic**]

clear bgp ip neighbor ipv6 all [**soft** [**in** | **out**] | **soft-outbound**]

clear bgp ip neighbor ipv6 dynamic all

Parameters

as-num

Specifies an autonomous system number. Range is from 1 through 4294967295.

ipv6-addr

Specifies an IPv6 address in dotted-decimal format.

last-packet-with-error

Specifies clearing connections identified as having the last packet received with an error.

notification-errors

Specifies clearing connections identified as having notification errors.

soft

Refreshes routes received from or sent to the neighbor.

in

Refreshes only received routes.

out

Refreshes only sent routes.

soft-outbound

Refreshes all outbound routes by applying new or changed filters, but sends only the existing routes affected by the new or changed filters to the neighbor.

Note

Use **soft-outbound** only when the outbound policy is changed. This operand updates all outbound routes by applying the new or changed filters. However, the device sends to the neighbor only the existing routes that are affected by the new or changed filters. The **soft out** option updates all outbound routes and then sends the entire BGP4 route table on the device to the neighbor after the device changes or excludes the routes affected by the filters.

traffic

Clears the counters (resets them to 0) for BGP4 messages.

all

Resets and clears all BGP4 connections to all neighbors.

dynamic all

Clears dynamically-learned neighbors through the listen range.

Modes

Privileged EXEC mode

Examples

The following example refreshes connections with all IPv4 over IPv6 neighbors.

```
device# clear bgp ip neighbor ipv6
```

clear cfm y1731 client-signal-fail statistics

Clears ETH-CSF statistics for all Maintenance Entity Group End Point (MEP) and associated Client interfaces.

Syntax

clear cfm y1731 client-signal-fail statistics

Command Default

Interfaces are not cleared by default.

Modes

Privileged EXEC mode

Examples

This example clears ETH-CSF statistics.

```
device# clear cfm y1731 client-signal-fail statistics
```

clear cfm y1731 statistics

Clears all Y.1731 statistics.

Syntax

clear cfm y1731 statistics

Modes

Privileged EXEC mode

Examples

This example shows how to clears all Y.1731 statistics.

```
device# clear cfm y1731 statistics
```

clear cfm y1731 statistics delay-measurement

Clears all Y.1731 statistics for Two-Way ETH-DM.

Syntax

clear cfm y1731 statistics delay-measurement

Modes

Privileged EXEC mode

Examples

This example shows how to clears all Y.1731 statistics for Two-Way ETH-DM.

```
device# clear cfm y1731 statistics delay-measurement
```

clear cfm y1731 statistics synthetic-loss-measurement

Clears all Y.1731 statistics for Two-way ETH-SLM.

Syntax

clear cfm y1731 statistics

Modes

Privileged EXEC mode

Examples

This example shows how to clears all Y.1731 statistics for Two-Way ETH-SLM.

```
device# clear cfm y1731 statistics
```

clear counters

Clears the IP counter statistics on the device.

Syntax

clear counters { **all** | **interface** { **ve** *ve-id* } }

clear counters slot *slot-id*

Parameters

all

Clears all IP counter statistics on the device or the selected interface. It also clears all VE Statistics.

interface

Specifies an interface.

ve *ve-id*

Clears all VE statistics for the specified VE ID.

slot *slot-id*

For devices that do not support line cards, specify `0`.

Modes

Privileged EXEC mode

This example clears all VE statistics for the specified VE ID.

```
9540
SLX# clear counters interface ve 138
9640
SLX# clear counters interface ve 15
```

clear counters access-list

Clears access-control list (ACL) statistical information for a given network protocol and inbound or outbound direction.

Syntax

clear counters access-list interface { **ethernet** *slot* **/** *port* | **port-channel** *index* | **vlan** *vlan-id* } { **in** | **out** }

clear counters access-list interface management *mgmt-id* **in**

clear counters access-list interface ve *vlan-id* { **in** | **out** }

clear counters access-list global-subnet-broadcast ip *acl-name*

clear counters access-list { **ip** | **ipv6** } [*acl-name* { **in** | **out** }]

clear counters access-list subnet-broadcast ip [*acl-name* [**interface** { **ethernet** *slot* **/** *port* | **ve** *vlan-id* }]]

clear counters access-list { **ip** | **ipv6** } *acl-name* **interface** { **ethernet** *slot* **/** *port* | **port-channel** *index* | **ve** *vlan-id* } { **in** | **out** }

clear counters access-list { **ip** | **ipv6** } *acl-name* **interface management** *mgmt-id* **in**

clear counters access-list receive { **ip** | **ipv6** } [*acl-name*]

clear counters access-list mac [*acl-name* { **in** | **out** }]

clear counters access-list mac *acl-name* **interface** { **ethernet** *slot* **/** *port* | **port-channel** *index* | **vlan** *vlan-id* } { **in** | **out** }

Parameters

interface

Specifies an interface.

ethernet

Specifies a physical Ethernet interface.

slot

Specifies a valid slot number. For devices that do not support linecards, specify **0**.

port

Specifies a valid port number.

global-subnet-broadcast ip

(SLX 9540 and SLX 9640 devices) Specifies an IP broadcast ACL (bACL) applied at device level.

management *mgmt-id*

Specifies the management interface. The only supported value is 0.

port-channel *index*

Specifies a port-channel.

in

Specifies incoming binding direction.

out

Specifies outgoing binding direction.

subnet-broadcast ip

(SLX 9540 and SLX 9640 devices) Specifies an IP broadcast ACL (bACL) applied at physical-interface or VE level.

vlan *vlan-id*

(Available only on Layer 2) Specifies a VLAN.

ve *vlan-id*

(Available only on Layer 3) Specifies a virtual Ethernet (VE) interface.

ip

Specifies the IPv4 Layer 3 network protocol.

ipv6

Specifies the IPv6 Layer 3 network protocol.

mac

Specifies the medium access control (MAC) Layer 2 network protocol.

receive

Specifies an ACL that applies to device recieve-path traffic.

acl-name

Specifies the ACL name. To clear statistics on all counters of an ACL-type, do not specify *acl-name*.

Modes

Privileged EXEC mode

Usage Guidelines

You can clear all statistics for a specified ACL or only for that ACL on a specified interface.

You can also clear statistical information for all ACLs bound to a specified Ethernet or management interface, a port-channnel, VLAN, or VE.

Examples

The following example clears ACL statistics on a specified Ethernet interface.

```
device# clear counters access-list interface ethernet 0/1
```

The following example clears ACL statistics for a specified MAC ACL on a specified Ethernet interface.

```
device# clear counters access-list mac MAC_ACL_1 interface ethernet 0/2
```

The following example clears ACL statistics for a specified MAC ACL on all interfaces on which this ACL is applied.

```
device# clear counters access-list mac MAC_ACL_1
```

The following example clears ACL statistics for a specified IPv4 ACL on a specified interface.

```
device# clear counters access-list ip IP_ACL_1 interface ethernet 0/3
```

The following example clears ACL statistics for a specified IPv4 ACL on all interfaces on which it is applied.

```
device# clear counters access-list ip IP_ACL_1
```

The following example clears incoming ACL statistics for a specified IPv6 ACL on a virtual Ethernet (VE) interface.

```
device# clear counters access-list ipv6 ip_acl_3 interface ve 10 in
```

The following example clears IPv6 receive-path ACL statistics.

```
device# clear counters access-list receive ipv6
```

clear counters access-list overlay type vxlan

Clears statistics of a specific overlay VXLAN ACL.

Syntax

clears counters access-list overlay type vxlan *acl-name*

Parameters

acl-name

Specifies the ACL name.

Modes

Privileged EXEC mode

Usage Guidelines

This command clears counters for overlay VXLAN ACLs applied to overlay transit nodes.

Overlay ACLs are not supported for SLX 9150 or SLX 9250 devices.

Examples

The following example clears the statistics of a specific overlay VXLAN ACL.

```
device# clear counters access-list overlay type vxlan abc_ext
```

clear counters storm-control

Clears all broadcast, unknown unicast, and multicast (BUM) related counters in the system.

Syntax

clear counters storm-control

clear counters storm-control [**broadcast** | **multicast** | **unknown-unicast**] [**interface ethernet** *slot/port*]

Parameters

broadcast

Clears all BUM-related counters in the system for the broadcast traffic type.

multicast

Clears all BUM-related counters in the system for the multicast traffic type.

unknown-unicast

Clears all BUM-related counters in the system for the unknown-unicast traffic type.

interface ethernet *slot/port*

Clears all BUM-related counters in the system for the specified interface. For devices that do not support linecards, specify 0.

Modes

Privileged EXEC mode.

Usage Guidelines

This command clears the counters for broadcast, unknown-unicast, and multicast traffic for the entire system, for specified traffic types, for specified interfaces, or for specified traffic types on specified interfaces.

Examples

Clear counters for broadcast traffic on an Ethernet interface.

```
device# clear counters storm-control broadcast interface ethernet 0/1
```

Clear counters for all traffic types enabled on an Ethernet interface.

```
device# clear counters storm-control interface ethernet 0/1
```

Clear counters for all multicast traffic in the system.

```
device# clear counters storm-control multicast
```

Clear all BUM-related counters in the system.

```
device# clear counters storm-control
```

clear dot1x statistics

Clears all accumulated dot1x port authentication statistics on the ports.

Syntax

clear dot1x statistics [**interface ethernet** *slot/port*]

Parameters

interface ethernet *slot/port*

Specifies to clear all dot1x statistics for a specified interface port.

Modes

Privileged EXEC mode

Examples

This example clears all accumulated dot1x port authentication statistics on all ports.

```
device# clear dot1x statistics
```

This example clears all dot1x statistics for a specified interface port.

```
device# clear dot1x statistics interface ethernet 1/1
```

clear erp statistics

Clears statistics of all Ethernet Ring Protection (ERP) interfaces for all ERP instances, or for a specified instance.

Syntax

clear erp statistics [*erp_id*]

Parameters

erp_id

Specifies an ERP ID.

Modes

Privileged EXEC mode

Usage Guidelines

This command clears the statistics of all the ERP instances present in the device. Use the *erp_id* to clear the statistics of a given ERP instance.

Examples

The following example clears all ERP statistics.

```
device# clear erp statistics
```

The following example clears ERP statistics for instance 1.

```
device# clear erp statistics 1
```

clear erp wtb-time

Clears the Wait to Block (WTB) timer of a specified Ethernet Ring Protection (ERP) protocol instance.

Syntax

clear erp wtb-time *erp_id*

Parameters

erp_id

Specifies an ERP ID.

Modes

Privileged EXEC mode

Usage Guidelines

This command is allowed only on the RPL-owner node. An error message is issued if it is executed on another node.

Examples

The following example clears the WTB timer for ERP instance 1.

```
device# clear erp wtb-time 1
```

clear erp wtr-time

Clears the Wait to Restore (WTR) timer of a specified Ethernet Ring Protection (ERP) protocol instance.

Syntax

clear erp wtr-time *erp_id*

Parameters

erp_id

Specifies an ERP ID.

Modes

Privileged EXEC mode

Usage Guidelines

This command is allowed only on the RPL-owner node. An error message is issued if it is executed on another node.

Examples

The following example clears the WTR timer for ERP instance 1.

```
device# clear erp wtr-time 1
```

clear filter-change-update

Clears the filter change update delay period.

Syntax

clear filter-change-update

Modes

Privileged EXEC mode

Usage Guidelines

When a previously-distributed BGP flowspec route map is updated, by default the changes are applied after a delay of 10 seconds. When you make multiple updates and to send a lesser number of changes to the hardware, you can configure a longer delay period by using the **filter-change-update-delay** command.

The **clear filter-change-update** command clears any previously-configured delay time. This prevents unnecessary delay in installing BGP flowspec rule changes in the hardware. When the delay time is cleared, all route-map changes are propagated to the hardware.

Examples

The following example shows how to clear the filter change update delay period so that all route-map changes are propagated to the hardware.

```
device# clear filter-change-update
```

clear ip arp inspection statistics

Clears Dynamic ARP Inspection (DAI) statistics for all DAI-enabled VLANs.

Syntax

clear ip arp inspection statistics

Modes

Privileged EXEC mode

Usage Guidelines

The capacity of each statistic counter is 64 bits, beyond which such a counter is reset to zero.

Examples

The following example clears DAI statistics for all DAI-enabled VLANs.

```
device# clear ip arp inspection statistics
```

clear ip arp suppression-cache

Clears the IPv4 ARP-suppression cache and downloads the current forwarding database from BGP-EVPN. You can also clear the cache for a specified bridge domain or VLAN.

Syntax

clear ip arp suppression-cache [**bridge-domain** *bridge-domain-id* | **vlan** *vlan-id*]

Parameters

bridge-domain *bridge-domain-id*

Specifies a bridge domain.

vlan *vlan-id*

Specifies a VLAN interface. The range is from 1 through 4090.

Modes

Privileged EXEC mode

Usage Guidelines

Running this command might impact traffic.

Examples

The following example clears the ARP-suppression cache.

```
device#  clear ip arp suppression-cache
```

clear ip arp suppression-statistics

Clears ARP suppression statistics. You can also clear statistics for a specified bridge domain or VLAN.

Syntax

clear ip arp suppression-statistics [**bridge-domain** *bridge-domain-id* | **vlan** *vlan-id*]

Parameters

bridge-domain *bridge-domain-id*

Specifies a bridge domain.

vlan *vlan-id*

Specifies a VLAN interface. The range is from 1 through 4090.

Modes

Privileged EXEC mode

Examples

The following example clears all ARP suppression statistics.

```
device#  clear ip arp suppression-statistics
```

clear ip bgp dampening

Reactivates suppressed BGP4 routes.

Syntax

clear ip bgp dampening [*ip-addr* { **/** *mask* }] [**vrf** *vrf-name*]

Parameters

ip-addr

IPv4 address of a specified route in dotted-decimal notation.

mask

(Optional) IPv4 mask of a specified route in CIDR notation.

vrf *vrf-name*

Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

This example unsuppresses all suppressed BGP4 routes.

```
device# clear ip bgp dampening
```

This example unsuppresses suppressed BGP4 routes for VRF "red".

```
device# clear ip bgp dampening vrf red
```

clear ip bgp flap-statistics

Clears the dampening statistics for a BGP4 route without changing the dampening status of the route.

Syntax

clear ip bgp flap-statistics [*ip-addr* { **/** *mask* } | **neighbor** *ip-addr* | **regular-expression** *string*] [**vrf** *vrf-name*]

Parameters

ip-addr

IPv4 address of a specified route in dotted-decimal notation.

mask

(Optional) IPv4 mask of a specified route in CIDR notation.

neighbor

Clears dampening statistics only for routes learned from the specified neighbor.
ip-addr

IPv4 address of the neighbor.

regular-expression

Specifies a regular expression.
string

Regular expression.

vrf *vrf-name*

Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

This example clears the dampening statistics for a BGP4 route.

```
device# clear ip bgp flap-statistics 10.0.0.0/16
```

This example clears the dampening statistics for a BGP4 route for VRF "red".

```
device# clear ip bgp flap-statistics 10.0.0.0/16 vrf red
```

clear ip bgp local routes

Clears BGP4 local routes from the IP route table and resets the routes.

Syntax

clear ip bgp local routes [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

This example clears all BGP4 local routes.

```
device# clear ip bgp local routes
```

This example clears BGP4 local routes for VRF "red".

```
device# clear ip bgp local routes vrf red
```

clear ip bgp neighbor

Requests a dynamic refresh of BGP4 connections or routes from a neighbor, with a variety of options.

Syntax

clear ip bgp neighbor { **all** | *as-num* | *ip-addr* | *peer-group-name* } [**last-packet-with-error** | **notification-errors** | **soft** [**in** [**prefix-filter**] | **out**] | **soft-outbound** | **traffic**] [**vrf** *vrf-name*]

Parameters

all

Resets and clears all BGP4 connections to all neighbors.

as-num

Clears all BGP4 connections within this autonomous system. Range is from 1 through 4294967295.

peer-group-name

Clears all BGP4 connections in this peer group. Range is from 1 through 63 characters.

ip-addr

Clears all BGP4 connections with this IPv4 address, in dotted-decimal notation.

last-packet-with-error

Clears all BGP4 connections identified as having the last packet received with an error.

notification-errors

Clears all BGP4 connections identified as having notification errors.

soft

Refreshes routes received from or sent to the neighbor.

in

Refreshes received routes.

prefix-filter

Refreshes Outbound Route Filters (ORFs) that are prefix-based.

out

Refreshes sent routes.

soft-outbound

Refreshes all outbound routes by applying new or changed filters, but sends only the existing routes affected by the new or changed filters to the neighbor.

Note
Use **soft-outbound** only if the outbound policy is changed. This operand updates all outbound routes by applying the new or changed filters. However, the device sends to the neighbor only the existing routes that are affected by the new or changed filters. The **soft out** operand updates all outbound routes and then sends the entire BGP4 route table on the device to the neighbor after the device changes or excludes the routes affected by the filters.

traffic

Clears the counters (resets them to 0) for BGP4 messages.

vrf *vrf-name*

Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

This example refreshes all BGP4 neighbor connections.

```
device# clear ip bgp neighbor all
```

This example refreshes all BGP4 neighbor connections for VRF "red".

```
device# clear ip bgp neighbor all vrf red
```

clear ip bgp neighbor dynamic

Clears all dynamic neighbor connections on a device, in a specified VRF, or in a VPNv4 or VPNv5 address family.

Syntax

clear ip bgp neighbor dynamic [**all** | **vrf** *vrf-name*]

clear ip bgp vpnv4 neighbor dynamic all

clear ip bgp vpnv6 neighbor dynamic all

Parameters

all | **vrf**

Specifies whether to clear all dynamic neighbors or only the neighbors in the specified VRF.

vrf-name

Specifies the name of the VRF from which to clear neighbors.

Modes

Privileged EXEC mode

Examples

This example removes all dynamic BGP4 neighbors.

```
device# configure terminal
device(config)# clear ip bgp neighbor dynamic all
```

This example removes all dynamic BGP4 neighbors from the VRF named vrf-red.

```
device# configure terminal
device(config)# clear ip bgp neighbor dynamic vrf vrf-red
```

clear ip bgp routes

Clears BGP4 routes from the IP route table and resets the routes.

Syntax

clear ip bgp routes [*ip-addr* [**/** *mask*]] [**vrf** *vrf-name*]

Parameters

ip-addr

IPv4 address of a specified route in dotted-decimal notation.

mask

(Optional) IPv4 mask of a specified route in CIDR notation.

vrf *vrf-name*

Specifies the name of the VRF instance to associate with subsequent address-family configuration mode commands.

Modes

Privileged EXEC mode

Examples

This example clears all BGP4 routes.

```
device# clear ip bgp routes 10.0.0.0/16
```

This example clears BGP4 routes for VRF instance "red":

```
device# clear ip bgp routes 10.0.0.0/16 vrf red
```

clear ip bgp rpki server

Use this command to stop and restart the RTR library configuration for this particular RPKI server. This command closes the current session and tries to re-establishes connection with the configured RPKI server. The *all* format of this command closes all sessions and tries to re-establish connections.

Syntax

clear ip bgp rpki server { *hostname* | *address* } **port** *port no*

clear ip bgp rpki server all

Parameters

hostname

The hostname of the remote RPKI cache server. You can use one of *hostname* or IP *address*.

address

The IP address of the remote RPKI cache server. You can use one of *hostname* or IP *address*.

port *port no*

The port number on which this RPKI cache server can be accessed.

all

This keyword indicates that the command must be performed on all the remote RPKI cache servers configured on this device.

Modes

Privileged EXEC mode

Usage Guidelines

Note
Since you can only connect to one remote RPKI server at a time, the two commands perform the same function.

Examples

This example command closes the TCP connection to the remote RPKI cache server with IP address 192.168.14.2, purges the ROAs downloaded from the server, reconnects back to the server, and downloads the ROAs again.

```
SLX# clear ip bgp rpki server 192.168.14.2 port 1030
Possible completions:
<cr>
```

clear ip bgp traffic

Clears the BGP4 message counter for all neighbors.

Syntax

clear ip bgp traffic [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example clears the BGP4 message counters.

```
device# clear ip bgp traffic
```

clear ip dhcp relay statistics

Clears IP DHCP Relay statistics.

Syntax

clear ip dhcp relay statistics ip-address *ip-address*

Command Default

DHCP relay statistics are present on the DHCP server.

Parameters

ip-address *ip-address*

IPv4 address of DHCP server where client requests are to be forwarded.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to clear IP DHCP Relay statistics for a specific IP DHCP Relay address or all addresses on the device.

Examples

The following example clears statistics for IP DHCP Relay

```
device# clear ip dhcp relay statistics ip-address 10.1.0.1
```

clear ip dhcp snooping binding

Deletes the specified binding entries from the DHCP snooping binding database.

Syntax

clear ip dhcp snooping binding [[*mac-addr*| *ip-addr*] |**vlan** *vlan-id* | **interface** *switchport interface*]

clear ip dhcp snooping binding vlan *vlan-id*

clear ip dhcp snooping binding interface *switchport interface*

Command Default

By default, DHCP snooping binding entries are present in the binding database.

Parameters

binding [*mac-addr*| *ip-addr*]

Specifies the MAC or IP address of the host for the entry in the binding database.

vlan *vlan-id* | **interface** [**switchport** | **physical interface**]]

Deletes the specified binding entry from the binding database.

vlan *vlan-id*

Deletes all binding entries for the specified VLAN from the binding database.

interface *switchport interface*

Deletes all binding entries from the binding database that were learned on the specified switchport.

Modes

Privileged EXEC mode

Examples

This example clears one binding entry from the database.

```
device# clear ip dhcp snooping binding <mac-addr> <ip-addr> vlan <vlan-id>
interface <switchport/physical interface>
```

This example clears all binding entries for the specified VLAN.

```
device# clear ip dhcp snooping binding vlan <vlan-id>
```

This example clears all binding entries learned on the specified switchport.

```
clear ip dhcp snooping binding interface <switchport/physical interface>
```

clear ip flowspec rules statistics

Clears statistics for Border Gateway Protocol flow specification (BGP flowspec) rules.

Syntax

clear ip flowspec rules statistics [**vrf** *vrf-name*]

Parameters

vrf-name

Name of a VRF instance in which BGP flowspec rules are used.

Modes

Privileged EXEC mode

Usage Guidelines

When a VRF is not specified, the **clear ip flowspec rules statistics** command clears BGP flowspec rule statistics for the default VRF.

Examples

The following example shows how to clear BGP flowspec rule statistics for a VRF named red.

```
device# clear ip flowspec rules statistics vrf red
```

The following example shows how to clear BGP flowspec rule statistics for the default VRF.

```
device# clear ip flowspec rules statistics
```

clear ip igmp groups

Removes the accumulated information about learned groups for a specified VLAN, bridge domain, MCT (Multi-Chassis Trunking) cluster, or CCEP (Cluster Client Edge Port) client.

Syntax

k

clear ip igmp groups [**vlan** *id* | **bridge-domain** *id* | **cluster** *id* | **client** *id*]

Parameters

vlan

Specifies the VLAN for which you want to remove group information.

id

Specifies the ID of the VLAN.

bridge-domain

Specifies the bridge domain for which you want to remove group information.

id

Specifies the ID of the bridge domain.

cluster

Specifies the MCT cluster for which you want to remove group information.

id

Specifies the ID of the cluster.

client

Specifies the CCEP client for which you want to remove group information.

id

Specifies the ID of the client.

Modes

Privileged EXEC mode

Examples

The following example clears the groups information for a VLAN.

```
clear ip igmp groups vlan 100
```

clear ip igmp statistics

Removes the accumulated IGMP statistics on the specified VLAN or bridge domain.

Syntax

clear ip igmp statistics [**vlan** *id* | **bridge-domain** *id*]

Parameters

vlan

Specifies the VLAN for which you want to remove IGMP statistics.
id

Specifies the ID of the VLAN.

bridge-domain

Specifies the bridge domain for which you want to remove IGMP statistics.
id

Specifies the ID of the bridge domain.

Modes

Privileged EXEC mode

Examples

The following example clears the statistics for a VLAN.

```
clear ip igmp statistics vlan 100
```

clear ip multicast snooping mcache

Removes the accumulated information about the multicast forwarding cache for a VLAN or a bridge domain.

Syntax

clear ip multicast snooping mcache [**vlan** *id* | **bridge-domain** *id*]

Parameters

vlan

Specifies the VLAN for which you want to clear the forwarding cache.

id

Specifies the ID of the VLAN.

bridge-domain

Specifies the bridge domain for which you want to clear the forwarding cache.

id

Specifies the ID of the bridge domain.

Modes

Privileged EXEC mode

Examples

The following example clears the forwarding cache for a VLAN.

```
clear ip multicast snooping mcache vlan 100
```

clear ip pim mdt

Clears the MDTs maintained by PIM.

Syntax

clear ip pim mdt [**group** *GROUP-IP-ADDRESS*]

Parameters

group *GROUP-IP-ADDRESS*

Specifies the group ip address.

Modes

Privileged EXEC mode

clear ip ospf

Clears OSPF data processes, graceful restart, counters, neighbors, or routes.

Syntax

clear ip ospf all [**vrf** *vrf-name*]

clear ip ospf graceful-restart { **vrf** *vrf-name* | *all-vrf* }

clear ip ospf counters { **all** | **ethernet** *slot/port* | **loopback** *number* | **port-channel** *number* | **ve** *vlan-id* } [**vrf** *vrf-name*]

clear ip ospf neighbor { *ip-addr* | **all** } [**vrf** *vrf-name*]

clear ip ospf routes { *ip-addr/mask* | **all** } [**vrf** *vrf-name*]

Parameters

all

Clears all OSPF data processes.

vrf *name*

Specifies a VRF.

gr *vrf-name*

Gracefully restarts the OSPF session for the specified VRF. If no VRF is specified, the default-vrf session is restarted.

counters

Clears OSPF counters.

all

Clears all counters.

ethernet *slot* **/** *port*

Specifies an Ethernet slot and port.

loopback *number*

Specifies a loopback interface. Valid values range from 1 through 255.

port-channel *number*

Specifies a port-channel.

ve *vlan-id*

Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

neighbor

Clears neighbors.

ip-addr

Specifies the IP address of the neighbor.

all

Clears all neighbors.

routes

Clears matching routes or clears all routes.
ip-addr/mask

Clears all routes that match the prefix and mask that you specify.

all

Clears all routes.

Modes

Privileged EXEC mode

Examples

The following example restarts all OSPF processes.

```
device# clear ip ospf all
```

This example gracefully restarts the OSPF session for the VRF named "red."

```
device# clear ip ospf gr red
```

clear ip route

Clears a specified route or all IP routes in the IP routing tables.

Syntax

clear ip route { *A.B.C.D* | *A.B.C.D/M* } [**vrf** *vrf-name*]

clear ip route all [**vrf** *vrf-name*]]

clear ip route slot *line-card-number* [*A.B.C.D* | *A.B.C.D/M*] [**vrf** *vrf-name*]

Parameters

A.B.C.D

Specifies an IPv4 address.

A.B.C.D/M

Specifies an IPv4 address and mask.

vrf *vrf-name*

Specifies a VRF instance from which the user is currently retrieving routes.

all

Specifies all routes.

slot *line-card-number*

Specifies a line card.

Modes

Privileged EXEC mode

Examples

The following example clears the IP route specified by IP address 192.158.1.1/24.

```
device# clear ip route 192.158.1.1/24
```

clear ipv6 bgp dampening

Reactivates suppressed BGP4 routes.

Syntax

clear ipv6 bgp dampening [*ipv6-addr* { **/** *mask* }] [**vrf** *vrf-name*]

Parameters

ipv6-addr

IPv6 address of a specified route in dotted-decimal notation.

mask

IPv6 mask of a specified route in CIDR notation.

vrf *vrf-name*

Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example unsuppresses all suppressed BGP4+ routes.

```
device# clear ipv6 bgp dampening
```

The following example unsuppresses suppressed BGP4+ routes for VRF "red".

```
device# clear ipv6 bgp dampening vrf red
```

clear ipv6 bgp flap-statistics

Clears route-flap statistics for BGP4+ routes.

Syntax

clear ipv6 bgp flap-statistics [*ipv6-addr* { **/** *mask* } | **neighbor** { *ipv6-addr* | *ipv4-addr* } | **regular-expression** *string*] [**vrf** *vrf-name*]

Parameters

ipv6-addr

IPv6 address of a specific route in dotted-decimal notation.

mask

(Optional) IPv6 mask of the specified route in CIDR notation.

neighbor

Clears route-flap statistics only for routes learned from the specified neighbor.

ipv6-addr

IPv6 address of the neighbor.

ipv4-addr

IPv4 address of the neighbor.

regular-expression

Specifies a regular expression.

string

Regular expression.

vrf *vrf-name*

Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

This example clears all dampening statistics for all BGP4+ route.

```
device# clear ipv6 bgp flap-statistics
```

This example clears the dampening statistics for a BGP4+ route for the VRF "red".

```
 device# clear ipv6 bgp flap-statistics vrf red
```

This example Clears route-flap statistics for routes learned from a IPv4 BGP Peer and an IPv6 BGP Peer.

```
SLX# clear ipv6 bgp flap-statistics neighbor 192.0.2.1 vrf vrf1
SLX# clear ipv6 bgp flap-statistics neighbor 2001:db8::01:01
```

clear ipv6 bgp local routes

Clears BGP4+ local routes from the IP route table and resets the routes.

Syntax

clear ipv6 bgp local routes [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

This example clears all BGP4+ local routes.

```
device# clear ipv6 bgp local routes
```

This example clears BGP4+ local routes for VRF "red".

```
device# clear ipv6 bgp local routes vrf red
```

clear ipv6 bgp neighbor

Requests a dynamic refresh of BGP4+ connections or routes from a neighbor, with a variety of options.

Syntax

clear ipv6 bgp neighbor [**all** | *as-num* | *peer-group-name* | *ipv6-addr*] [**last-packet-with-error** | **notification-errors** | **soft** [**in** [**prefix-filter**] | **out**]] | **soft-outbound** | **traffic**] [**vrf** *vrfname*]

Parameters

all

Resets and clears all BGP4+ connections to all neighbors.

as-num

Clears all BGP4+ connections within this autonomous system. Range is from 1 through 4294967295.

peer-group-name

Clears all BGP4+ connections in this peer group. Range is from 1 through 63 characters.

ipv6-addr

Clears all BGP4+ connections with this IPv6 address, in dotted-decimal notation.

last-packet-with-error

Clears all BGP4+ connections identified as having the last packet received with an error.

notification-errors

Clears all BGP4+ connections identified as having notification errors.

soft

Refreshes routes received from or sent to the neighbor.

in

Refreshes received routes.

prefix-filter

Refreshes Outbound Route Filters (ORFs) that are prefix-based.

out

Refreshes sent routes.

soft-outbound

Refreshes all outbound routes by applying new or changed filters, but sends only the existing routes affected by the new or changed filters to the neighbor.

Note
Use **soft-outbound** only if the outbound policy is changed. This operand updates all outbound routes by applying the new or changed filters. However, the device sends to the neighbor only the existing routes that are affected by the new or changed filters. The **soft out** operand updates all outbound routes and then sends the entire BGP4+ route table on the device to the neighbor after the device changes or excludes the routes affected by the filters.

traffic

Clears the counters (resets them to 0) for BGP4+ messages.

vrf *vrf-name*

Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

This example refreshes all BGP4+ neighbor connections.

```
device# clear ipv6 bgp neighbor all
```

This example resets all the counters for BGP4+ messages.

```
device# clear ipv6 bgp neighbor all traffic
```

This example clears BGP4+ connections with a specified peer group.

```
device# clear ipv6 bgp neighbor P1
```

This example clears BGP4+ connections with a specified peer group for VRF "red".

```
device# clear ipv6 bgp neighbor P1 vrf red
```

clear ipv6 bgp neighbor dynamic

Clears all dynamic neighbor connections on a device or all dynamic neighbor connections in a specified VRF.

Syntax

clear ipv6 bgp neighbor dynamic [**all** | **vrf** *vrf-name*]

Parameters

all | **vrf**

Specifies whether to clear all dynamic neighbors or only the neighbors in the specified VRF.

vrf-name

Specifies the name of the VRF from which to clear neighbors.

Modes

Privileged EXEC mode

Examples

This example removes all dynamic BGP4+ neighbors.

```
device# configure terminal
device(config)# clear ipv6 bgp neighbor dynamic all
```

This example removes all dynamic BGP4+ neighbors from the VRF named vrf-red.

```
device# configure terminal
device(config)# clear ipv6 bgp neighbor dynamic vrf vrf-red
```

clear ipv6 bgp routes

Clears BGP4+ routes from the IP route table and resets the routes.

Syntax

clear ipv6 bgp routes [*ipv6-addr* [**/** *mask*]] [**vrf** *vrfname*]

Parameters

ipv6-addr

IPv6 address of a specified route in dotted-decimal notation.

mask

(Optional) IPv6 mask of a specified route in CIDR notation.

vrf *vrf-name*

Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

This example clears specific BGP4+ routes.

```
device# clear ipv6 bgp routes 2000::/64
```

This example clears specific BGP4+ routes for VRF "red".

```
device# clear ipv6 bgp routes 2000::/64 vrf red
```

clear ipv6 bgp traffic

Clears the BGP4+ message counter for all neighbors.

Syntax

clear ipv6 bgp traffic [**vrf** *vrf-name*]

Modes

Privileged EXEC mode

Parameters

vrf *vrf-name*

Specifies the name of a VRF instance.

Examples

This example clears all BGP4+ message counters.

```
device# clear ipv6 bgp traffic
```

This example clears BGP4+ message counters for VRF "red".

```
device# clear ipv6 bgp traffic vrf red
```

clear ipv6 counters

Clears IPv6 counters on all interfaces or on a specified interface.

Syntax

clear ipv6 counters { **all** | **interface** { **ethernet** *slot/port* | **loopback** *port-number* | **port-channel** *number* | **ve** *ve-id* }}

Parameters

all

Specifies all interfaces.

ethernet

Represents a valid, physical Ethernet subtype.

slot

Specifies a valid slot number. For devices that do not support line cards, specify **0**.

port

Specifies a valid port number.

loopback

Specifies a loopback interface.

port-number

Port number of the loopback interface. The range is from 1 through 255.

port-channel *number*

Specifies a port-channel.

ve

Specifies a virtual Ethernet (VE) interface.

ve_id

ID of the VE interface. The range is from 1 through 4096.

Modes

Privileged EXEC mode

Examples

The following example clears counters on Ethernet 2/3.

```
device# clear ipv6 counters interface ethernet 2/3
```

clear ipv6 dhcp relay delegated-prefixes

Clears IPv6 DHCP delegated prefixes for specific VRF.

Syntax

clear ipv6 dhcp relay delegated-prefixes { **vrf** *vrf-name* } { **ipv6-prefix** | **all** | **interface** { **ethernet** *slot/port* | **ve** *ve-id* | **po** *po-id* } }

Parameters

vrf *vrf-name*

Specifies the VRF from which to remove all prefix configuration.

ipv6-prefix

Specifies the IPv6 prefix address in this format: X:X::X:X/M.

all

Clears all delegated prefixes and remove the corresponding routes permanently from the router for the vrf.

interface

Configures the interface on which all delegated prefixes must be removed from. This action also permanently removes the corresponding routes from the router for this interface. This action can be performed on an Ethernet or a VE interface.

ethernet *slot/port*

Configures the ethernet slot/port on which all delegated prefixes must be removed from. This action also permanently removes the corresponding routes from the router for this interface.

ve *ve-id*

Configures the VE on which all delegated prefixes must be removed from. This action also permanently removes the corresponding routes from the router for this interface.

po *po-id*

Configures the port-channel interface on which all delegated prefixes must be removed from. This action also permanently removes the corresponding routes from the router for this interface.

Modes

Privileged EXEC mode

Usage Guidelines

None.

Examples

Clear all the delegated prefix parameter

```
device# clear ipv6 dhcp relay delegated-prefixes
```

clear ipv6 dhcp relay statistics

Clears IPv6 DHCP Relay statistics

Syntax

clear ipv6 dhcp relay statistics ip-address *ip-address*

Command Default

DHCP relay statistics are present on the DHCP server.

Parameters

ip-address *ip-addr*

IPv6 address of DHCP server where client requests are to be forwarded.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to clear all the DHCP Relay statistics.

Examples

Clear all the DHCP Relay statistics on the device.

```
device# clear ipv6 dhcp relay statistics
```

clear ipv6 mld groups

Removes the accumulated information about learned groups for a specified bridge domain, VLAN, MCT (Multi-Chassis Trunking) cluster, or CCEP (Cluster Client Edge Port) client.

Syntax

clear ipv6 mld groups [*ipv6 address* [**bridge-domain** *bd id* |**interface** [**ethernet** | **port-channel**] *interface name* | **vlan** *vlan id* |**cluster** *cluster id* |**client** *client id*]

Parameters

ipv6 address

Specifies the address for which to clear group information

bridge-domain

Specifies the bridge domain for which to clear group information.
bd id

Specifies the ID of the bridge domain.

interface

Specifies the interface for which to clear group information.
ethernet *interface name*

Specifies the Ethernet name.

port channel *interface name*

Specifies the port channel name.

vlan

Specifies the VLAN for which to clear group information.
vlan id

Specifies the ID of the VLAN.

cluster

Specifies the MCT cluster for which to clear group information.
cluster id

Specifies the ID of the cluster.

client

Specifies the CCEP client for which to clear group information.
client id

Specifies the ID of the client.

Modes

Privileged EXEC mode

Examples

The following example shows the syntax for clearing the MLD groups for IPv6-specific addresses.

```
device# clear ipv6 mld groups ff28::1 bridge-domain 10
device# clear ipv6 mld groups ff38::2 vlan 100
```

The following example shows the syntax for clearing the MLD groups for a VLAN and a bridge domain.

```
device# clear ipv6 mld groups bridge-domain 10
device# clear ipv6 mld groups vlan 10
```

clear ipv6 mld snooping

Clears the IPv6 multicast snooping database, including entries for MLD snooping and IPv6 PIM snooping, for a VLAN or a bridge domain.

Syntax

clear ipv6 mld snooping [**vlan**| **bridge-domain** *id*]

Parameters

vlan

Specifies the VLAN for which to clear the multicast snooping database.

id

Specifies the ID of the VLAN.

bridge-domain

Specifies the bridge domain for which to clear the multicast snooping database.

id

Specifies the ID of the bridge domain.

Modes

Privileged EXEC mode

Examples

The following example clears the snooping database for a VLAN.

```
device# clear ipv6 mld snooping vlan 10
```

clear ipv6 mld statistics

Removes the accumulated MLD statistics on the specified VLAN or bridge domain.

Syntax

clear ipv6 mld statistics [**bridge-domain** *bd id* | **vlan** *vlan id*]

Parameters

bridge-domain

Specifies the bridge domain for which to remove MLD statistics.
bd id

The ID of the bridge domain.

vlan

Specifies the VLAN for which to remove MLD statistics.
vlan id

The ID of the VLAN.

Modes

Privileged EXEC mode

Examples

The following example shows the syntax for removing MLD statistics for a bridge domain and for a VLAN.

```
device# clear ipv6 mld statistics bridge-domain 100
device# clear ipv6 mld statistics vlan 100
```

clear ipv6 multicast snooping mcache

Removes the accumulated information about the multicast forwarding cache for a VLAN or bridge domain.

Syntax

clear ipv6 multicast snooping mcache [**vlan|bridge-domain** *id*]

Parameters

vlan

Specifies the VLAN for which to clear the forwarding cache.

id

Specifies the ID of the VLAN.

bridge-domain

Specifies the bridge domain for which to clear the forwarding cache.

id

Specifies the ID of the bridge domain.

Modes

Privileged EXEC mode

Examples

The following example clears the forwarding cache for a VLAN.

```
clear ipv6 multicast snooping mcache vlan 12
```

clear ipv6 nd suppression-cache

Clears the neighbor discovery (ND)-suppression cache. You can also clear the cache for a specified bridge domain or VLAN.

Syntax

clear ipv6 nd suppression-cache [**bridge-domain** *bridge-domain-id* | **vlan** *vlan-id*]

Parameters

bridge-domain *bridge-domain-id*

Specifies a bridge domain. The range is from 1 through 8192.

vlan *vlan-id*

Specifies a VLAN interface. The range is from 1 through 4090.

Modes

Privileged EXEC mode

Examples

The following example clears the ND-suppression cache.

```
device#  clear ipv6 nd suppression-cache
```

clear ipv6 nd suppression-statistics

Clears suppression statistics for neighbor discovery. You can also clear statistics for a bridge domain or VLAN.

Syntax

clear ipv6 nd suppression-statistics [**bridge-domain** *bridge-domain-id* | **vlan** *vlan-id*]

Parameters

bridge-domain *bridge-domain-id*

Specifies a bridge domain.

vlan *vlan-id*

Specifies a VLAN interface. The range is from 1 through 4090.

Modes

Privileged EXEC mode

Examples

The following example clears all neighbor discovery suppression statistics.

```
device# clear ipv6 nd suppression-statistics
```

clear ipv6 neighbor

Removes entries from the IPv6 neighbor table.

Syntax

clear ipv6 neighbor [**ipv6-address**] [**ethernet** *port/slot* | **ve** *ve-number*] [**force-delete** | **no-refresh** | **vrf** *vrf-name*]

Parameters

ipv6-address

Removes cache entries for the specified IPv6 address.

ethernet

Removes neighbor entries for the Ethernet interface.

ve *ve-number*

Removes neighbor entries for the the specified Virtual Ethernet (VE) interface.

force-delete

Force deletes all the dynamic neighbor entries.

no-refresh

Deletes all the dynamic neighbor entries.

vrf *vrf-name*

Removes entries from the IPv6 neighbor table for the specified VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

You must specify the *ipv6-address* parameter in hexadecimal using 16-bit values between colons as documented in RFC 2373.

Examples

The following example removes neighbor entries for Ethernet interface 1/3.

```
device# clear ipv6 neighbor ethernet 1/3 force-delete
```

clear ipv6 ospf

Clears OSPFv3 data processes, graceful restart, counters, force-spf, neighbors, redistribution, routes, and traffic.

Syntax

clear ipv6 ospf all [**vrf** *vrf-name*]

clear ipv6 ospf graceful-restart { **vrf** *vrf-name* | *all-vrf* }

clear ipv6 ospf counts [**vrf** *vrf-name*]

clear ipv6 ospf counts neighbor *A.B.C.D* [**vrf** *vrf-name*]

clear ipv6 ospf counts neighbor interface { **ethernet** *slot/port* | **loopback** *number* | **port-channel** *number* | **ve** *vlan_id* } [*A.B.C.D*]

clear ipv6 ospf { **force-spf** | **redistribution** | **traffic** } [**vrf** *vrf-name*]

clear ipv6 ospf neighbor *A.B.C.D* [**vrf** *vrf-name*]

clear ipv6 ospf neighbor all [**vrf** *vrf-name*]

clear ipv6 ospf neighbor interface { **ethernet** *slot/port* | **loopback** *number* | **port-channel** *number* | **ve** *vlan_id* } [*A.B.C.D*]

clear ipv6 ospf routes { *IPv6addr* | **all** } [**vrf** *vrf-name*]

Parameters

all

Clears all OSPFv3 data.

gr *vrf-name*

Gracefully restarts the OSPFv3 session for the specified VRF. If no VRF is specified, the default-vrf session is restarted.

counts

Clears OSPFv3 counters.

neighbor

Clears all OSPFv3 counters for a specified neighbor.
A.B.C.D

Specifies a neighbor.

vrf *vrf-name*

Specifies a VRF.

interface

Specifies an interface.

ethernet *slot* **/** *port*

Specifies an Ethernet slot and port.

loopback *number*

Specifies a loopback interface. Valid values range from 1 through 255.

port-channel *number*

Specifies a port-channel.

ve *vlan_id*

Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

force-spf

Performs the shortest path first (SPF) calculation without clearing the OSPFv3 database.

redistribution

Clears OSPFv3 redistributed routes.

traffic

Clears OSPFv3 traffic statistics.

routes

Clears OSPFv3 routes.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **force-spf** keyword to perform the shortest path first (SPF) calculation without clearing the OSPFv3 database.

Examples

The following example restarts the OSPFv3 processes.

```
device# clear ipv6 ospf all
```

The following example clears all OSPFv3 counters for a specified neighbor.

```
device# clear ipv6 ospf counts neighbor 10.10.10.1
```

This example gracefully restarts the OSPFv3 session for the VRF named "red."

```
device# clear ipv6 ospf gr red
```

clear ipv6 pim mcache

Clears the IPv6 PIM forwarding cache.

Syntax

clear ipv6 pim mcache

Modes

Privileged EXEC mode

Examples

The following example clears the IPv6 PIM forwarding cache for the current node.

```
device# clear ipv6 pim mcache
```

clear ipv6 pim rp-map

Clears the RP-to-group mappings in the static IPv6 PIM forwarding table.

Syntax

clear ipv6 pim rp-map

Modes

Privileged EXEC mode

Usage Guidelines

Use this command after the static Rendezvous Point (RP) configuration is changed. After the static multicast forwarding table is cleared, IPv6 PIM can use the new RP without waiting for the old information to time out.

Examples

The following example clears the static IPv6 PIM forwarding table for the current node.

```
device# clear ipv6 pim rp-map
```

clear ipv6 pim traffic

Clears the IPv6 PIM traffic counters.

Syntax

clear ipv6 pim traffic

Modes

Privileged EXEC mode

Examples

The following example clears the traffic counters on the current node.

```
device# clear ipv6 pim traffic
```

clear ipv6 route

Clears IPv6 routes.

Syntax

clear ipv6 route [*ipv6-address* **vrf** *vrf-name*] [**all vrf** *vrf-name*]

Parameters

ipv6-address

Removes IPv6 routes for the specified IPv6 address.

vrf *vrf-name*

Removes IPv6 routes for the specified VPN Routing and Forwarding (VRF) instance.

all

Removes all IPv6 routes.

slot *line-card-number*

(Not currently supported) Removes IPv6 routes for the specified line card.

Modes

Privileged EXEC mode

Examples

The following example clears IPv6 routes associated with the prefix 2000:7838::/32.

```
device# clear ipv6 route 2000:7838::/32
```

clear ipv6 vrrp statistics

Clears IPv6 VRRPv3 session statistics for all virtual groups, for a specified interface, or for a specified virtual group.

Syntax

clear ipv6 vrrp statistics [**all**]

clear ipv6 vrrp statistics [**interface** { **ethernet** *slot*/*port* | **ve** *vlan_id* }]

clear ipv6 vrrp statistics [**session** *VRID*]

Parameters

all

Clears all IPv6 VRRP statistics.

session *VRID*

Specifies the virtual group ID on which to clear statistics. The range is from 1 through 128.

interface

Specifies an interface.

ethernet *slot port*

Specifies a valid, physical Ethernet interface with a slot and port number.

ve *vlan_id*

Specifies the VE VLAN number. The range is from 1 through 4096.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported in IPv6 VRRPv3 and VRRP-E-v3.

Examples

The following example clears all IPv6 VRRPv3 statistics for all virtual groups.

```
device# clear ipv6 vrrp statistics all
```

The following example clears statistics for an IPv6 VRRPv3 session of virtual group 25.

```
device# clear ipv6 vrrp statistics session 25
```

The following example clears IPv6 VRRPv3 statistics on a specified virtual Ethernet interface.

```
device# clear ipv6 vrrp statistics interface ve 10
```

clear isis all

Clears all IS-IS information.

Syntax

clear isis all

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

This example clears all IS-IS information for a device.

```
device# clear isis all
```

clear isis counts

Clears IS-IS error statistics for a device.

Syntax

clear isis counts

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

This example clears IS-IS error statistics.

```
device# clear isis counts
```

clear isis database

Clears IS-IS database entries.

Syntax

clear isis database [**lsp-id level-1** | **level-2**]

Parameters

lsp-id

Specifies a link-state packet (LSP) n HHHH.HHHH.HHHH.HH-HH format or by entering a name, HH-HH.

level-1

Specifies Level 1 packets only.

level-2

Specifies Level 2 packets only.

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

This example clears IS-IS database entries, specifying an LSP name of “XMR.00-00”.

```
device# clear isis database XMR-1.00-00
```

This example clears IS-IS database entries for Level 1 LSPs.

```
device# clear isis database level-1
```

clear isis force-spf

Performs the shortest path first (SPF) calculation without clearing the IS-IS database.

Syntax

clear isis force-spf [**level-1** | **level-2**]

Parameters

level-1

Specifies Level 1 packets only.

level-2

Specifies Level 2 packets only.

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

This example specifies that SPF calculations can be performed without clearing the IS-IS database for Level 2 packets.

```
device# clear isis force-spf level-2
```

clear isis force-v6spf

Performs the IPv6 shortest path first (SPF) calculation without clearing the IS-IS database.

Syntax

clear isis force-v6spf [**level-1** | **level-2**]

Parameters

level-1

Specifies Level 1 packets only.

level-2

Specifies Level 2 packets only.

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

This example specifies that IPv6 SPF calculations can be performed without clearing the IS-IS database for Level 1 packets.

```
device# clear isis force-v6spf level-1
```

clear isis ipv6 spf-log

Clears IPv6 IS-IS SPF logs.

Syntax

clear isis ipv6 spf-log [**level-1** | **level-2**]

Parameters

level-1

Specifies Level 1 packets only.

level-2

Specifies Level 2 packets only.

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

This example clears IPv6 IS-IS logs for Level 1 packets.

```
device# clear isis ipv6 spf-log level-1
```

clear isis neighbor

Clears IS-IS neighbors.

Syntax

clear isis neighbor { **lsp-id** | **all** } [**ethernet** *slot/port* | **ve** *vlan_id*]

Parameters

lsp-id

Specifies a link-state packet (LSP) n HHHH.HHHH.HHHH.HH-HH format or by entering a name, HH-HH.

all

Specifies all neighbors.

ethernet *slot* **/** *port*

Specifies an Ethernet slot and port.

ve *vlan_id*

Specifies a virtual Ethernet (VE) interface.

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

This example clears IS-IS neighbors, specifying a LSP name of “XMR.00-00”.

```
device# clear isis neighbor XMR-1.00-00
```

This example clears all IS-IS connections for a specified Ethernet interface.

```
device# clear isis neighbor all ethernet 1/1
```

This example refreshes all IS-IS neighbors.

```
device# clear isis neighbor all
```

clear isis route

Clears IS-IS routes.

Syntax

clear isis route { *ip-address* | *ip-address/mask* | **all** }

Parameters

ip-address

Clears all routes that match the prefix that you specify.

ip-address/mask

Clears all routes that match the prefix and mask that you specify.

all

Specifies all routes.

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

This example clears IS-IS routes that match the IP address 10.1.1.1.

```
device# clear isis route 10.1.1.1
```

This example clears all IS-IS routes.

```
device# clear isis route all
```

clear isis spf-log

Clears IPv4 IS-IS SPF logs.

Syntax

clear isis spf-log [**level-1** | **level-2**]

Parameters

level-1

Specifies Level 1 packets only.

level-2

Specifies Level 2 packets only.

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

This example clears IPv4 IS-IS logs for Level 2 packets.

```
device# clear isis spf-log level-2
```

clear isis traffic

Clears IS-IS packet counters.

Syntax

clear isis traffic

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

This example clears IS-IS packet counters.

```
device# clear isis traffic
```

clear lacp

Clears the Link Aggregation Group Control Protocol (LACP) counters on a specific port-channel.

Syntax

clear lacp *number* **counters**

Parameters

number

Specifies the port channel-group number.

counters

Clears traffic counters.

Modes

Privileged EXEC mode

Examples

To clear the LACP counters for a specific port-channel:

```
device# clear lacp 10 counters
```

clear lacp counters

Clears the Link Aggregation Group Control Protocol (LACP) counters on all port-channels.

Syntax

clear lacp counters

Modes

Privileged EXEC mode

Examples

To clear the counters for all port-channels:

```
device# clear lacp counters
```

clear link-oam statistics

Clears the Link OAM statistics.

Syntax

clear link-oam statistics

Modes

Privileged EXEC mode

Examples

This example shows how to clears the Link OAM statistics.

```
device# clear link-oam statistics
```

clear lldp neighbors

Clears the Link Layer Discovery Protocol (LLDP) neighbor information on all or specified ethernet interfaces.

Syntax

clear lldp neighbors [**interface ethernet** *slot/port*]

Parameters

ethernet

Use this parameter to specify an ethernet interface, followed by the slot or port number.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

If the **interface** parameter is not specified, this command clears the LLDP neighbor information received on all the interfaces.

Examples

To clear the LLDP neighbor information for all interfaces:

```
device# clear lldp neighbors
```

To clear LLDP neighbor information on a specific ethernet interface:

```
device# clear lldp neighbors interface ?
Possible completions:
ethernet   Ethernet interface
device# clear lldp neighbors interface ethernet ?
Description: The list of Ethernet interfaces.
Possible completions:
  1/1
  1/2
  1/3
  1/4
  1/5
  1/6
```

```
  1/8
  1/9
  1/10
  1/11
  1/12
  1/13
  1/14
  1/15
  1/16
  1/17
  1/18
  1/19
  1/20
  1/21
  1/22
  1/23
  1/24
  1/25
  1/29
  1/30
  1/31
device# clear lldp neighbors interface ethernet 1/24
device#
```

clear lldp statistics

Clears LLDP statistics for all interfaces or a specified Ethernet interface.

Syntax

clear lldp statistics [**interface ethernet** *slot/port*]

Parameters

ethernet

Use this parameter to specify an ethernet interface, followed by the slot or port number.

slot

Specifies a valid slot number. For devices that do not support linecards, specify **0**.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

If the **interface** parameter is not specified, this command clears all the LLDP statistics on all interfaces.

Examples

To clear all the LLDP statistics for all interfaces:

```
device# clear lldp statistics
```

To clear LLDP neighbor information on a specific ethernet interface:

```
device# clear lldp statistics interface ?
Possible completions:
ethernet   Ethernet interface
device# clear lldp statistics interface ethernet ?
Description: The list of Ethernet interfaces.
Possible completions:
  0/1
  0/2
  0/3
  0/4
  0/5
  0/6
  0/8
  0/9
```

```
  0/10
  0/11
  0/12
  0/13
  0/14
  0/15
  0/16
  0/17
  0/18
  0/19
  0/20
  0/21
  0/22
  0/23
device#clear lldp statistics interface ethernet 0/23
device#
```

clear logging raslog

Clears RASLog messages from the router.

Syntax

clear logging raslog [**message-type** { **DCE** | **SYSTEM** }]

Command Default

Clear all RASLog messages on the local router.

Parameters

message-type

Clears RASLog messages of the specified repository type.

SYSTEM

Clears system LOG messages.

DCE

Clears DCE application messages.

Modes

Privileged EXEC mode

Usage Guidelines

This command clears all RASLog messages by default.

SLX-OS maintains two separate internal message storage repositories, SYSTEM and DCE. A RASLog message can have one or more type attributes. For example, a message can be of type DCE, FFDC, and AUDIT.

Note
A message cannot have both LOG and DCE type attributes. LOG type messages are stored in the SYSTEM message-type repository and DCE type messages are stored in the DCE message-type repository. LOG type messages are not stored in the DCE message-type repository and DCE type messages are not stored in the SYSTEM message-type repository.

Examples

To clear all RASLog messages:

```
device# clear logging raslog

DCE Raslogs are cleared
SYSTEM Raslogs are cleared
```

To clear all messages from the DCE message-type repository:

```
device# clear logging raslog message-type DCE

DCE Raslogs are cleared
```

To clear all messages from the SYSTEM message-type repository:

```
device# clear logging raslog message-type SYSTEM

SYSTEM Raslogs are cleared
```

clear loop-detection

Enables ports that were disabled by the loop detection (LD) protocol, and clears LD statistics at the global, interface, or VLAN level.

Syntax

clear loop-detection [**interface** { **ethernet** *interface* | **port-channel** *interface* } | **vlan** *vlan-id*]

Command Default

This feature is disabled.

Parameters

interface

Specifies an Ethernet or port-channel interface.

ethernet*interface*

Specifies an Ethernet interface.

port-channel*interface*

Specifies a port-channel interface.

vlan *vlan-id*

Specifies a VLAN.

Modes

Privileged EXEC mode

Examples

To enable LD-disabled ports and clear LD statistics on all interfaces:

```
device# clear loop-detection
```

To enable LD-disabled ports and clear LD statistics on an Ethernet interface:

```
device# clear loop-detection interface ethernet 2/6
```

To enable LD-disabled ports and clear LD statistics on a port-channel interface:

```
device# clear loop-detection interface port-channel 20
```

To enable LD-disabled ports and clear LD statistics on a VLAN:

```
device# clear loop-detection interface vlan 10
```

clear loop-detection bridge-domain

Enables ports associated with the bridge domain (BD) that were disabled as part of loop detection, and also clears the LD statistics per BD.

Syntax

clear loop-detection bridge-domain *BD_ID*

Command Default

None

Parameters

BD_ID

Specifies a BD.

Modes

Privileged EXEC mode

Examples

The following example enables ports associated with BD 8 and clears LD statistics for that BD.

```
device# clear loop-detection bridge-domain 8
```

clear mac-address-table

Removes interface entries from the MAC address table.

Syntax

clear mac-address-table { **cluster** *cluster-id* [**client** [*client-id*]] }

clear mac-address-table dynamic [**address** *mac-address* | **bridge-domain** [*id*] | **interface ethernet** *slot/port* | **port-channel** *number* | **logical-interface ethernet** *slot/port* [*:brk-out*]*. lif-id* | **vlan** *vlan-id*]

clear mac-address-table mac-move [**shut-list**]

Parameters

bridge-domain

Specifies clearing MAC addresses learned under a bridge domain.

id

Specifies a bridge-domain identifier.

cluster *cluster-id*

Specifies clearing MAC addresses from an MCT cluster ID. The ID range is 1 - 65535.

client *client-id*

Specifies clearning the client instance. Specify the client ID with a maximum of 64 characters.

dynamic address *MAC-address*

Specifies clearning the dynamic MAC address. The valid format is *H.H.H* (available in Privileged EXEC mode only).

interface ethernet *slot/port*

Specifies clearning the ethernet interface with a valid slot number/port number.

port-channel *number*

Specifies clearning the port channel interface number.

logical-interface ethernet *slot/port* [*:brk-out*]*. lif-id*

Specifies clearning the logical ethernet interface on a specified slot/port number. The breakout interface option can be used with the LIF ID.

vlan *vlan id*

Specifies clearning the VLAN interface. The VLAN ID range is from 1 - 4090.

shut-list

Specifies clearning the interfaces from the shutdown list.

Modes

Privileged EXEC mode.

Usage Guidelines

When a bridge-domain identifier is not specified, MAC addresses learned under all bridge domains are removed from the MAC address table. If a specific address is not specified, all dynamic mac-addresses are deleted from the MAC address table.

Examples

The following example shows how to clear MAC addresses learned under bridge domain 1 from the MAC address table.

```
device# clear mac-address-table dynamic bridge-domain 1
```

The following example shows how to clear MAC addresses learned from vlan 1 from the MAC address table.

```
device# clear mac-address-table dynamic vlan 1
```

The following example shows how to clear MAC addresses from a logical interface ethernet 3/10 LIF breakout interface.

```
device# clear mac-address-table dynamic 3/10:5.200
```

clear mpls auto-bandwidth-samples

Deletes the sample-history from the auto-bandwidth LSPs.

Syntax

clear mpls auto-bandwith-samples [**lsp** *lsp_name* **| all**]

Parameters

lsp *lsp_name*

The lsp option clears the auto-bandwidth sample history for the LSP specified through the *lsp_name*.

all

Clears all the auto-bandwidth sample history.

Modes

Privileged EXEC mode

Usage Guidelines

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example clears the sample history for *LSP1*.

```
device# auto-bandwidth-samples lsp lsp1
```

clear mpls lsp

Allows the user to reset normal LSPs. The user has the option of supplying the primary or secondary parameter for a normal LSP to reset only the primary or secondary path of the LSP.

Syntax

clear mpls lsp *lsp_name* [**primary** | **secondary**]

Parameters

lsp_name

Specifies the target LSP by name.

primary

Specifies that the primary LSP path associated with the *lsp_name* is reset and restarted.

secondary

Specifies that the secondary LSP path associated with the *lsp_name* is reset and restarted.

Modes

Privileged EXEC mode

Usage Guidelines

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

When the user resets an LSP with the clear mpls lsp command, the following information message is displayed.

```
"Disconnecting signaled LSP name"
"Connecting signaled LSP name"
```

clear mpls statistics

Clears the MPLS statistics.

Syntax

clear mpls statistics oam

clear mpls statistics { **transit** [**label** *label* | **ldp** [*ip_addr* | *submask* | *label*] | **rsvp** *label*] }

clear mpls statistics { **tunnel** [**destination** *ip_addr* | **index** *vif_index* | **ldp** [**destination** *ip_addr* | **index** *vif_index*] | **rsvp** [**destination** *ip_addr* | **index** *vif_index* | **name** *name*]] }

Parameters

oam

Clears the MPLS OAM statistics.

transit

Clears the MPLS transit statistics.

label *label*

Clears the MPLS transit statistics for the selected label.

ldp *ip_addr*

Clears the MPLS transit LDP statisticsfor the selected IP address.

rsvp

Clears the MPLS transit RSVP statistics .

tunnel

Clears the MPLS tunnel statistics.

destination *destination*

Clears the MPLS tunnel statistics for the selected tunnel destination.

index *vif_index*

Clears the MPLS tunnel statistics for the selected tunnel index.

ldp

Clears the MPLS tunnel LDP statistics.

destination *destination*

Clears the MPLS tunnel statistics for the selected tunnel destination.

index *vif_index*

Clears the MPLS tunnel statistics for the selected tunnel index.

rsvp

Clears the MPLS tunnel RSVP statistics.

destination *destination*

Clears the MPLS tunnel statistics for the selected tunnel destination.

index *vif_index*

Clears the MPLS tunnel statistics for the selected tunnel index.

name *name*

Clears the MPLS tunnel statistics for the selected named tunnel.

Modes

MPLS policy mode

Usage Guidelines

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example clears the MPLS statistics.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-mpls-policy)# clear mpls statistics
```

clear mvrp statistics

Clears the MVRP statistics for all Ethernet and port-channel interfaces, or for a specific Ethernet or port-channel interface.

Syntax

clear mvrp statistics [**interface** { **ethernet** *slot/port* | **port-channel** *number* }]

Parameters

interface

Clears the MVRP statistics for a specific interface.

ethernet *slot/port*

Specifies an Ethernet interface.

port-channel *number*

Specifies the port-channel interface.

Modes

Privileged EXEC mode

Usage Guidelines

If you enter this command without any options, the MVRP statistics for all Ethernet and port-channel interfaces are cleared.

This feature is supported on the SLX 9250, SLX 9540, SLX 9640, SLX 9740, Extreme 8520, and Extreme 8820 devices.

Examples

The following command clears the MVRP statistics for all Ethernet and port-channel interfaces.

```
device# clear mvrp statistics
```

The following command clears the MVRP statistics for a specified Ethernet interface.

```
device# clear mvrp statistics interface ethernet 0/1
```

clear overlay-gateway

Clear counters for the specified gateway.

Syntax

clear overlay-gateway *name* { **statistics** | **vlan statistics** }

Parameters

name

Specifies the name of the VXLAN gateway profile.

statistics

Clears all statistics for the VXLAN gateway.

vlan statistics

Clears per-VLAN statistics for the VXLAN gateway.

Modes

Privileged EXEC mode

Usage Guidelines

If you specify the VXLAN gateway name, the gateway must already be configured.

If you specify VLAN IDs, these VLANS must already be configured as exported VLANs for the gateway.

Examples

The following example clears all counters for the already configured VXLAN gateway named gateway1.

```
device# clear overlay-gateway gateway1 statistics
```

clear policy-map-counters

Clears the policy map counters.

Syntax

```
clear policy-map-counters [ control-plane [ policy-map-name ]]|
   [ interface ethernet slot/port ] [ in | out ]
```

Parameters

control-plane [*policy-map-name*]

Clears the control-plane policy map counters. You can optionally enter the name of the policy-map name.

interface

Specifies an interface.

ethernet

Represents a valid, physical Ethernet type for all available Ethernet speeds.

slot/port

Specifies a slot and port number.

in

Specifies clearing the ingress counters.

out

Specifies clearing the egress counters.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **clear policy-map-counters** command without any keyword options to clear all of the policy map counters.

Examples

To clear the control-plane policy map counters, use the following command:

```
device# clear policy-map-counters control-plane
```

To clear the policy map counters for a specific interface use the following command:

```
device# clear policy-map-counters interface ethernet 2/2
```

clear qos flowcontrol statistics

Clears flow control statistics for a specific interface, port channel, or all interfaces on the device.

Syntax

clear qos flowcontrol statistics { **all** | **ethernet** *slot/port* | **port-channel** *number* }

Parameters

all

Clears the flow control statistics on all interfaces in the device.

ethernet *slot/port*

Clears the flow control statistics on the specified interface.

port-channel *number*

Clears the flow control statistics on the interface for the specified port channel.

Modes

Privileged EXEC mode

Examples

The following example clears the flow control statistics for all interfaces, as displayed by the **show qos flowcontrol interface** command.

```
device# clear qos flowcontrol statistics interface all
```

clear spanning-tree counter

Clears all spanning-tree counters on an Ethernet or port-channel interface.

Syntax

clear spanning-tree counter [**interface** { **ethernet** *slot/port* | **port-channel** *number* }]

Parameters

interface

Specifies an interface.

ethernet

Specifies an Ethernet interface.

slot

Specifies a valid slot number. Must be 0 if the switch does not contain slots.

port

Specifies a valid port number.

port-channel *number*

Specifies a port-channel.

Modes

Privileged EXEC mode

Usage Guidelines

If the **interface** parameter is not specified, spanning-tree counters are cleared for all interfaces.

Examples

To clear spanning-tree counters for all interfaces:

```
device# clear spanning-tree counter
```

To clear spanning-tree counters for an Ethernet interface:

```
device# clear spanning-tree counter interface ethernet 0/1
```

To clear spanning-tree counters for port-channel 23:

```
device# clear spanning-tree counter interface port-channel 23
```

clear spanning-tree detected-protocols

Clears all spanning-tree detected protocols on an Ethernet or port-channel interface.

Syntax

clear spanning-tree detected-protocols [**interface** { **ethernet** *slot/port* | **port-channel** *number* }]

Parameters

interface

Specifies an interface.

ethernet

Specifies an Ethernet interface.

slot

Specifies a valid slot number. Must be 0 if the switch does not contain slots.

port

Specifies a valid port number.

port-channel *number*

Specifies a port-channel.

Modes

Privileged EXEC mode

Usage Guidelines

If the **interface** parameter is not specified, spanning-tree detected protocols are cleared for all interfaces.

Examples

To clear detected protocols on all interfaces:

```
device# clear spanning-tree detected-protocols
```

To clear detected protocols on an Ethernet interface:

```
device# clear spanning-tree detected-protocols interface ethernet 0/1
```

To clear detected protocols on port-channel 23:

```
device# clear spanning-tree detected-protocols interface port-channel 23
```

clear statistics bridge-domain

Clears the statistics for all the logical interfaces on bridge domains.

Syntax

clear statistics bridge-domain *bd-id*

Parameters

bd-id

The bridge domain ID.

Command Default

Statistics are disabled.

Modes

Privileged EXEC mode

Usage Guidelines

This command is also available in global configuration mode.

The **clear statistics bridge-domain bd-id** command clears the statistics for all the logical interfaces on a specific bridge domain.

Examples

The following example shows how to clear the statistics for all the logical interfaces on all bridge domains.

```
device# clear statistics bridge-domain
```

The following example shows how to clear the statistics for all the logical interfaces on bridge domain 1.

```
device# clear statistics bridge-domain 1
```

clear statistics vlan

Clears the statistics for all the ports and port channels on configured VLANs.

Syntax

clear statistics vlan vlan-id

Parameters

vlan-id

The specific VLAN ID.

Command Default

Statistics are disabled.

Modes

Privileged EXEC mode

Usage Guidelines

This command is also available in global configuration mode.

The **clear statistics vlan vlan-id** command clears the statistics for all the ports and port channels on the given VLAN.

Examples

The following example shows how to clear the statistics for all the ports and port channels on the given VLAN.

```
device# clear statistics vlan
```

The following example shows how to clear the statistics for all the ports and port channels on VLAN 10.

```
device# clear statistics vlan 10
```

clear tm voq-stat ingress-device

Clears the traffic management VOQ statistics on the ingress device for a specified Ethernet port, or for all ports.

Syntax

clear tm voq-stat ingress-device ethernet *slot/port* **egress-port** { **ethernet** *slot/port* | **all** }

clear tm voq-stat ingress-device all egress-port { **ethernet** *slot/port* | **all** }

Parameters

ethernet *slot/port*

Specifies the Ethernet interface in slot/port format.

egress-port ethernet *slot/port*

Specifies clearing the traffic management statistics on the egress Ethernet slot/port.

all

Specifies clearing the traffic management statistics for all ports.

Modes

Privileged EXEC mode

Examples

To clear VOQ statistics information on the egress-port for Ethernet 0/1, use the following command.

```
device# clear tm voq-stat ingress-device ethernet 0/1 egress-port ethernet 0/1
```

To clear all VOQ statistics information on the egress-port for Ethernet 0/1, use the following command.

```
device# clear tm voq-stat ingress-device all egress-port ethernet 0/1
```

clear tm voq-stat slot

Clears the traffic management VOQ (virtual output queuing) statistics for one or all CPU group or one or all egress ports.

Syntax

clear tm voq-stat slot *line-card-number* **cpu-group** { **all** | *cpu-group-id* }

clear tm voq-stat slot *line-card-number* **egress-port** { **all** | **ethernet** *slot/port* }

Parameters

line-card-number

Specifies the line card slot. For devices without line cards, specify `0`.

cpu-group *cpu-group-id*

Specifies the ID number for the CPU group.

egress-port

Specifies an Ethernet egress port.

ethernet *slot/port*

Specifies the Ethernet interface in slot/port format.

all

Specifies clearing the traffic management statistics for all CPU groups or all egress ports.

Modes

Privileged EXEC mode

Examples

The following example clears information about the VOQ for the line card in slot 0 CPU group 1.

```
device# clear tm voq-stat slot 0 cpu-group 1
```

clear tunnel statistics

Clears statistics from the tunnel interfaces.

Syntax

clear tunnel statistics *tunnel-id*

Parameters

tunnel-id

Specifies the tunnel ID.

Modes

Privileged EXEC mode

Examples

This example removes statistics from a tunnel interface.

```
device# clear tunnel statistics 10
```

clear udld statistics

Clears UDLD statistics.

Syntax

clear udld statistics[**interface** { **ethernet** *slot*/*port* }]

Parameters

interface

Specifies an interface.

ethernet *slot port*

Specifies a valid, physical Ethernet interface with a slot and port number.

Modes

Privileged EXEC mode

Usage Guidelines

Clears either all unidirectional link detection (UDLD) protocol statistics or clears the statistics on a specified port.

Examples

To clear UDLD statistics on a specific interface:

```
device# clear udld statistics interface 0/1
```

clear vrrp statistics

Clears VRRP statistics.

Syntax

clear vrrp statistics

clear vrrp statistics [**interface** { **ethernet** *slot*/*port* | **ve** *vlan_id* }]

clear vrrp statistics session *VRID*

Parameters

interface

Specifies an interface.

ethernet *slot port*

Specifies a valid, physical Ethernet interface with a slot and port number.

ve *vlan_id*

Specifies the VE VLAN number. The range is from 1 through 6144.

session *VRID*

Specifies the virtual group ID on which to clear statistics. The range is from 1 through 255.

Modes

Privileged EXEC mode

Usage Guidelines

This command clears VRRP session statistics for all virtual groups, for a specified interface or for a specified virtual group.

This command is for VRRP and VRRP-E. VRRP-E supports only the **ve** *vlan_id* interface type.

To clear all vrrp statistics, use the **clear vrrp statistics** command with no operands.

Examples

The following example clears all VRRP statistics for all virtual groups.

```
device# clear vrrp statistics
```

The following example clears statistics for Ethernet interface 1/6.

```
device# clear vrrp statistics interface ethernet 1/6
```

The following example clears statistics for a session for a VRRP virtual group called "vrrp-group-25".

```
device# clear vrrp statistics session 25
```

The following example clears VRRP statistics on a specified virtual Ethernet (VE) interface.

```
device# clear vrrp statistics interface ve 10
```

CLI

In a Python shell, runs a device CLI command or series of commands. You can also assign the output of such commands to a Python object.

Syntax

```
CLI (' device-CLI-command ' [ \n ' device-CLI-command ' ] [ [ do_print
   = ] { True | False } ] )
```

Parameters

device-CLI-command

An SLX-OS CLI command. You separate additional commands with **\n**.

do_print =

Specify whether or not to print the output of *device-CLI-command* to the default device. The default is to print the output.

True

Print the output.

False

Do not print the output.

Modes

Python command shell

Usage Guidelines

Divergences between the CLI syntax and Python syntax include the following differences:

- Although in general, the CLI syntax is not case-sensitive, our convention is to use lower-case.
- Python syntax is case sensitive. Regarding the syntax documented in the current topic, note the following:
  - The syntax of the command is upper case (CLI) and not lower case (cli).
  - The syntax of the **do_print =** options is to capitalize the first letter: { **True** | **False** }

In Python, double quotes (") and single quotes (') are equivalent.

As delimiter between multiple CLI commands, use \n.

There is a difference between running a sequence of SLX-OS CLI commands in the Python shell rather than in the standard SLX-OS interface. Whereas in the standard interface the result of a command is persistent, in the Python shell each CLI( ) statement is independent of any preceding ones.

For support of the `CLI( )` command, although a Python script must include a `from CLI import CLI` statement, this statement is automatically implemented when launching the Python interpreter interactively.

Within a script or interactive session, if you assign a CLI command or series of commands to a Python variable, you can then append the following functions to the variable:

- **`.rerun()`**—updates the variable from a new run of the CLI command or series of commands.

```
device# python
Python 3.5.2 (default, Apr 11 2019, 13:05:18)
[GCC 4.8.2] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> cmd_show_running_ve = CLI('show running-config interface ve')
!Command: show running-config interface ve
!Time: Mon Aug 22 16:53:13 2016

% No entries found.
# The SLX-OS show running-config interface ve command is run,
# and that command is assigned to the Python variable cmd_show_running_ve.

>>> cmd_config_ve = CLI('configure \n interface ve 101-103')
# A series of three commands are run and assigned to the Python variable cmd_config_ve.
!Command: configure
 interface ve 101-103
!Time: Mon Aug 22 16:53:13 2016


>>> cmd_show_running_ve.rerun()
# The rerun() function appended to cmd_show_running_ve gives the following output:
!Command: show running-config interface ve
!Time: Mon Aug 22 16:53:13 2016

interface Ve 101
 shutdown
!
interface Ve 102
 shutdown
!
interface Ve 103
 shutdown
!
!
```

- **`.get_output()`**—returns the value of a new run of the CLI command or series of commands, as a list. Running this script displays the "Firmware name" line of the **`show version`** command.

```
#Required in all scripts for SLX:
from CLI import CLI

# Import the Python Regular Expressions (re) module:
import re

# Create Python objects:
slot_firmware = {}
cmd_show_ver = CLI("show ver", False)

# Using .get_output(), assign the result of show ver to a Python object named output:
output = cmd_show_ver.get_output()
```

```
for line in output:
    found = re.search(r'^(Firmware name:)\s+(\S+)$', line, re.M)
    if found:
        slot_firmware[found.group(1)] = found.group(2)

print("FIRMWARE:\n")
for key in slot_firmware:
    print("\t", key, "\t=> ", slot_firmware[key])
```

Examples

The following example launches the Python shell and then both assigns a series of CLI configuration commands to a Python variable and runs those commands.

```
device# python
Python 3.5.2 (default, Apr 11 2019, 13:05:18)
[GCC 4.8.2] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> cmd_config_ve = CLI('configure \n interface ve 101-103')
!Command: configure
 interface ve 101-103
!Time: Mon Aug 22 16:57:36 2016
>>>
```

The following example launches the Python shell and then both assigns a CLI operational command (**`reload system`**) to a Python variable and runs that command.

```
device# python
Python 3.5.2 (default, Apr 11 2019, 13:05:18)
[GCC 4.8.2] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> cmd_reload_system = CLI('reload system \n y')
```

client

Configures a Multi-Chassis Trunking (MCT) client for a cluster and access cluster client configuration mode.

Syntax

client *client-name client-id*

no client *client-name client-id*

Parameters

client-name

Specifies the client name as an ASCII string. The name can be up to 64 characters in length.

client-id

Specifies the cluster client ID. The ID value range can be from 1 through 512.

Modes

Cluster client configuration mode

Usage Guidelines

On both MCT nodes, you must configure the same client ID.

The **no** form of the command removes the client from the MCT cluster configuration.

Examples

The following example configures a cluster client.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# client MCT1-client 200
device(config-cluster-client-200)#
```

client-interface

Configures a CEP or CCEP interface to the cluster client instance.

Syntax

client-interface { **ethernet** *slot/port* | **port-channel** *number* }

no client-interface

Parameters

ethernet *slot/port*

Configures the specified Ethernet port as the client CEP or CCEP.

port-channel *number*

Configures the specified port channel as the client CEP or CCEP. The port channel *number* specifies the LAG ID.

Modes

Cluster client configuration mode

Usage Guidelines

The **no** form of the command removes the client interface.

The same client interface cannot be added under multiple client entries.

A client interface is not allowed to be updated when the client is in deploy state. It needs to be removed first before adding a new interface.

Examples

The following example shows how to configure a client interface.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# client MCT1-client 200
device(config-cluster-client-200)# client-interface port-channel 3
```

client-interface (Y1731)

Associates either a physical interface or a port-channel interface to a Y1731 Maintenance Entity Group End Point (MEP) as a client interface.

Syntax

client-interface { **ethernet** *slot/port* [*:subport*] | **port-channel** *number* }
csf-type { **loss-of-signal** } **tx-period** [**1-minute** | **1-second**]

no client-interface { **ethernet** *slot/port* [*:subport*] | **port-channel** *number* }

Command Default

This command has no defaults.

Parameters

ethernet *slot/port*

Specifies an Ethernet slot and port with optional subport.

port-channel *number*

Specifies a port-channel.

csf-type loss-of-signal

Specifies the Client Signal Failure (CSF) type as C-LOS (the currently supported option).

tx-period

Specifies a transmission period. The following options are currently supported.

1-minute

Specifies 1 minute.

1-second

Specifies 1 second.

Modes

MEP configuration mode

Usage Guidelines

This command associates an Ethernet Client Signal Fail (ETH-CSF) client interface to an MEP and configures a transmission-period for the ETH-CSF frames to be transmitted towards the peer Remote MEP (RMEP).

Use the **no** form of this command to remove the association of the client interface with the MEP.

Examples

This example specifies a client interface on Ethernet interface 1/2 with CSF type C-LOS and transmission period of 1 minute for Down MEP 1 in MD md1 and MA ma1.

```
device# configure terminal
Entering configuration mode terminal
device(config)# protocol cfm
device(config-cfm)# domain-name md1 id 1 level 3
device(config-cfm-md-md1)# ma-name ma1 id 1 vlan 10 priority 7
device(config-cfm-md-ma-ma1)# mep 1 down ethernet 1/1
device(config-cfm-md-ma-mep-1)# client-interface ethernet 1/2 csf-type loss-of-signal tx-
period 1-minute
```

This example removes the association of the client interface with the MEP.

```
device(config-cfm-md-ma-mep-1)# no client-interface ethernet 1/2
```

client-interfaces-shutdown

Disables the local client interfaces administratively in the cluster to move all traffic on the device to a remote MCT peer device, resulting in failover of traffic to the peer device.

Syntax

client-interfaces shutdown

no client-interfaces shutdown

Modes

Cluster configuration mode

Usage Guidelines

You can use this command to move traffic to a peer device when you are upgrading the local client interfaces.

The **no** form of the command reenables the local client interfaces.

Examples

The following example shows the disabling of all the client interfaces in the cluster.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# client-interfaces shutdown
```

client-pw

Configures the pseudowire (PW) client for an MCT cluster used with VPLS or VLL and access cluster client PW configuration mode.

Syntax

client-pw

no client-pw

Modes

Cluster configuration mode

Usage Guidelines

This command is not supported on the SLX 9150 or SLX 9250 devices.

Only one instance of the PW client represents all VPLS or VLL PWs over all bridge domains.

The **no** form of the command removes the PW client from the MCT cluster configuration.

Examples

The following example configures a cluster client.

```
device# configure terminal
device(config)# cluster MCT1 1
device(config-cluster-1)# client-pw
device(config-cluster-client-pw)#
```

client-to-client-reflection

Enables routes from one Route Reflector (RR) client to be reflected to other clients by the host device on which it is configured.

Syntax

client-to-client-reflection

no client-to-client-reflection

Command Default

Enabled

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family L2VPN EVPN configuration mode

Usage Guidelines

When this command is used, the host device on which it is configured becomes the route-reflector server.

The **no** form of the command disables route reflection between clients.

Examples

The following example configures client-to-client reflection on the BGP host device for the IPv4 unicast address-family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# client-to-client-reflection
```

The following example disables client-to-client reflection on the BGP host device for the IPv6 unicast address-family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# no client-to-client-reflection
```

The following example configures client-to-client reflection in L2VPN EVPN configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# client-to-client-reflection
```

clock set

Sets the local clock time and date.

Syntax

clock set *hh:mm:ss mm-dd-yy/yyyy*

Parameters

hh:mm:ss

Specifies the local clock time in hours, minutes, and seconds.

mm-dd-yy/yyyy

Specifies the local clock date in month, day, and year format. Year may be specified with two or four numbers.

Modes

Privileged EXEC mode

Usage Guidelines

Valid date and time settings range from January 1, 1970 to December 31, 2035.

An active NTP server, if configured, automatically updates and overrides the local clock time.

Examples

The following example sets the time and date to 31 minutes past 4 pm in the afternoon on July 28, 2016, for the local device:

```
device# clock set 16:31:35 07-28-16
```

clock timezone

Sets the device system clock time zone options using either Greenwich Mean time (GMT) or one of the US time zones that uses Universal Time Coordinated (UTC) plus or minus a number of hours.

Syntax

clock timezone { **gmt** *gmt-time* | **us** *us-time* }

no clock timezone { **gmt** *gmt-time* | **us** *us-time* }

Parameters

gmt *gmt-time*

Specifies the GMT time zone. The value can be one of the following: gmt+00 (United Kingdom), gmt+01 (France, Germany), gmt+02 (Eastern Europe, South Africa), gmt+03, gmt+03:30, gmt+04, gmt+04:30, gmt+05, gmt+05:30 (India), gmt+06, gmt+06:30, gmt+07, gmt+08 (China, Hong Kong, Taiwan), gmt+09 (Japan, Korea), gmt+09:30, gmt+10 (Australia), gmt+10:30, gmt+11, gmt+11:30, gmt+12, gmt-01, gmt-02, gmt-03, gmt-03:30, gmt-04, gmt-05, gmt-06, gmt-07, gmt-08, gmt-08:30, gmt-09, gmt-09:30, gmt-10, gmt-11, gmt-12.

us *us-time*

Specifies the US time zone. The value can be one of the following: alaska, aleutian, arizona, central, east-indiana, eastern, hawaii, michigan, mountain, pacific, samoa.

Modes

Global configuration mode

Examples

The following example sets the system date and time to the US Samoa time zone.

```
device(config)# clock timezone us samoa
```

cluster

Configures a Multi-Chassis Trunking (MCT) cluster and access the cluster configuration mode.

Syntax

cluster *cluster-name*

no cluster *cluster-name*

Parameters

cluster-name

Specifies the cluster name as an ASCII string. The cluster name can be up to 64 characters in length.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command removes the MCT cluster configuration.

Examples

The following example configures an MCT cluster.

```
device(config)# cluster MCT1
device(config-cluster-MCT1)#
```

cluster-client auto

Configures a Multi-Chassis Trunking (MCT) client for a cluster in auto mode.

Syntax

cluster-client { <NUMBER:1-1000> | auto}

no cluster-client

Parameters

Number

The user can use any client ID between 1 to 1000.

auto

Client ID will be derived as 1000+Port-channel number.

Modes

Port-channel mode.

Usage Guidelines

On both MCT nodes, you must configure the same client ID (either auto/client-id). The no form of the command removes the client from the MCT cluster configuration.

Examples

The following example configures a cluster-client auto.

```
device# configure terminal
device(config)# interface Port-channel 10
device(config-Port-channel-10)#cluster-client auto
          (or)
device# configure terminal
device(config)# interface Port-channel 30
device(config-Port-channel-30)# cluster-client 325
```

```
device# show cluster
Cluster c1
================
Cluster State: Active
Bringup Delay: 90 seconds
Configured Member Vlan Range: All
Active Member Vlan Range: 1
Configured Member BD Range: All
Active Member BD Range: 501
No. of Clients: 2
Peer Info:
==========
Peer IP: 4.1.1.10, State: Up
Peer Interface: Ethernet 0/4, Source IP: 4.1.1.11
Keep-Alive:
==========
```

```
IP: 10.24.8.220, State: Up
Interface: Management 0 (mgmt-vrf), Source IP: 10.24.8.221
Client-Isolation Role: Primary
```

```
Client Info:
============
Interface               Id              Description          Local/Remote State
Exceptions
 ---------               --              -----------          ------------------
----------
Port-channel 10         1010                                  Up/Up
Port-channel 30         325                                   Up/Up
PW                      34816                                 Up/Up
```

cluster-track

Configures interface to track state of MCT cluster.

Syntax

cluster-track

[no] cluster-track

Parameters

cluster-track

Configures interface to track state of MCT cluster.

Modes

Interface sub-mode

Usage Guidelines

This command helps reduce convergence for reload cases by diverting traffic to alternate paths. The cluster tracked ports are brought down along with MCT clients for these reasons:

1. Maintenance mode is enabled or cluster 'shutdown all.`
2. Peer-interface goes down on the MCT secondary node, while the peer node is up (split-brain).
3. Cluster bring-up is in progress after reload .

Once the cluster status comes up, the cluster tracking interfaces are brought up along with the cluster clients. When none of the above conditions are true, the configuration has no effect on the interface state.

When the interface is disabled due to cluster status, admin shut/no shut on the port has no effect. **[no cluster-track]** removes the cluster-track configuration from the port. This port no longer tracks the status of the MCT cluster.

This command can be configured on L2 or L3 Ethernet or port-channel interfaces. The interface should not be a port channel member and is only valid when cluster configuration is present.

Cluster-track cannot be configured on an interface if it is configured with any of the below:

1. Peer-interface (under cluster)
2. Cluster-client
3. Channel-group
4. Reload-delay enable

Examples

```
SLX(config)# int eth 0/3
SLX(conf-if-eth-0/3)# cluster-track
SLX(conf-if-eth-0/3)# do sh run int eth 0/3
interface Ethernet 0/3
description uplink_spine1
cluster-track
switchport
switchport mode trunk
switchport trunk tag native-vlan
no shutdown

SLX# show interface ethernet 0/3
Ethernet 0/3 is admin down, line protocol is down (Cluster triggered shutdown)
```

commit

Use the **commit** command to commit modifications done to adaptive parameters of a bypass LSP. This command also applies to LSPs. This is not a configuration persistent command; it is a functional command.

Syntax

commit

Command Default

Automatic commit is considered when it is configured to do so in the MPLS global mode.

Modes

MPLS router bypass LSP configuration mode (config-router-mpls-bypass-*lsp_name*).

Usage Guidelines

Once modifying one or more adaptive parameters, the user can commit the changes such that the new instance of the bypass LSP can be brought up. When successful, then a make-before-break switch happens from the current instance of the bypass to the new UP instance.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example shows the configuration for the **commit** command.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# bypass-lsp my-bypass-lsp
device(config-router-mpls-bypass-lsp-my-bypass-lsp)# commit
```

compare-med-empty-aspath

Enables comparison of Multi-Exit Discriminators (MEDs) for internal routes that originate within the local autonomous system (AS) or confederation

Syntax

compare-med-empty-aspath

no compare-med-empty-aspath

Command Default

Disabled.

Modes

BGP configuration mode

Usage Guidelines

The **no** form of the command restores the default.

Examples

The following example configures the device to compare MEDs.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# compare-med-empty-aspath
```

compare-routerid

Enables comparison of device IDs, so that the path-comparison algorithm compares the device IDs of neighbors that sent otherwise equal-length paths.

Syntax

compare-routerid

no compare-routerid

Modes

BGP configuration mode

Examples

The following example configures the device always to compare device IDs.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# compare-routerid
```

confederation identifier

Configures a BGP confederation identifier.

Syntax

confederation identifier *autonomous-system number*

no confederation identifier

Command Default

No BGP confederation identifier is identified.

Parameters

autonomous-system number

Specifies an autonomous system number (ASN). The configurable range of values is from 1 through 4294967295.

Modes

BGP configuration mode

Usage Guidelines

The **no** form of the command removes a BGP confederation identifier.

Examples

The following example specifies that confederation 65220 belongs to autonomous system 100.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 65220
device(config-bgp-router)# confederation identifier 100
```

confederation peers

Configures subautonomous systems to belong to a single confederation.

Syntax

confederation peers *autonomous-system number* [*…autonomous-system number*]

no confederation peers

Command Default

No BGP peers are configured to be members of a BGP confederation.

Parameters

autonomous-system number

Autonomous system (AS) numbers for BGP peers that will belong to the confederation. The configurable range of values is from 1 through 4294967295.

Modes

BGP configuration mode

Usage Guidelines

The **no** form of the command removes an autonomous system from the confederation.

Examples

The following example configures autonomous systems 65520, 65521, and 65522 to belong to a single confederation under the identifier 100.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 65020
device(config-bgp-router)# confederation identifier 100
device(config-bgp-router)# confederation peers 65520 65521 65522
```

configure terminal

Enters global configuration mode.

Syntax

configure terminal

Modes

Privileged EXEC mode

Examples

The following example moves from privileged EXEC mode to global configuration mode.

```
device# configure terminal
Entering configuration mode terminal
device(config)#
```

config-drift-track

Disables configuration drift detection for the current session.

Syntax

config-drift-track off

Parameters

off

Switches off configuration drift detection for the current session.

Modes

Privilege Execution Mode

Usage Guidelines

Configuration drift detection is turned off for the current session when this command is executed. Any configuration changes made after turning off drift detection is not tracked by SLX.

Configuration drift detection is enabled by default for all sessions. It must be explicitly turned off for a session to prevent SLX from tracking configuration changes made in that session.

Examples

The following example shows how to switch off the configuration drift tracking feature.

```
SLX# config-drift-track off
```

connector

Accesses connector configuration mode for the ports that support the breakout feature and the insight port feature.

Syntax

connector 0/*port*

Parameters

0/*port*

Specifies a valid port number on the device that supports breakout mode or insight mode.

Modes

Hardware configuration mode

Usage Guidelines

In connector configuration mode, you can break out the port that supports the breakout feature into four 10G or 25G breakout interfaces, or you can enable or disable the port that supports the insight port feature.

Examples

This example shows how to access the connector configuration mode on a supported port on SLX 9640.

```
device# configure terminal
device(config)# hardware
device(config-hardware)# connector 0/25
```

control-word

Enables control word for a pseudowire (PW) profile.

Syntax

control-word

no control-word

Command Default

By default, control word is disabled for PW profiles.

Modes

Pseudowire profile configuration mode

Usage Guidelines

The **no** form of the command disables control word for a PW profile.

For a PW that is sensitive to packet misordering to operate correctly, all packets in the PW must follow the same path over a Multi-Protocol Label Switched (MPLS) packet switched network (PSN).

PW control word is a mechanism that prevents packet misordering. Without the control word mechanism, a label switching router (LSR) performing, for example, equal-cost multiple-path load-balancing (ECMP) could mistake a PW payload for an IPv4 or IPv6 packet and route it over a different path, resulting in misordered packet delivery to the egress provider edge (PE) device.

When control word is enabled, LSRs use it to distinguish a specific PW payload from an IP payload and ensure that all packets for the PW follow the same path over the MPLS PSN.

Note
When control word is enabled for a previously configured PW, control word capabilities between PE devices are activated only after LDP neighbors are cleared by using the **clear mpls ldp neighbor** command. For further information on clearing LDP neighbors, refer to *Extreme SLX-OS MPLS Configuration Guide*.

Examples

The following example shows how to enable PW control word for a PW profile named pw_example

```
device# configure terminal
```

```
device(config)# pw-profile pw_example
device(config-pw-pw_example)# control-word
```

The following example shows how to disable PW control word for a PW profile named pw_example

```
device# configure terminal
device(config)# pw-profile pw_example
device(config-pw-pw_example)# no control-word
```

console

Configures the height and width of the serial console terminal.

Syntax

console [**height** *number_of_rows*] [**width** *number_of_columns*]

Command Default

By default, the serial console is 24 rows high and 80 rows wide.

Parameters

height *number_of_rows*

Specifies the height of the serial console in rows. Valid values range from 1 through 256.

width *number_of_columns*

Specifies the width of the serial console in columns. Valid values range from 1 through 256.

Modes

Privileged EXEC mode

Usage Guidelines

Configure the size of the serial console terminal to prevent overwritten or misaligned console output when multiple users connect to the serial console. The terminal emulators that connect to the console must have the same window size as the console to prevent overwritten or misaligned output.

The configuration of the console size does not persist after a reboot.

Use the **console** command without options to display the size of the serial console terminal.

Examples

The following example displays the size of the serial console terminal.

```
device# console

Serial console height 24 width 80
```

The following example configures a height of 43 rows and a width of 132 columns.

```
device# console height 43 width 132

Set serial console height 43 width 132
```

The following example configures a height of 24 rows.

```
device# console height 24

Set serial console height 24
```

The following example configures a width of 80 columns.

```
device# console width 80

Set serial console width 80
```

copy

Copies configuration data.

Syntax

copy *source_file destination_file* [**remove-tpvm**]

Parameters

source_file

The source file to be copied. Specify one of the following parameters:
default-config

The default configuration.

running-config

The running configuration.

startup-config

The startup configuration.

flash:// *filename*

A file in the local flash memory.

ftp:// *username:password@host_ip_address/path*

A file on a remote host. Transfer protocol is FTP.

scp:// *username:password@host_ip_address/path*

A file on a remote host. Transfer protocol is SCP.

sftp:// *username:password@host_ip_address/path*

A file on a remote host. Transfer protocol is SFTP.

tftp:// *username:password@host_ip_address/path*

A file on a remote host. Transfer protocol is TFTP.

usb:// *path*

A file on an attached USB device.

destination_file

The destination file. Specify one of the following parameters:
default-config

The default configuration.

running-config

The running configuration.

startup-config

The startup configuration.

flash:// *filename*

A file in the local flash memory.

ftp:// *username:password@host_ip_address//path*

A file on a remote host. Transfer protocol is FTP.

scp:// *username:password@host_ip_address//path*

A file on a remote host. Transfer protocol is SCP.

sftp:// *username:password@host_ip_address/path*

A file on a remote host. Transfer protocol is SFTP.

tftp:// *username:password@host_ip_address/path*

A file on a remote host. Transfer protocol is TFTP.

usb:// *path*

A file on an attached USB device.

remove-tpvm

By default, TPVM configuration is persisted and the TPVM is reinstalled and reconfigured when the **copy default-config startup-config** is executed. When the **copy default-config startup-command** command is executed with this parameter, any installed TPVM is also removed and the device reboots with a clean install without TPVM.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to back up and restore configuration files with various protocols.

This command is supported only on the local switch.

IPv4 and IPv6 addresses are supported.

The special characters of dollar sign "$" and exclamation point "!" can be used as part of the password variable, provided they are paired with the correct escape characters. The "$" must be paired with two backslashes "\\". For example, if your password choice was "$password" on a remote server, you must use "username:\\$password@1.1.1.1" for the **copy** command. The exclamation point must be paired with a single backslash in the **copy** command, such as "username:\!password@1.1.1.1".

When using a file to restore a backed up configuration as the *startup* configuration, care must be taken to ensure that the source file's TPVM configuration is the same as the running TPVM's configuration. Particularly, if the source's TPVM configuration is partial, and does not have some of the configured parameters of the running TPVM instance. In such a scenario, it is advised not to proceed with this change as it will result in the configuration of the installed TPVM not being similar to the configuration of the previous TPVM instance.

On SLX 9740 and Extreme 8720 devices, you cannot access a remote FTP server with its IPv6 address. Instead, use the remote FTP server's IPv4 address.

Examples

To save the running configuration to a file:

```
device# copy running-config flash://myconfig
```

To overwrite the startup configuration with a locally saved configuration file:

```
device# copy flash://myconfig running-config
```

To overwrite the startup configuration with a remotely archived configuration file:

```
device# copy scp://user:password@10.10.10.10//myconfig startup-config
```

To overwrite the startup configuration with a configuration file saved on an attached USB device:

```
device# copy usb://myconfig startup-config
```

To overwrite the startup configuration with the default configuration. This will wipe out the device's configuration but will reinstall and reconfigure the TPVM installation on the device.

```
device# copy default-config startup-config
```

To overwrite the startup configuration with the default configuration. This will wipe out the device's configuration including the TPVM installed on the device.

```
device# copy default-config startup-config remove-tpvm
```

core-isolation-disable

Core Isolation feature shuts down ESI interface(s) when all the core interfaces between the Leaf and Spine nodes go down. This feature is enabled by default. Use this command to disable this feature. When disabled, the ESI interface will not be brought down when all the core interfaces between the Leaf and Spine go down.

Syntax

core-isolation-disable

no core-isolation-disable

Command Default

Core Isolation is enabled by default. It has to be explicitly disabled using this command.

Modes

Global configuration mode

Examples

The following example shows the disabling of the *core-isolation* feature

```
SLX # configure terminal
SLX (config)# core-isolation-disable
```

core-isolation-track

Core Isolation feature shuts down ESI interface(s) when all the core interfaces between the Leaf and Spine nodes go down. During core-isolation, data traffic will be black-holed in the multi-homing nodes if the single homed edge port interfaces are present and the Ethernet VPN Instance VLANs are shared with these interfaces. These single homed edge port interfaces need to be brought up/down along with the ESI client interfaces for better data convergence. This command enables tracking these single homed edge port interfaces to ensure that they are brought up/down along with ESI client interfaces.

Syntax

core-isolation-track

no core-isolation-track

Command Default

Core Isolation tracking is disabled by default. It has to be explicitly enabled using this command.

Modes

Interface Configuration Mode (for Ethernet and Port Channel interfaces only).

Usage Guidelines

This command ensures that that the configured single homed edge port interface is brought down along with the ESI interfaces. When the BGP EVPN sessions come up, these tracked single homed edge port interfaces are brought up along with the ESI interfaces to have better data traffic convergence.

This feature is only available when ESI is configured on (at least) a single interface.

Core Isolation Tracking cannot be applied to an interface that is a port-channel member. That is, the interface must not have **channel-group** configuration present.

The interface on which *Core Isolation Tracking* is applied to, must not be a multi-homed client. Post this configuration, the tracked interface cannot be assigned as a PO member or a multi-homing client.

During firmware downgrade, **core-isolation track** configurations are removed.

Examples

The following example shows the configuration of Core Isolation Tracking on a port-channel interface.

```
SLX (config)# interface port-channel 1
SLX (config-Port-channel-1)#  core-isolation-track
```

The following example shows the configuration of Core Isolation Tracking on an ethernet interface.

```
SLX (config)# interface ethernet 0/1
SLX (config)# core-isolation-track
```

cos (MPLS)

Configures the a Class of Service (CoS) priority value for all packets traveling through the LSP.

Syntax

cos *number*

no cos *number*

Parameters

number

Specifies the CoS priority value. Enter a number from 0 to 7. The lowest priority is 0, the default value. The highest priority is 7.

Modes

MPLS LSP configuration mode.

MPLS router bypass LSP configuration mode (config-router-mpls-bypass-lsp-*bypass_name*).

MPLS router MPLS interface dynamic bypass configuration mode (config-router-mpls-if-ethernet-*slot/port*-dynamic-bypass)

Usage Guidelines

The 3-bit EXP field in the MPLS header defines a CoS value for packets traveling through the LSP. When you set the CoS value, it is applied to the EXP field in the MPLS header of all packets entering this LSP. Then, all packets traveling through an LSP have the same priority as they travel the MPLS domain.

The MPLS CoS value determines the priority within an MPLS domain only. When the label is pops, the CoS value in the MPLS header is discarded and it is not copied back to the IP ToS field.

Use the **no** form of the command to remove the configured setting.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures the CoS priority of 7 to all packets traveling through the tunnel4 LSP.

```
device(config-router-mpls)# lsp tunnel4
device(config-router-mpls-lsp-tunnel4)# cos 7
```

The following example configures the CoS priority of *6* to dynamic bypass MPLS Ethernet interface *0/8*.

```
device>configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/8
device(config-router-mpls-if-ethernet-0/8)# dynamic-bypass
device(config-router-mpls-if-ethernet-0/8-dynamic-bypass)# cos 6
```

cos (Y1731)

Configures class of service (CoS).

Syntax

cos *class-of-service*

no cos

Parameters

class-of-service

Specifies the CoS value. The range is from 1 to 8. The default value is 7.

Modes

Y1731 configuration mode

Usage Guidelines

Use the **no** form of the command to delete the CoS configuration.

Examples

This example shows how to configure CoS.

```
device# configure terminal
device (config-cfm)# prtocol cfm
device (config-cfm)# y1731
device(config-cfm-y1731)# test-profile my_test_profile
device(config-cfm-y1731-test-profile-my_test_profile)# type delay-measurement
device(config-cfm-y1731-test-profile-my_test_profile)# tx-interval 60
device(config-cfm-y1731-test-profile-my_test_profile)# measurement-interval 30
device(config-cfm-y1731-test-profile-my_test_profile)# start at 00:00:00 daily
device(config-cfm-y1731-test-profile-my_test_profile)# stop at 23:59:00
device(config-cfm-y1731-test-profile-my_test_profile)# cos 7
```

convergence-time

Configures the convergence time when transitioning out of Maintenance Mode. Convergence time comes into play only when Maintenance Mode is disabled.

Syntax

convergence-time *time*

Command Default

The default convergence time is 300 seconds.

Parameters

time

The convergence time in seconds. Range is 100-500.

Modes

System Maintenance mode

Usage Guidelines

Use the *no* form of this command to revert the convergence time to the default interval of 300 seconds.

Examples

The following example configures the convergence time to 250 seconds.

```
SLX# configure terminal
SLX (config)# system maintenance
SLX (config-system-maintenance)# convergence-time 250
SLX (config-system-maintenance)# enable
SLX (config-system-maintenance)#
```

The following example removes the existing convergence time configuration and resets it to the default value of 300 seconds.

```
SLX# configure terminal
SLX (config)# system maintenance
SLX (config-system-maintenance)# no convergence-time
SLX (config-system-maintenance)# enable
SLX (config-system-maintenance)#
```

crypto ca authenticate

Identifies the root CA certificate, which is used to sign the Certificate Signing Request (CSR) to generate the server certificate.

Syntax

crypto ca authenticate {*trustpoint-name cert-type* { **commoncert** | **https** | **ssh-x509v3**}**directory** *dirname* **file** *file-name* **host** *host-address* **protocol source-ip***source-ip*{**FTP** | **SCP**} **user** *user-name* **password** *password*}

no crypto ca authenticate { *trustpoint_name cert-type* { **commoncert** | **https** | **ssh-x509v3**}

Parameters

trustpoint-name

Defines the name of the trustpoint you are authenticating. This name needs to be the same as that of the trustpoint created by the **crypto ca trustpoint** command. The string for the name cannot be left blank. The length of the string can range from 1 through 64 characters.

cert-type {**commoncert** | **https** | **ssh-x509v3**}

Indicates that the certificate is used for common, HTTPS, or SSH-x509v3 server authentication.

directory *dir-name*

Defines the path to the directory where the certification file resides.

file *file-name*

Defines the name of the certification file.

host *host-address*

Specifies the host name or IP address of the remote certificate server.

protocol {**FTP** | **SCP**}

Specifies the use of either FTP or SCP protocol for accessing the certification file.

user *user-name*

Specifies the user name for the host server.

source-ip *source-ip*

(SCP only) Specifies the source IP address to use in the header.

password *password*

Specifies the password for the user to access the host server.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to identify the CA certificate of the Trusted CA that you want to sign the CSR and generate the identity certificate.

The *trustpoint-name* name needs to be the same as that of the trustpoint created by the **crypto ca trustpoint** command.

The **no** form of the command deletes the specified certificate.

Note
As a best practice, do not list the password in the command line for security purposes. The user will be prompted for the password.

Examples

This example specifies HTTPS authentication and the SCP protocol.

```
device# crypto ca authenticate t1 cert-type https protocol SCP host 10.70.12.102
user fvt directory /users/home/crypto file cacert.pem password ****
```

This example specifies SSH-x509v3 authentication and the SCP protocol.

```
crypto ca enroll myca cert-type ssh-x509v3 protocol SCP country IN state KA
locality Bangalore organization Extreme orgunit Engg common 10.24.12.xx directory /root/
certs
host x.x.x.x user root password ****
```

crypto ca enroll

Enrolls the trustpoint by generating the Certificate Signing Request (CSR) and exporting it to the remote certificate server.

Syntax

crypto ca enroll {*trustpoint-name* **cert-type** {**commoncert** | **https** | **ssh-x509v3**} **common** *common-name* **country** *country-name* **state** *state-name* **locality** *locality-name* **organization** *org-name* **orgunit** *org-unit* **directory** *dir-name* **file** *file-name* **host** *host-address* **source-ip** *source-ip* **protocol** {**FTP** | **SCP**} **user** *user-name* **password** *password*}

Parameters

trustpoint-name

Defines the name of the trustpoint you are enrolling. This name needs to be the same as that of the trustpoint created by the **crypto ca trustpoint** command. The string for the name cannot be left blank. The length of the string can range from 1 through 64 characters.

cert-type commoncert | **https** | **ssh-x509v3**}

Indicates that the certificate is used for common, HTTPS, or SSH-x509v3 server authentication.

common *common-name*

Identifies the name used to connect to the device through HTTPS. Enter a Fully Qualified Domain Name (FQDN) or IP address. If a FQDN is used, you need to configure a domain name and name server on the device.

country *country-name*

Defines the two-letter country code for generating the CSR.

state *state-name*

Defines the state name for generating the CSR.

locality *locality-name*

Defines the locality name for generating the CSR.

organization *org-name*

Defines the organizational unit name for generating the CSR.

orgunit *orgunit*

Defines the name of the certification file.

directory *dir_name*

Defines the path of the directory to export the Certificate Signing Request.

file *file-name*

Defines the file name of the CSR.

host *host-address*

Specifies the host name or IP address of the remote certificate server.

source-ip *source-ip*

(SCP only) Specifies the source IP address to use in the header.

protocol {**FTP** | **SCP**}

Specifies the use of either FTP or SCP protocol for exporting the certification file.

user *user-name*

Defines the user name for the host server.

password *password*

Defines the password for the user name for the host server.

Note
As a best practice, do not list the password in the command line for security purposes. The user will be prompted for the password.

Modes

Privileged EXEC mode

Usage Guidelines

The *trustpoint_name* name needs to be the same as that of the trustpoint created by the **crypto ca trustpoint** command.

Examples

Typical command example:

```
device# crypto ca enroll t1 cert-type https country US state CA locality SJ
organization EXT orgunit SFI common myhost.extreme.com protocol SCP host 10.70.12.102
user fvt directory /proj/crypto
```

crypto ca import

Imports the Identity Certificate for security configuration.

Syntax

crypto ca import { *trustpoint-name* **cert-type** {**commoncert** | **https** | **ssh-x509v3** } **protocol** {**FTP** | **SCP**} **directory** *dir-name* **file** *file-name* **host** *host-address* **user** *user-name* **password** *password* **source-ip** *source-ip*}

no crypto ca import {*trustpoint-name* **cert-type** {**commoncert** | **https** | **ssh-x509v3** } }

Parameters

trustpoint-name

Defines the name of the trust point you are authenticating. This name needs to be the same as that of the trust point created by the **crypto ca trustpoint** command. The string for the name cannot be left blank. The length of the string can range from 1 through 64 characters.

cert-type commoncert | **https** | **ssh-x509v3**}

Indicates that the certificate is used for common, HTTPS, or SSH-x509v3 server authentication.

protocol {**FTP** | **SCP**}

Specifies the use of either FTP or SCP protocol for accessing the certificate file.

directory *dir-name*

Defines the directory where the certificate resides.

file *file-name*

Defines the name of the certificate file.

host *host-address*

Defines the host name or IP address of the remote certificate server.

user *user-name*

Defines the user name for the host server.

source-ip *source-ip*

(SCP only) Specifies the source IP address to use in the header.

password *password*

Defines the password for the user name on the host server.

Note
As a best practice, do not list the password in the command line for security purposes. The user will be prompted for the password.

Modes

Privileged EXEC mode

Usage Guidelines

The *trustpoint-name* name needs to be the same as that of the trust point created by the **crypto ca trustpoint** command.

Use the **no** form of the command to remove the certificate.

Examples

This example specifies HTTPS authentication and the SCP protocol.

```
device# crypto ca import t1 certificate cert-type https protocol SCP host 10.70.12.102
user fvt directory /users/crypto file cacert.pem
Password: **********
```

This example specifies SSH-x509v3 authentication and the SCP protocol.

```
device# crypto ca import myca certificate cert-type ssh-x509v3 protocol SCP
directory /root/certs file sshserver.pem host x.x.x.x user root password ****
```

crypto ca import-pkcs

Imports a TLS certificate and a private key in PKCS12 format.

Syntax

crypto ca import-pkcs { **type pkcs12 cert-type** { **gNMI-server** | **https** | **ldap-client** | **radius-client** | **syslog-client** } **protocol** { **FTP** | **SCP** } **directory** *dir-name* **file** *file-name* **source-ip** *source-ip* **host** *host-address* **user** *user-name* **password** *scp-password* [**pkcs-passphrase** *pkcs-export-password*] [**use-vrf** *vrf-name*] }

no crypto ca import-pkcs type pkcs12 cert-type {**gNMI-server** | **https** | **ldap-client** | **radius-client** | **syslog-client** }

Parameters

type pkcs12

Indicates that the private key for the CA certificate is in the <term>pkcs12</term> format.

cert-type {https | **gNMI-server** | **https** | **ldap-client radius-client** | **syslog-client** }

Indicates that the certificate is used for HTTPS and gNMI server authentication. Additionally, now certificates for LDAP Client, RADIUS Client, and SYSLOG Clients can be imported and used for authentication.

protocol { **FTP** | **SCP** }

Specifies the use of either FTP or SCP protocol for accessing the remote certificate file.

directory *dir_name*

Defines the remote directory where the certificate resides.

file *file-name*

Defines the file name of the certificate file in .pfx or .p12 format.

host *host-address*

Defines the host name or IP address of the remote certificate server.

source-ip *source-ip*

(SCP only) Specifies the source IP address to use in the header.

user *user-name*

Defines the user name for the remote certificate server.

password *scp-password*

Defines the password for the user name on the remote certificate server.

Note
When the password is not provided in the CLI command, the user will be prompted for it when the CLI is executed.

pkcs-passphrase *pkcs-export-password*

Defines the password used at the creation of the .pfx or .p12 certificate file.

use-vrf *vrf-name*

Defines the VRF to use to reach the remote certificate server.

Modes

Privileged EXEC mode

Usage Guidelines

Use the below mentioned command to import a TLS server certificate and private key (`in PKCS12` format) to an SLX device (with no trust point) and establish a secure connection.

Note
Server Certificates are to be imported on the SLX device mandatorily, before configuring gNMI server.

CLI Command:

```
crypto ca import-pkcs {type pkcs12 cert-type gNMI-server } protocol {FTP | SCP} directory
dir-name file file-name source-ip source-ip host host-address user user-name password scp
password [ pkcs-passphrase pkcs-export-password ] [ use-vrf vrf-name ]}
crypto ca import-pkcs {type pkcs12 cert-type https } protocol {FTP | SCP} directory dir-
name file file-name source-ip source-ip host host-address user user-name password scp
password [ pkcs-passphrase pkcs-export-password ] [ use-vrf vrf-name ]}
```

Certificates for the following servers can be imported:

- HTTPS Server
- gNMI Server

Certificates for the following clients can be imported:

- LDAP Client
- RADIUS Client
- SYSLOG Client

Use the **no** form of the command to remove a certificate and key.

Examples

This example specifies HTTPS authentication and SCP using a VRF named red.

```
device# crypto ca import-pkcs12 cert-type https protocol SCP host 10.70.12.102
user fvt directory /users/crypto file pkcs12cert.p12 password **********
pkcs-passphrase ******** use-vrf red
```

This example removes an HTTPS certificate and key.

```
device# no crypto ca import-pkcs type pkcs12 cert-type https
```

This example specifies gNMI server authentication.

```
device# crypto ca import-pkcs type pkcs12 cert-type gNMI-server directory /root/gselvaraj/
NH217/ file nh217.pfx protocol SCP host 10.24.12.107 user root password *** pkcs-
passphrase ***
```

This example removes gNMI server certificate and key.

```
device# no crypto ca import-pkcs type pkcs12 cert-type gNMI-server
```

crypto ca trustpoint

Defines the trust point for HTTPS security configuration.

Syntax

crypto ca trustpoint *trustpoint-name*

no crypto ca trustpoint *trustpoint-name*

Parameters

trustpoint-name

Defines the name of the trustpoint. The string for the name cannot be left blank. The length of the string can range from 1 through 64 characters.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of the command to remove the trustpoint.

Examples

Typical command examples:

```
device(config)# crypto ca trustpoint t1
device(config)# crypto ca trustpoint trustpoint2
device(config)# crypto ca trustpoint tp3
device(config)# crypto ca trustpoint t4
device(config)# crypto ca trustpoint t5
```

Example using the no form of the command:

```
device(config)# no crypto ca trustpoint t1
```

crypto cert expiry-level

Configures generating notifications for certificate expiry. Depending on the number of days to certificate expiry, notifications with different warnings are generated. Notifications can be RASLog or SNMP or both.

Syntax

crypto cert expiry-level [*info* | *minor* | *major* | *critical*] **period** *alert-period*

no crypto cert expiry-level [*info* | *minor* | *major* | *critical*] **period** *alert-period*

Parameters

expiry-level [*info* | *minor* | *major* | *critical*]

Type of certificate expiry warning to be generated.

period *alert-period*

Defines the duration, in number of days, when the notification alert will be generated, before a certificate actually expires. This value is in the range 1-90 days.

Modes

Global Configuration Mode

Usage Guidelines

Note
Notifications can be RASLog or SNMP or both.

When configured, notification is generated with a warning with the configured severity level along with a serial number of the certificate for which this entry is being generated. A notification is generated for every certificate that will expire within the configured number of days.

A single warning is generated when the number of days remaining for expiry is equal to (=) or becomes lesser than (<) the configured period for that severity level.

Certificate expiry checks are done once every day at 00:00 hours (midnight). Depending on the setting of the *notAfter* field in each certificate, Notification generation may be delayed up to 24 hours.

Note
Notifications are generated only after successful configuration using the **crypto cert** command.

When a certificate expires, a notification with an severity *error* is generated every 24 hours till the expired certificate is renewed. Generation of this notification is not affected by the configurations of the expiry levels.

If the SLX device's system time is manually changed after a notification is generated, SLX does not send the same notification again unless the specific crypto severity level is reconfigured to previous notification configuration or the specific certificate for which the notification is sent is re-imported.

When more than one alert level is configured with same period value, a notification is generated for higher severity level.

Examples

The following example show the configuration of the four (4) certificate expiry warning levels.

```
SLX # configure terminal
SLX (config)# crypto cert expiry-level info period    90
SLX (config)# crypto cert expiry-level minor period   60
SLX (config)# crypto cert expiry-level major period   30
SLX (config)# crypto cert expiry-level critical period 7
SLX (config)#
```

The **No** form of this command will turn off the warning for the provided severity level.

```
SLX# conf term
Entering configuration mode terminal
SLX(config)# no crypto cert expiry-level minor period 60
SLX(config)# end
SLX#
```

crypto import

Imports the Identity Certificate for security configuration.

Syntax

crypto import { **ldapca** | **radiusca** | **syslogca** | **gnmiclientca** | **httpsclientca** } **directory** *dir-name* **file** *file-name* **host** *host-address* **protocol** { **FTP** | **SCP** } **source-ip** *source-ip* **user** *user-name* **password** *password*

no crypto import { **ldapca** | **radiusca** | **syslogca** |**gnmiclientca** | **httpsclientca** }

Parameters

ldapca | **radiusca** | **syslogca** | **gnmiclientca** | **httpsclientca**

Defines the type of certificate to import. Select from *ldapca*, *radiusca*, *syslogca*, *gnmiclientca*, or *httpsclientca*.

directory *dir-name*

Defines the remote directory where the certificate file resides.

file *file-name*

Defines the name of the certification file.

host *host-address*

Defines the host name or IP address of the remote certificate server.

protocol { **FTP** | **SCP** }

Specifies the use of either FTP or SCP protocol for accessing the certificate file.

source-ip *source-ip*

(SCP only) Specifies the source IP address to use in the header.

user *user-name*

Defines user name for the remote certificate server.

password *password*

Defines the password for the user name for the remote certificate server.

Note
When the password is not provided in the CLI command, the user will be prompted for it when the CLI is executed.

Note
gNMI Client CA is needed for mutual TLS communication. For server based authentication, gNMI Client CA is optional.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **no** form of the command to remove the Identity Certificate.

Examples

This example imports a RADIUS certificate over SCP.

```
device# crypto import radiusca t1 certificate protocol SCP host 10.10.10.10
                    user fvt directory /users/crypto file cacert.pem password ****
```

This example imports a gNMI client CA certificate over SCP.

```
device# crypto import gnmiclientca directory  /home/kokila/ocsp_cert_116/certs/ file
ca.cert.pem host 10.23.20.116 protocol SCP user kokila password ***
```

This example deletes gNMI client CA certificate.

```
device# no crypto import gnmiclientca
```

This example deletes RADIUS server CA certificate.

```
device # no crypto import radiusca
```

crypto key

Generates an RSA, ECDSA, or DSA key pair to sign or encrypt and decrypt the security payload during security protocol exchanges for applications. You must sign and encrypt or decrypt the key pair before you obtain a certificate for your device.

Syntax

crypto key label *key-name* [**rsa** | **ecdsa** | **dsa**] [**modulus** *bit-value*]

no crypto key label *key-name*

Parameters

label *key-name*

The name of the key pair.

rsa

Generates an RSA key pair.

ecdsa

Generates an ECDSA key pair.

dsa

Generates a DSA key pair.

modulus *bit-value*

Specifies the key size. The corresponding key sizes supported for each key type are:

- RSA: 1024 or 2048
- DSA: 1024
- ECDSA: 256,384, or 521

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to remove the key pair.

The key label must contain alphanumeric characters.

Examples

Typical command examples for generating a key pair.

```
device(config)# crypto key label k1 rsa modulus 1024
device(config)# crypto key label key2 rsa modulus 2048
device(config)# crypto key label pvtkey3 dsa modulus 1024
```

```
device(config)# crypto key label k4 ecdsa modulus 384
device(config)# crypto key label k5 ecdsa modulus 521
```

The following is an example of removing a key pair.

```
device(config)# no crypto key label k1
```

csnp-interval

Configures the Complete Sequence Number PDU (CSNP) interval.

Syntax

csnp-interval *secs*

no csnp-interval

Command Default

The default CSNP interval is 10 seconds.

Parameters

secs

Specifies the interval in seconds. Valid values range from 0 through 65535 seconds.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The interval configured on the device applies to both Level 1 and Level 2 CSNPs and Partial Sequence Number PDUs (PSNPs).

The **no** form of the command restores the default value.

Examples

The following example configures a CSNP interval of 25 seconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# csnp-interval 25
```

cspf-computation-mode

The path calculation metric implementation allows you to specify the path calculation for a given tunnel.

Syntax

cspf-computation-mode { [**ignore-overload-bit** | **metric-type** [**use-bypass-metric** | **use-igp-metric** | **use-te-metric**]] }

no cspf-computation-mode { [**ignore-overload-bit** | **metric-type** [**use-bypass-metric** | **use-igp-metric** | **use-te-metric**]] }

Command Default

By default, all LSPs use the TE-metric global configuration.

Parameters

ignore-overload-bit

Ignores the overload bit during CSPF computation.

metric-type

Select for CSPF computation.

use-bypass-metric

Use the bypass metric to enable the bypass path cost for the backup path.

use-igp-metric

Use to configure the metric plane to IGP-configured metric while computing the CSPF path.

use-te-metric

Use to configure the metric plane to the TE-configured metric while computing the CSPF path.

Modes

Global level (config-router-mpls-policy): This configuration covers all RSVP LSPs (primary, secondary LSPs).

MPLS router bypass LSP configuration mode. (config-router-mpls-bypass-lsp)

Individual LSP mode: This configuration covers all RSVP LSPs.

MPLS router MPLS interface dynamic bypass configuration mode (config-router-mpls-if-ethernet-*slot/port*-dynamic-bypass).

Usage Guidelines

The CLI configuration at the LSP level always overrides the configuration at the global level. That is, the decision to use-te-metric or use-igp-metric for CSPF path calculation if configured at the LSP level, always overrides the configuration at the global level.

The user can configure the CSPF computation mode for the CSPF Path calculation of dynamic bypass LSPs that get created. CSPF can make use of either the TE-metric as cost or the IGP metric as cost for the shortest path first algorithm.

The **no** form of the command removes the CSPF computation mode.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

In the following example, the CSPF computation mode is set back to a default value of the te-metric at the global level.

```
device# configure
device(config)# router-mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# cspf-computation-mode metric-type use-igp-metric
device(config-router-mpls-policy)# no cspf-computation-mode metric-type use-te-metric
Error:CSPF computation is configured to use igp-metric
device(config-router-mpls-policy)# no cspf-computation-mode metric-type use-igp-metric
```

In the following example, the CSPF computation mode is set back to a default value of the use-te-metric at the LSP level.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp test
device(config-router-mpls-lsp-test)# cspf-computation-mode metric-type use-igp-metric
device(config-router-mpls-policy)# no cspf-computation-mode metric-type use-te-metric
Error:CSPF computation is configured to use-igp-metric
device(config-router-mpls-policy)# no cspf-computation-mode metric-type use-igp-metric
```

In the following example, both the cost and number of riding backups are considered using the use-bypass-metric command.

```
device# configure
device(config)# router-mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# cspf-computation-mode metric-type use-bypass-metric
```

In the following example, both the cost and number of riding backups are considered using the **use-igp-metric** command for dynamic bypass MPLS Ethernet interface *0/8*.

```
device# configure
device(config)# router-mpls
device(config-router-mpls)# mpls-interface ethernet 0/8
device(config-router-mpls-if-ethernet-0/8)# dynamic-bypass
device(config-router-mpls-if-ethernet-0/8-dynamic-bypass)# cspf-computaion-mode use-igp-
metric
```

cspf-interface-constraint

Forces the CSPF calculation to include any specified interface when creating an LSP.

Syntax

cspf-interface-constraint

no cspf-interface-constraint

Command Default

The command is disabled, by default.

Modes

MPLS policy mode.

Usage Guidelines

The command may be dynamically turned on or off. Turning the command off or on has no effect on LSPs that have already been established (primary and secondary). For LSPs that are currently retried, changing the constraint setting changes the behavior on the next retry such as when an LSP whose path is configured to use that interface fails to come up due to an interface down condition.

The command has significance for the ingress node only, where the CSPF calculation takes place for an LSP or a detour segment.

The **no** form of the command disables the configuration.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures the command.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# cspf-interface-constraint
```

cspf-group

Configures a CSPF fate-sharing group by assigning a name to the group.

Syntax

cspf-group *group_name*

no cspf-group

Command Default

The command is disabled by default.

Parameters

group_name

Specifies the name of the fate-sharing group. The group-name variable can be up to128 characters. The objects that can be specified for a fate-sharing group are interface, point-to-point link, node, and subnet.

Modes

MPLS router mode

Usage Guidelines

The **no** form of the command disables the command.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example assigns the name *group3* to the fate sharing group configuration.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# cspf-group group3
```

cspf-group-computation

Use the **cspf-group-computation** mode when setting up a fate-sharing group.

Syntax

cspf-group-computation [**add-penalty** | **ignore-overload-bit** | **metric-type** [**use-igp-metric** | **use-te-metric**] | **use-bypass-metric**]

no cspf-group-computation

Command Default

The CSPF group computation mode is disabled, by default.

Parameters

add-penalty

Adds penalty of all matching cspf-groups to TE metric of the TE link.

ignore-overload-bit

Ignores the overload bit during CSPF computaton.

metric-type

Selects the metric type for CSPF computation.

use-igp-metric

Uses the IGP metric of the link for CSPF computation.

use-te-metric

Uses the TE metric of the link for CSPF computation.

use-bypass-metric

Uses the bypass LSPs path cost for the selection between bypass LSPs

Modes

MPLS policy configuration mode (config-router-mpls-policy).

Usage Guidelines

The no form of the command disables the CSPF group computation mode.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example specifies the CSPF-group computation for a fate-sharing group, and enables the add-penalty option.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# cspf-group-computation add-penalty
```

The following example enables the liberal mode of the bypass LSP selection.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# cspf-group-computation use-bypass-liberal
```

dampening

Sets dampening parameters for the route in BGP address-family mode.

Syntax

dampening { *half-life reuse suppress max-suppress-time* | **route-map** *route-map* }

no dampening

Command Default

Disabled.

Parameters

half-life

Number of minutes after which the route penalty becomes half its value. Range is from 1 through 45. Default is 15.

reuse

Minimum penalty below which the route becomes usable again. Range is from 1 through 20000. Default is 750.

suppress

Maximum penalty above which the route is suppressed by the device. Range is from 1 through 20000. Default is 2000.

max-suppress-time

Maximum number of minutes a route can be suppressed by the device. Range is from 1 through 255. Default is 40.

route-map

Enables selection of dampening values established in a route map by means of the **route-map** command.

route-map

Name of the configured route map.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use the **no** form of this command to disable dampening.

Use **dampening** without operands to set default values for all dampening parameters.

To use the dampening values established in a route map, configure the route map first, and then enter the **route-map** command, followed by the name of the configured route map.

A full range of dampening values (*half-life*, *reuse*, *suppress*, *max-suppress-time*) can also be set by means of the **set as-path prepend** command.

Examples

The following example enables default dampening as an IPv4 address-family function.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# dampening
```

The following example changes all the dampening values as an IPv6 address-family function.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# dampening 20 200 2500 40
```

database-overflow-interval (OSPFv2)

Configures frequency for monitoring database overflow.

Syntax

database-overflow-interval *interval*

no database-overflow-interval

Command Default

0 seconds. If the device enters OverflowState, you must reboot before the device leaves this state.

Parameters

interval

Time interval at which the device checks to see if the overflow condition has been eliminated. Valid values range from 0 through 86400 seconds.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

This command specifies how long a device that has entered the OverflowState waits before resuming normal operation of external LSAs. However, if the external link state database (LSDB) is still full, the device lapses back into OverflowState. If the configured value of the database overflow interval is zero, then the device never leaves the database overflow condition.

When the maximum size of the LSDB is reached (this is a configurable value in the *external-lsdb-limit* CLI), the device enters OverflowState. In this state, the device flushes all non-default AS-external-LSAs that the device had originated. The devie also stops originating any non-default external LSAs. Non-default external LSAs are still accepted if there is space in the database after flushing. If no space exists, the Non-default external LSAs are dropped and not acknowledged.

The **no** form of the command disables the overflow interval configuration.

Examples

The following example configures a database-overflow interval of 60 seconds.

```
device# configure terminal
```

```
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# database-overflow-interval 60
```

database-overflow-interval (OSPFv3)

Configures frequency for monitoring database overflow.

Syntax

database-overflow-interval *interval*

no database-overflow-interval

Command Default

10 seconds. If the router enters OverflowState, you must reboot before the router leaves this state.

Parameters

interval

Time interval at which the device checks to see if the overflow condition has been eliminated. Valid values range from 0 through 86400 seconds (24 hours).

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

This command specifies how long after a router that has entered the OverflowState before it can resume normal operation of external LSAs. However, if the external link state database (LSDB) is still full, the router lapses back into OverflowState.

When the maximum size of the LSDB is reached (this is a configurable value in the *external-lsdb-limit* CLI), the router enters OverflowState. In this state, the router flushes all non-default AS-external-LSAs that the router had originated. The router also stops originating any non-default external LSAs. Non-default external LSAs are still accepted if there is space in the database after flushing. If no space exists, the Non-default external LSAs are dropped and not acknowledged.

The **no** form of the command disables the overflow interval configuration.

Examples

The following example configures a database-overflow interval of 120 seconds.

```
device# configure terminal
device(config)# ipv6 router ospf
```

```
device(config-ipv6-router-ospf-vrf-default-vrf)# database-overflow-interval 120
```

debug access-list-log buffer

Configures or clears the ACL buffer.

Syntax

debug access-list-log buffer { **circular** | **linear** } **packet-count** *count-value*

debug access-list-log buffer clear

no debug access-list-log buffer

Parameters

circular

Specifies circular buffer type.

linear

Specifies linear buffer type.

packet-count *count-value*

Specifies a value from 64 through 2056.

clear

Clears the buffer contents.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Work closely with Extreme Networks technical support when running **debug** or **show system internal** commands and interpreting their results.

Use the no form of this command to disable debugging.

Examples

The following example clears the buffer.

```
device# debug access-list-log buffer clear
```

debug arp packet buffer

Configures or clears the ARP-packet buffer.

Syntax

debug arp packet buffer all

no debug arp packet buffer all

debug arp packet buffer { **circular** | **linear** } **packet-count** *num-packets* [**vrf** *vrf-name*]

debug arp packet buffer clear [**vrf** *vrf-name*]

debug arp packet buffer interface { **ethernet** *slot* **/** *port* | **port-channel** *number* | **ve** *ve-id* } [**rx** | **tx**]

no debug arp packet buffer interface { **ethernet** *slot* **/** *port* | **port-channel** *number* | **ve** *ve-id* } [**rx** | **tx**]

Parameters

all

Specifies all ARP-packet buffers.

circular

Specifies circular buffer type.

linear

Specifies linear buffer type.

packet-count *num-packets*

Specifies a value from 64 through 2056.

clear

Clears the buffer contents.

vrf *vrf-name*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

interface

Specifies an Ethernet or VE interface.

ethernet

Specifies a physical Ethernet interface.

slot

Specifies a valid slot number. For devices that do not support linecards, specify **0**.

port

Specifies a valid port number.

port-channel *number*

Specifies a port-channel interface.

ve *ve-id*

Specifies a virtual ethernet (VE) interface.

rx

Specifies whether to capture only transmitted packets.

tx

Specifies whether to capture received packets.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Work closely with Extreme Networks technical support when running **debug** or **show system internal** commands and interpreting their results.

If neither **rx** nor **tx** are specified, both transmitted and received packets are captures.

To disable ARP packet capture on a specified interface, use the **no debug dhcp packet buffer interface** command.

To disable ARP packet capture on all interfaces, use the **no debug dhcp packet buffer all** command.

Examples

The following command enables ARP packet capture for transmitting data on Ethernet interface 1/5.

```
device# debug arp packet buffer interface ethernet 1/5 tx
```

The following command disables ARP packet capture on all interface.

```
device# no debug arp packet buffer all
```

debug dhcp packet buffer

Configures a buffer to capture DHCP packets.

Syntax

debug dhcp packet buffer [**all** | **circular** *packet count* | **clear** *vrf name* | **interface** *ethernet/port-channel* | **linear***packet count*]

Command Default

The buffer wraps around to overwrite earlier captures (circular).

Parameters

circular

Buffer wraps around to overwrite earlier captures.

linear

Buffer stops capture when the packet-count value is reached.

clear

Clears the packet buffer.

all

Captures DHCP packets on all interfaces.

interface

Represents a valid interface such as Ethernet or port channel.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Work closely with Extreme Networks technical support when running **debug** or **show system internal** commands and interpreting their results.

This command configures the capturing buffer behavior by allowing captures to wrap and overwrite earlier captures or stop capturing when a packet-count limit is reached. The current buffer content is cleared when the configuration changes.

Use the no form of this command to disable debugging.

Examples

The following example configures a buffer to capture 510 maximum packets in a circular fashion.

```
device# debug dhcp packet buffer circular packet-count 510
```

debug dot1x packet

Displays processing information related to IEEE 802.1X port-based access control.

Syntax

debug dot1x packet { **all** | **interface ethernet** *slot/port* } [**detail**] [**both** | **rx** | **tx**]

no debug dot1x packet { **all** | **interface ethernet** *slot/port* }

Parameters

all

Causes the display of information for all interfaces.

interface

Causes the display of information for a specific interface.
ethernet *slot/port*

Specifies an Ethernet interface in slot and port number format; when the device does not contain slots, the slot number must be 0.

detail

Causes the display of detailed information.

both

Causes the display of information about received and transmitted packets. By default, information about both received and transmitted packets is displayed.

rx

Causes the display of information about only received packets.

tx

Causes the display of information about only transmitted packets.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Work closely with Extreme Networks technical support when running **debug** or **show system internal** commands and interpreting their results.

The **no** form of the command disables the display of processing information related to IEEE 802.1X port-based access control.

Examples

The following example shows how to display detailed processing information related to IEEE 802.1X port-based access control for all interfaces.

```
device# debug dot1x packet all detail

2017/04/26-04:16:35.131863 [DOT1X]: [EAP-Request]: TX SA(609c.9f5a.251e)
DA(0180.c200.0003) Port: Ethernet 0/6 Type: Identity
```

The follow example shows how to disable the display of processing information related to IEEE 802.1X port-based access control for port 0/1.

```
device# no debug dot1x packet interface ethernet 0/1
```

debug ip bgp

Displays information related to the processing of BGP4, with a variety of options.

Syntax

debug ip bgp { **cli** | **dampening** | **events** | **general** | **graceful-restart** | **ip-prefix** *ip-addr/mask-len* | **ip-prefix-list** *name* | **keepalives** | **route-map** *name* | **route-selection** | **traces** | **updates** [**rx** | **tx**] } [**all-vrfs** | **vrf** *vrf-name*]

no debug ip bgp

Parameters

cli

Displays information about BGP CLI

dampening

Displays BGP4 dampening.

events

Displays all BGP4 events.

general

Displays BGP4 common events.

graceful-restart

Displays BGP graceful restart events.

ip-prefix

Displays information filtered by IP prefix.

ip-addr

IPv4 address in dotted-decimal notation.

mask-len

IPv4 mask length in CIDR notation.

ip-prefix-list

Displays information filtered by IP prefix list.

name

Name of IP prefix list.

keepalives

Displays BGP4 keepalives.

route-map

Displays configured route map tags.

name

Name of route map.

route-selection

Displays BGP4 route selection.

traces

Displays BGP traces.

updates

Displays BGP4 updates.

rx

Displays BGP4 received updates.

tx

Displays BGP4 transmitted updates

all-vrfs

Specifies all VRFs.

vrf

Specifies a VRF instance or all VRFs.

vrf-name

Specifies a VRF instance

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Work closely with Extreme Networks technical support when running **debug** or **show system internal** commands and interpreting their results.

If you want to see BGP4 keepalives for a specific neighbor, you must first specify the neighbor using the **debug ip bgp neighbor** command. Only keepalive traces for the specified neighbor will appear in the debugging message.

The **no** form of the command disables debugging.

Examples

The following example sets debugging on BGP4 events.

```
device# debug ip bgp events
```

The following example sets debugging on BGP4 graceful restart events.

```
device# debug ip bgp graceful-restart
```

The following example specifies that BGP4 keepalives for a specified neighbor appear in debugging messages.

```
device# debug ip bgp keepalive
device# debug ip bgp neighbor 10.1.1.1
```

The following example sets debugging on BGP4 events for VRF instance "red".

```
device# debug ip bgp events vrf red
```

debug ip bgp neighbor

Displays information related to the processing of BGP4 for a specific neighbor.

Syntax

debug ip bgp neighbor *ip-addr* [**all-vrfs** | **vrf** *vrf-name*]

no debug ip bgp neighbor *ip-addr* [**all-vrfs** | **vrf** *vrf-name*]

Parameters

ip-addr

IPv4 address in dotted-decimal notation.

all-vrfs

Specifies all VRFs.

vrf

Specifies a VRF instance or all VRFs.

vrf-name

Specifies a VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Work closely with Extreme Networks technical support when running **debug** or **show system internal** commands and interpreting their results.

The **no** form of the command disables debugging.

Examples

The following example sets debugging on information related to the processing of BGP4 for a specific neighbor.

```
device# debug ip bgp neighbor 10.11.12.13
```

The following example specifies that BGP4 keepalives for a specified neighbor appear in debugging messages.

```
device# debug ip bgp keepalive
device# debug ip bgp neighbor 10.1.1.1
```

The following example sets debugging on information related to the processing of BGP4 for a specific neighbor for VRF instance "red".

```
device# debug ip bgp neighbor 10.11.12.13 vrf red
```

The following example sets debugging information related to the processing of BGP4 for a specific neighbor for all VRFs.

```
device# debug ip bgp neighbor 10.11.12.13 all-vrfs
```

debug ip igmp

Enables or disables debugging for IGMP information.

Syntax

debug ip igmp { **all** | **errors** | **group** *A.B.C.D* | **packet** | **rx** | **tx** | **interface** *ethernet* | *port-channel tunnel* | **vlan** *vlan_id* | **bridge-domain** *bd_id* }

no debug ip igmp

Parameters

all

Enables all debugs.

errors

Enables only error type debugs, such as memory allocation failures.

group *A.B.C.D*

Specifies the group address, as a subnet number in dotted decimal format (for example, 10.0.0.1), as the allowable range of addresses included in the multicast group.

packet

Enables debug for queries or reports per the chosen option.

rx

Specifies only ingressing flow debugs to be captured in traces.

tx

Specifies only egressing packet flows to be captured in traces.

interface

Specifies the interface (ethernet, port-channel, tunnel) to be monitored.

vlan

Specifies the VLAN to be monitored.

bridge-domain

Specifies the bridge domain to be monitored.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Work closely with Extreme Networks technical support when running **debug** or **show system internal** commands and interpreting their results.

When debugging is enabled, all of the IGMP packets received and sent and IGMP-host related events are displayed.

The **no** form of this command disables debugging.

Examples

The following example enables error debug flags.

```
device# debug ip igmp error
```

debug ip ospf shortcuts

Enables IP OSPF Shortcuts related debugs in the RAS traces.

Syntax

debug ip ospf shortcuts

Parameters

None

Modes

Privilege Execution Mode

Examples

This example shows how to enable IP OSPF shortcuts related debugging.

```
SLX# debug ip ospf shortcuts
SLX#
```

debug ip pim

Enables debugging for IP Protocol Independent Multicast.

Syntax

debug ip pim { **add-del-oif** | **bootstrap** | **group** | **join-prune** | **nbr-change** | **packets** | **parent** | **regproc** | **route-change** | **rp** | **source** | **state** | **all** }

no debug ip pim all

Command Default

All flags are disabled.

Parameters

add-del-oif

Controls the OIF change flag.

bootstrap

Controls the bootstrap processing flag.

group

Controls the processing for a group flag.

join-prune

Controls the Join/Prune processing flag.

nbr-change

Controls the neighbor changes flag.

packets

Controls the packet processing flag.

parent

Controls the parent change processing flag.

regproc

Controls the register processing flag.

route-change

Controls the route changes flag.

rp

Controls the Rendezvous Point (RP) processing flag.

source

Controls the processing for a source flag.

state

Controls the state processing flag.

all

Controls all of the states.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Work closely with Extreme Networks technical support when running **debug** or **show system internal** commands and interpreting their results.

Use the **no debug ip pim all** command to disable debugging.

debug ipv6 bgp

Displays debug information related to BGP processing for IPv6 prefix lists.

Syntax

debug ipv6 bgp ipv6-prefix *ipv6-address /mask* [**all-vrfs** | **vrf** *vrf-name*]

debug ipv6 bgp ipv6-prefix *name* [**all-vrfs** | **vrf** *vrf-name*]

debug ipv6 bgp ipv6-prefix-list *name* [**all-vrfs** | **vrf** *vrf-name*]

no debug ipv6 bgp ipv6-prefix *ipv6-address /mask* [**all-vrfs** | **vrf** *vrf-name*]

no debug ipv6 bgp ipv6-prefix *name* [**all-vrfs** | **vrf** *vrf-name*]

no debug ipv6 bgp ipv6-prefix-list *name* [**all-vrfs** | **vrf** *vrf-name*]

Parameters

ipv6-address /mask

Specifies an IPv6 address and network mask.

all-vrfs

Specifies all VRFs.

vrf

Specifies a VRF instance or all VRFs.

vrf-name

Specifies a VRF instance

name

Specifies a prefix list name.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Work closely with Extreme Networks technical support when running **debug** or **show system internal** commands and interpreting their results.

Use the no form of this command to disable debugging.

Examples

This example enables debugging for IPv6 prefix list "myv6list" for VRF instance "red".

```
device# debug ipv6 bgp ipv6-prefix-list myv6list vrf red
```

This example enables debugging for a specified IPv6 address for all VRFs.

```
device# debug ipv6 bgp ipv6-prefix 2001::/16 all-vrfs
```

debug ipv6 bgp neighbor

Displays debug information related to BGP processing for a specified neighbor.

Syntax

debug ipv6 bgp neighbor *ipv6-addr* [**all-vrfs** | **vrf** *vrf-name*]

no debug ipv6 bgp neighbor *ipv6-addr* [**all-vrfs** | **vrf** *vrf-name*]

Parameters

ipv6-addr

IPv6 address of a neighbor.

all-vrfs

Specifies all VRFs.

vrf

Specifies a VRF instance or all VRFs.

vrf-name

Specifies a VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Work closely with Extreme Networks technical support when running **debug** or **show system internal** commands and interpreting their results.

The **no** form of the command disables debugging.

Examples

The following example sets debugging for a neighbor.

```
device# debug ipv6 bgp neighbor 2000::1
```

The following example specifies that BGP keepalives for a specified neighbor appear in debugging messages.

```
device# debug ip bgp keepalive
device# debug ipv6 bgp neighbor 2001::1
```

The following example sets debugging for a neighbor for VRF instance "red".

```
device# debug ipv6 bgp neighbor 2000::1 vrf red
```

The following example sets debugging for a neighbor for all VRFs.

```
device# debug ipv6 bgp neighbor 2000::1 all-vrfs
```

debug ipv6 dhcp pd

Sets the debugging parameters for the DHCP PD feature.

Syntax

debug ipv6 dhcp pd { **all** | **datafile** | **pd-option** | **rib** }

Command Default

None

Parameters

all

Enables all Prefix Delegation debugging.

datafile

Enables Prefix Delegation debugging and writing to the *iphelperv6_delegated_prefixes_data* file.

pd-option

Enables debugging for processing Prefix Delegation options in the DHCPv6 messages.

rib

Enables debugging the DHCPv6 interface with the RIB module.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Work closely with Extreme Networks technical support when running **debug** or **show system internal** commands and interpreting their results.

This command enable debugging of DHCPv6 Prefix Delegation and configures its debugging parameters.

Use the no form of this command to disable debugging.

Examples

The following debug command enables capturing debug information for DHCPv6 Prefix Delegation.

```
SLX# debug ipv6 dhcp pd all
```

debug ipv6 mld

Enables IPv6 MLD debug flags.

Syntax

debug ipv6 mld { **errors** | **group** | **interface** | **l2-port** | **packet** | **rx** | **tx** | **vlan** | **all** }

no debug ipv6 mld { **errors** | **group** | **interface** | **l2-port** | **packet** | **rx** |**tx** | **vlan** | **all** }

Command Default

By default, all debug flags are disabled.

Parameters

errors

Controls the error change flag.

group

Controls the multicast group processing flag.

interface

Controls the interface processing flag.

l2-port

Controls the Layer 2 port processing flag.

packet

Controls the packet processing flag.

rx

Controls the packet received processing flag.

tx

Controls the packet transmitted processing flag.

vlan

Controls the VLAN interface processing flag.

all

Controls the state of all the flags.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Work closely with Extreme Networks technical support when running **debug** or **show system internal** commands and interpreting their results.

The **no debug ipv6 mld all** form of the command disables all debug flags.

Examples

The following example shows the syntax for enabling all debug flags.

```
device# debug ipv6 mld all
```

The following example shows the syntax for disabling the interface flag.

```
device# no debug ipv6 mld interface
```

debug ipv6 ospf graceful-restart

Enables or disables graceful restart debugs for all VRFs or the specified VRF.

Syntax

debug ipv6 ospf graceful-restart {**all-vrfs** | **vrf** *vrf-name* }

no debug ipv6 ospf graceful-restart {**all-vrfs** | **vrf** *vrf-name* }

Parameters

all-vrfs

Specifies the IPv6 OSPFv3 debugs on all VRFs.

vrf *vrf-name*

Specifies the IPv6 OSPFv3 debugs on the indicated VRF.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Work closely with Extreme Networks technical support when running **debug** or **show system internal** commands and interpreting their results.

When this command is enabled, it begins logging debugs related to graceful restart.

Examples

This example enables debug logging for the VRF named "red."

```
device# debug ipv6 ospf graceful-restart vrf red
```

The following example disables the debugs on all VRFs.

```
device# no debug ipv6 ospf graceful-restart all-vrfs
```

debug ipv6 pim

Enables IPv6 PIM debug flags.

Syntax

debug ipv6 pim { **add-del-oif** | **bootstrap** | **group** | **join-prune** | **nbr-change** | **packets** | **parent** | **regproc** | **route-change** | **rp** | **source** | **state** | **all** }

no debug ipv6 pim { **add-del-oif** | **bootstrap** | **group** | **join-prune** | **nbr-change** | **packets** | **parent** | **regproc** | **route-change** | **rp** | **source** | **state** | **all** }

Command Default

By default, all debug flags are disabled.

Parameters

add-del-oif

Controls the OIF change flag.

bootstrap

Controls the bootstrap processing flag.

group

Controls the group processing flag.

join-prune

Controls the Join/Prune processing flag.

nbr-change

Controls the neighbor changes flag.

packets

Controls the packet processing flag.

parent

Controls the parent change processing flag.

regproc

Controls the register processing flag.

route-change

Controls the route changes flag.

rp

Controls the Rendezvous Point (RP) processing flag.

source

Controls the source processing flag.

state

Controls the state processing flag.

all

Controls the state of all the flags.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Work closely with Extreme Networks technical support when running **debug** or **show system internal** commands and interpreting their results.

The **no debug ipv6 pim all** form of the command disables all debug flags.

Examples

This example shows enables all debug flags.

```
device# debug ipv6 pim all
```

This example disables the Rendezvous Point flag.

```
device# no debug ipv6 pim rp
```

debug lacp

Enables or disables debugging for the Link Aggregation Control Protocol (LACP).

Syntax

debug lacp { **all** | **cli** | **event** | **ha** | **pdu** [**rx** { **all** | **interface ethernet** *slot/port* | **tx** { **all** | **sync** | **timer** | **trace level** *number* }

no debug lacp

Command Default

LACP debugging is disabled.

Parameters

all

Turns on all debugging.

cli

Turns on command line interface debugging.

event

Turns on event debugging.

ha

(Not currently supported) Echo HA events to the console.

pdu

Echo PDU content to the console.

rx all

Turns on debugging for received LACP packets on all interfaces.

rx interface

Turns on debugging for received LACP packets on the specified interface.

interface

Specifies the interface to be monitored.

ethernet

Represents a valid, physical Ethernet interface.

slot

Specifies a valid slot number. The only valid value is 0.

port

Specifies a valid port number.

tx all

Turns on debugging for transmitted LACP packets on all interfaces.

tx interface

Turns on debugging for transmitted LACP packets on the specified interface.

sync

Echo synchronization to consoles.

timer

Echo timer expiration to console.

trace level *number*

Specifies the trace level number. Valid values range from 1 through 7.

Modes

Privileged EXEC mode

Usage Guidelines

Enter **terminal monitor** to display debugging outputs on a particular cmsh session.

Enter **no debug lacp** to disable LACP debugging.

Examples

To enable debugging of LACP PDUs for transmitted and received packets on all interfaces:

```
device# debug lacp pdu tx all

device # debug lacp pdu rx all

device# show debug lacp
LACP rx debugging is on
LACP tx debugging is on
```

debug lldp dump

Dumps debugging information for the Link Layer Discovery Protocol (LLDP) to the console.

Syntax

debug lldp dump { **all** | [**ethernet** *slot/port*] [**both**]] | [**detail** [**both** | **rx** | **tx**] }

Command Default

LLDP debugging is disabled.

Parameters

all

Dumps all information to the console.

ethernet

Represents a valid, physical Ethernet port.

slot

Specifies a valid slot number. The only valid value is 0.

port

Specifies a valid port number.

both

Turns on debugging for both transmit and receive packets.

detail

Turns on debugging with detailed information.

both

Turns on detailed debugging for both transmit and receive packets.

rx

Turns on detailed debugging for only received LLDP packets.

tx

Turns on detailed debugging for only transmitted LLDP packets.

Modes

Privileged EXEC mode

debug lldp packet

Enables or disables debugging for the Link Layer Discovery Protocol (LLDP).

Syntax

debug lldp packet { **all** | [**ethernet** *slot/port*] [**both**]] | [**detail** [**both** | **rx** | **tx**] }

no debug lldp packet { **all** | **interface ethernet** *slot/port* }

Command Default

LLDP debugging is disabled.

Parameters

all

Turns on LLDP packet debugging on all interfaces.

ethernet

Represents a valid, physical Ethernet port.

slot

Specifies a valid slot number. For devices that do not support linecards, specify **0**.

port

Specifies a valid port number.

both

Turns on debugging for both transmit and receive packets.

detail

Turns on debugging with detailed information.

both

Turns on detailed debugging for both transmit and receive packets.

rx

Turns on detailed debugging for only received LLDP packets.

tx

Turns on detailed debugging for only transmitted LLDP packets.

Modes

Privileged EXEC mode

Usage Guidelines

Enter **terminal monitor** to display debugging outputs on a particular cmsh session.

Enter **no debug lldp packet** to disable LLDP debugging.

Examples

To enable debugging of LLDP for both received and transmitted packets on the 10-gigabit Ethernet interface 0/1:

```
device# debug lldp packet interface ethernet 0/1 both

device# show debug lldp

LLDP debugging status:
Interface 0/1    : Transmit Receive
```

debug spanning-tree

Enables debugging for the Spanning Tree Protocol (STP).

Syntax

debug spanning-tree { **all** | **bpdu** [**rx** | **tx** [**all** | [**interface** { **ethernet** *slot/port* | **port-channel** *number* }

no debug spanning-tree { **all** | **bpdu** [**rx** | **tx** [**all** | [**interface** { **ethernet** *slot/port* | **port-channel** *number* }

Command Default

STP debugging is disabled.

Parameters

all

Turns on spanning tree packet debugging on all interfaces.

bpdu

Turns on Bridge Protocol Data Unit debugging.

rx

Turns on debugging for only received spanning-tree packets.

tx

Turns on debugging for only transmitted spanning-tree packets.

interface

Specifies an interface.

ethernet

Specifies an Ethernet interface.

slot

Specifies a valid slot number. Must be 0 if the switch does not contain slots.

port

Specifies a valid port number.

port-channel *number*

Specifies a port-channel.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Work closely with Extreme Networks technical support when running **debug** or **show system internal** commands and interpreting their results.

Enter **terminal monitor** to display debugging outputs.

Enter **no debug spanning-tree** to disable debugging.

Examples

To enable debugging of spanning-tree for both Rx and Tx on Ethernet interface 0/1:

```
device# debug spanning-tree bpdu rx interface ethernet 0/1

device# debug spanning-tree bpdu tx interface ethernet 0/1

device# show debug spanning-tree

MSTP debugging status:
Spanning-tree rx debugging is off
Eth 0/1 rx is on
Spanning-tree tx debugging is off
Eth 0/1 tx is on
```

debug udld packet

Enables debugging for the Unidirectional Link Detection (UDLD) protocol.

Syntax

debug udld packet { **all** | **interface ethernet** *slot/port* } { **both** | **rx** | **tx** }

no debug udld packet

Command Default

UDLD debugging is disabled.

Parameters

all

Activates UDLD debugging on all ports on the switch.

ethernet

Represents a valid, physical Ethernet type for all available Ethernet speeds.

slot/port

Specifies a valid slot and port number. For devices that do not support linecards, specify **0** for the slot.

both

Sets debugging for both received and transmitted packets.

rx

Sets debugging for received packets only.

tx

Sets debugging for transmitted packets only.

Modes

Privileged EXEC mode

Usage Guidelines

Diagnostic commands are developed and intended for specialized troubleshooting. Work closely with Extreme Networks technical support when running **debug** or **show system internal** commands and interpreting their results.

When debugging is enabled, UDLD PDUs are written to the console as they are transmitted and received on one or all ports.

Use the **show debug udld** command to view your current debug settings.

Use the **no** form of this command to turn off either all dumping of UDLD PDUs or dumping on a specific port.

Examples

To turn on debugging of transmitted packets on a specific ethernet interface:

```
device# debug udld packet interface ethernet 0/1 tx
```

default-information-originate (BGP)

Configures the device to originate and advertise a default BGP route.

Syntax

default-information-originate

no default-information-originate

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The no form of the command restores the default.

Examples

The following example originates and advertises a default BGP4 route.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# default-information-originate
```

The following example originates and advertises a default BGP4+ route for VRF "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# default-information-originate
```

default-information-originate (IS-IS)

Generates a default route into an Intermediate System-to-Intermediate System (IS-IS) routing domain.

Syntax

default-information-originate [**route-map** *name*]

no default-information-originate [**route-map** *name*]

Command Default

Disabled.

Parameters

route-map *name*

Specifies that the default route is generated if the route map is satisfied. The route map name can be from 1 through 63 characters in length.

Modes

IS-IS address-family IPv4 unicast configuration mode

IS-IS address-family IPv6 unicast configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command disables default route origination.

Examples

The following example generates a default external route into an IS-IS domain.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# default-information-originate
```

The following example generates a default external route into an IS-IS domain if the route map “myroutemap” is satisfied.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv6 unicast
device(config-router-isis-ipv6u)# default-information-originate route-map myroutemap
```

default-information-originate (OSPFv2)

Controls distribution of default information to an OSPFv2 device.

Syntax

default-information-originate [**always**] [**metric** *metric*] [**metric-type** { **type1** | **type2** }] [**route-map** *name*]

no default-information-originate

Command Default

The default route is not advertised into the OSPFv2 domain.

Parameters

always

Always advertises the default route. If the route table manager does not have a default route, the router advertises the route as pointing to itself.

metric *metric*

specifies the cost for reaching the rest of the world through this route. If you omit this parameter and do not specify a value using the *default-metric* router configuration command, a default metric value of 1 is used. Valid values range from 1 through 65535. The default is 10.

metric-type

Specifies how the cost of a neighbor metric is determined. The default is **type1**. However, this default can be changed with the **metric-type** command.

type1

Type 1 external route.

type2

Type 1 external route,

route-map *name*

Specifies that the default route is generated if the route map is satisfied. This parameter overrides other options. If the **set metric** and **set metric-type** commands are specified in the route-map, the command-line values of metric and metric-type if specified, are “ignored” for clarification.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

This configuration provides criteria for the redistribution of any default routes found in the route table manager (RTM),whether static or learned from another protocol, to its neighbors.

The corresponding route-map should be created before configuring the **route-map** option, along with the **default-information-originate** command. If the corresponding route-map is not created beforehand, an error message is displayed stating that the route-map must be created.

The route-map option cannot be used with a non-default address in the match conditions. The default route LSA is not generated if a default route is not present in the routing table and a **match ip address** condition for an existing non-default route is configured in the route-map. The **match ip address** command in the route-map is a no-op operation for the default information originate command.

The **no** form of the command disables default route origination.

Examples

The following example creates and advertises a default route with a metric of 30 and a type 1 external route.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# default-information-originate metric 30
metric-type type1
```

default-information-originate (OSPFv3)

Controls distribution of default information to an OSPFv3 device.

Syntax

default-information-originate [**always**] [**metric** *metric*] [**metric-type** { **type1** | **type2** }]

no default-information-originate

Command Default

The default route is not advertised into the OSPFv3 domain.

Parameters

always

Always advertises the default route. If the route table manager (RTM) does not have a default route, the router advertises the route as pointing to itself.

metric *metric*

Used for generating the default route, this parameter specifies the cost for reaching the rest of the world through this route. If you omit this parameter, the value of the **default-metric** command is used for the route. Valid values range from 1 through 65535.

metric-type

Specifies the external link type associated with the default route advertised into the OSPF routing domain.

type1

The metric of a neighbor is the cost between itself and the router plus the cost of using this router for routing to the rest of the world.

The default is **type1**.

type2

The metric of a neighbor is the total cost from the redistributing routing to the rest of the world.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

This configuration provides criteria for the redistribution of any default routes found in the RTM (whether static or learned from another protocol) to its neighbors.

The **no** form of the command disables default route origination.

Examples

The following example specifies a metric of 20 for the default route redistributed into the OSPFv3 routing domain and an external metric type of Type 2.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# default-information-originate metric 20
metric-type type2
```

default-ipv6-gateway

Configures the IPv6 address of the default gateway on a VLAN.

Syntax

default-ipv6-gateway *ipv6-address* [*metric*]

no default-ipv6-gateway

Parameters

ipv6-address

IPv6 address of the default gateway.

metric

A decimal value from 1 through 5.

Modes

VLAN configuration mode

Usage Guidelines

A device should have a default gateway, for the following reasons:

- Although IPv6 discovers neighbors and routes dynamically, in some cases Router Advertisement (RA) and Router Solicitation (RS) operations are disabled and a default gateway is required to send traffic. RA and RS are not suppressed if a default gateway is confifured.
- Management devices (for example, TFTP servers, Telnet or SSH clients) are not members of the same subnet as the management IPv6 address.

If a management VLAN is not configured, the device can have only one IPv6 default gateway in the global configuration.

If a management VLAN is configured, the device can have a maximum of 5 IPv6 default gateways, with an optional metric (1 through 5), under the management VLAN. Multiple gateways can have the same metric value.

Configured gateway addresses and the default gateway address must be in same subnet.

The best default gateway is first chosen as the device whose neighbors are reachable (in the REACH state), in the sequence of metric values. Otherwise, the gateway with the highest priority (the lowest metric value) is chosen.

If a static default gateway is configured, that gateway takes precedence over the best default gateway configured by means of RA. If the static default-gateway configuration is removed, the best default gateway learned by RA is restored.

Use the **no** form of the command to remove the IPv6 address and disable the default gateway.

Selection of the best default router among configured IPv6 routers occurs under the following conditions:

- Disabling an interface
- Processing of an NA message receipt
- Adding or deleting an IPv6 neighbor to or from the neighbor list
- Configuring the IPv6 static default gateway by means of the CLI

The process of resolving the link layer for the IPv6 default gateway by sending NS occurs during the following conditions:

- Configuration of the default gateway configured by means of the CLI
- Addition or deletion of a management VLAN configuration

Examples

The following example configures the maximum of 5 IPv6 default gateways with the management VLAN configuration, and specifies metrics for each.

```
device# configure terminal
device(config)# vlan 66
device(config-vlan-66)# default-ipv6-gateway 2620:100:c:fe23:10:37:65:129 3
device(config-vlan-66)# default-ipv6-gateway 2620:100:c:fe23:10:37:65:129 2
device(config-vlan-66)# default-ipv6-gateway 2620:100:c:fe23:10:37:65:130 2
device(config-vlan-66)# default-ipv6-gateway 2620:100:c:fe23:10:37:65:131 1
device(config-vlan-66)# default-ipv6-gateway 2620:100:c:fe23:10:37:65:132 5
```

Use the **show ipv6** command to confirm the configuration and view the best default gateway (router).

```
device(config)# show ipv6
Global Settings
  IPv6 is enabled
  Link-local address(es):
    fe80::768e:f8ff:fef9:6d80 [Preferred]
  Global unicast address(es):
    2620:100:c:fe23:768e:f8ff:fef9:6d80 [Preferred],  subnet is 2620:100:c:fe23::/64
  Joined group address(es):
    ff02::1:fff9:6d80
    ff02::1
  Best Default Router : 2620:100:c:fe23:10:37:65:129 PMTUS : 0
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 3
  ND reachable time is 30000 miliseconds
  ND retransmit interval is 1000 miliseconds
  Current Hop Limit is 64
  Hosts use stateless autoconfig for addresses
  No Inbound Access List Set
  No Outbound Access List Set
  No IPv6 Domain Name Set
  No IPv6 DNS Server Address set
```

default-link-metric

Configures the metric value globally on all active Intermediate System-to-Intermediate System (IS-IS) interfaces for a specified address family.

Syntax

default-link-metric { **level-1** | **level-2** } *value*

no default-link-metric { **level-1** | **level-2** }

Command Default

Disabled.

Parameters

level-1

Specifies the default-link-metric parameter as Level 1.

level-2

Specifies the default-link-metric parameter as Level 2.

value

Specifies the default-link-metric value in metric style. The narrow metric range is from 1 through 63. The wide metric range is from 1 through 16777215. The default is 10.

Modes

IS-IS address-family IPv4 unicast configuration mode

IS-IS address-family IPv6 unicast configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

This command is useful when you have a common IS-IS metric value on all IS-IS interfaces (other than the default metric value of 10). This command is not applicable to MPLS IS-IS shortcuts and tunnel interfaces.

If you change the metric style configuration, the value of the default link metric also changes. The new value of the default link metric is equal to the minimum of the configured value and the maximum value supported by the new metric style. For example, if the metric style changes from wide metric to narrow metric, and the default-link-metric value is greater than 63, the default-link-metric value changes to 63 because it is the maximum value supported in the narrow metric style. When the metric style changes from a narrow metric to a wide metric, there is no change to the default-link-metric value.

You can change the metric value for a specific interface using the **isis metric** command or the **isis ipv6 metric** command. The **isis metric** command configuration takes precedence over the **default-link metric** *value* command configuration.

The **no** form of the command resets the metric value to the default value 10.

Examples

The following example configures the IS-IS default-link-metric value to 30 for Level 1 for the IPv4 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# default-link-metric level-1 30
```

The following example configures the IS-IS default-link-metric value to 30 for Level 1, and the IS-IS default-link-metric value to 40 for Level 2 for the IPv6 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family-ipv6 unicast
device(config-router-isis-ipv6u)# default-link-metric level-1 30
device(config-router-isis-ipv6u)# default-link-metric level-2 40
```

default-local-preference

Enables setting of a local preference value to indicate a degree of preference for a route relative to that of other routes.

Syntax

default-local-preference *num*

no default-local-preference

Parameters

num

Local preference value. Range is from 0 through 65535. The default is 100.

Modes

BGP configuration mode

Usage Guidelines

Local preference indicates a degree of preference for a route relative to that of other routes. BGP4 neighbors can send the local preference value as an attribute of a route in an UPDATE message.

Examples

The following example sets the local preference value to 200.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# default-local-preference 200
```

default-metric (BGP)

Changes the default metric used for redistribution.

Syntax

default-metric *value*

no default-metric

Command Default

The default metric value is 1.

Parameters

value

Metric value. Range is from 0 through 4294967295.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command restores the default.

Examples

The following example changes the default metric used for redistribution to 100.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# default-metric 100
```

default-metric (IS-IS)

Sets the default redistribution metric value for the Intermediate System-to-Intermediate System (IS-IS) routing protocol.

Syntax

default-metric *value*

no default-metric

Command Default

The default metric value is 0.

Parameters

value

Specifies the default metric value. Valid values range from 0 through 65535. The default is 0.

Modes

IS-IS address-family IPv4 unicast configuration mode

IS-IS address-family IPv6 unicast configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command resets the default metric value to the default value of 0.

Examples

The following example sets the default metric value to 20 for the IPv4 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# default-metric 20
```

The following example sets the default metric value to 40 for the IPv6 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv6 unicast
device(config-router-isis-ipv6u)# default-metric 40
```

default-metric (OSPF)

Sets the default metric value for the OSPFv2 or OSPFv3 routing protocol.

Syntax

default-metric *metric*

no default-metric

Parameters

metric

OSPF routing protocol metric value. Valid values range from 1 through 65535. The default is 10.

Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

This command overwrites any incompatible metrics that may exist when OSPFv2 or OSPFv3 redistributes routes. Therefore, setting the default metric ensures that neighbors use the correct cost and router computation.

The **no** form of the command restores the default setting.

Examples

The following example sets the default metric to 20 for OSPF.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# default-metric 20
```

default-passive-interface

Marks all OSPFv2 and OSPFv3 interfaces passive by default.

Syntax

default-passive-interface

no default-passive-interface

Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

When you configure the interfaces as passive, the interfaces drop all the OSPFv2 and OSPFv3 control packets.

You can use the **ip ospf active** and **ip ospf passive** commands in interface subconfiguration mode to change active/passive state on specific OSPFv2 interfaces. You can use the **ipv6 ospf active** and **ipv6 ospf passive** commands in interface subconfiguration mode to change the active and passive state on specific OSPFv3 interfaces.

The **no** form of the command disables the passive state.

Examples

The following example marks all OSPFv2 interfaces as passive.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# default-passive-interface
```

delay

For an implementation of an event-handler profile, specifies a delay from when a trigger is received until execution of the event-handler action.

Syntax

delay *seconds*

no delay

Command Default

There is no delay from when a trigger is received until execution of the event-handler action.

Parameters

seconds

Specifies the number of seconds from when a trigger is received until the execution of the specified action begins. Valid values are 0 or a positive integer.

Modes

Event-handler activation mode

Usage Guidelines

The **no** form of this command resets the **delay** setting to the default 0 seconds.

Examples

The following example specifies a delay of 60 seconds.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# delay 60
```

The following example resets **delay** to the default value of 0 seconds.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# no delay
```

delay-link-event

Configures the port transition hold timer to set a delay in the sending of port up or down port events, or both, to Layer 2 protocols.

Syntax

delay-link-event *multiple-iteration* { **down** | **up** | **both** }

no delay-link-event

Command Default

The sending of an up or down port event is not delayed.

Parameters

multiple-iteration

Specifies the number of times that the polling iteration occurs. Enter an integer from 1 to 200.

The polling iteration is 50 ms. The delay time is the *multiple-iteration* times 50 ms.

both

Sets the delay for the port down and up events.

down

Sets the delay for the port down event.

up

Sets the delay for the port up event.

Modes

Interface Ethernet configuration mode.

Usage Guidelines

Use the **no** form of the command to remove the delay from the port events on the interface.

While link down events are reported immediately in the Syslog, their effect on higher level protocols such as OSPF is delayed according to how the hold timer is configured. When configured, the timer affects the physical link events. However, the resulting logical link events are also delayed.

Note
All LAG member ports must have the same delayed-link-event configuration.

Note
The delayed-link-event configuration is applicable only on a physical interface. It is not valid on a VLAN, VE, LAG, or loopback interfaces.

Note
The port transition hold timer does not take effect when the interface is administratively shut down.

Examples

The following example shows the steps in the previous configuration.

```
device# configure terminal
device(config)# interface ethernet 4/2
device(conf-if-eth-4/2)# delay-link-event 2 down
```

delete

Deletes a user-generated file from the flash memory.

Syntax

delete *file*

Parameters

file

The name of the file to be deleted.

Modes

Privileged EXEC mode

Usage Guidelines

The delete operation is final; there is no mechanism to restore the file.

System configuration files cannot be deleted. If you try to delete a system configuration file, an appropriate message is displayed.

Examples

To delete a user-generated copy of a configuration file:

```
device# delete myconfig

% Warning: File will be deleted (from flash:)!
Continue?(y/n): y
```

delete-packet

Configures the logging or monitoring interval for all Traffic Management (TM) deleted packets on the SLX-OS device.

Syntax

delete-packet { **logging-interval** *minutes* } | { **threshold** *deleted-packets* }

no delete-packet logging-interval | **threshold**

Command Default

The logging interval is 60 minutes.

The default threshold is zero (0) deleted packets.

Parameters

logging-interval *minutes*

Specifies the logging interval in minutes. Enter an integer from from 10 to 2880.

threshold *deleted-packets*

Specifies the threshold limit for all deleted packets of the TM device. Enter a value from 0 to 10000. The value of 0 disables the monitoring of the all TM deleted packets.

Modes

System monitor TM configuration mode

Usage Guidelines

Use the **no** version of this command to reset the default interval or threshold values.

A RASlog message for the TM device statistics is generated within the logging interval similar to the following format:

```
M1 | Active, WARNING, SLX, TM threshold, Head deleted packets 34462
on device 3.1.1.
```

Examples

The following example configures the logging interval to 120 minutes.

```
device# configure terminal
device(config)# system-monitor tm
device(config-sys-mon-tm)# delete-packet logging-interval 120
```

The following example configures the threshold to 50 deleted packets.

```
device# configure terminal
device(config)# system-monitor tm
device(config-sys-mon-tm)# delete-packet threshold 50
```

deploy

Deploys the MCT cluster or cluster client.

Syntax

deploy

no deploy

Modes

Cluster configuration mode

Cluster client configuration mode

Cluster client PW configuration mode (SLX 9540 and SLX 9640 devices only)

Usage Guidelines

Before deploying a cluster, the cluster client must be configured.

Before deploying a cluster client, the client interface and ESI settings must be configured under the client configuration.

On the SLX 9540 and SLX 9640 devices:

- Before deploying a cluster PW client, the ESI value must be configured under the PW client configuration.
- An LSP is automatically created when you deploy a cluster. When you undeploy a cluster, the LSP is removed.

The client will not operate in MCT mode unless the remote client is also deployed.

The **no** form of the command undeploys the cluster or cluster client.

When the client is undeployed, all MAC addresses are removed locally and a withdraw message is sent to the MCT peer to remove all associated client MAC addresses.

Examples

The following example shows the deployment of a cluster.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# deploy
```

The following example shows the deployment of a cluster client.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# client MCT1-client 200
device(config-cluster-client-200)# deploy
```

On the SLX 9540 and SLX 9640 devices, the following example shows the deployment of a PW cluster client.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# client-pw
device(config-cluster-client-pw)# deploy
```

description (BD)

Specify a string that contains the description for a bridge-domain or multiple bridge-domains.

Syntax

description [*description-string*]

no description [*description-string*]

Parameters

description-string

Specifies the description in a string format. The space character between the description keyword and the *description-string* is allowed.

Modes

Global bridge-domain configuration mode.

Usage Guidelines

The **no description** of the command removes the description specified for a bridge-domain.

The **show bridge-domain** command displays an extra field in the output displaying the description of the bridge-domain.

Examples

The following example shows how to specify a description for bridge-domain 10.

```
device# configure terminal
device(config)# bridge-domain 10
device(config-bridge-domain-10)# description myBD10
```

description (event-handler)

Defines a description for an event-handler profile.

Syntax

description *description-text*

no description

Command Default

No description is defined.

Parameters

description-text

Characters describing the event-handler profile. The string can be 1 through 128 ASCII characters in length. Do not use the ? character. If you need to use ! or \, precede each with \.

Modes

Event-handler configuration mode

Usage Guidelines

An event-handler profile supports only one description.

To delete a description, use the **no** form of this command.

To change a description, you do not need to first delete the existing description. Just create a new description.

Examples

The following example defines a description for eventHandler1.

```
device# configure terminal
device(config)# event-handler eventHandler1
device(config-event-handler-eventHandler1)# description This is a sample description.
```

description (interfaces)

Specify a string that contains the description of a specified interface.

Syntax

description *line*

Parameters

line

Specifies characters describing the interface. The string must be between 1 and 63 ASCII characters in length.

Modes

Interface subtype configuration mode

Examples

To set the string describing internal Ethernet interface 3/2:

```
device# configure terminal
device(config)# interface ethernet 3/2
device(conf-if-eth-3/2)# description converged_101
```

description (LLDP)

Specifies a string that contains the LLDP description.

Syntax

description *string*

no description

Parameters

string

Characters describing LLDP. The string must be between 1 and 50 ASCII characters in length.

Modes

Protocol LLDP and profile configuration modes

Usage Guidelines

Enter **no description** to remove the LLDP description.

The LLDP description can also be configured for a specific LLDP profile. When you apply an LLDP profile on an interface using the **lldp profile** command, it overrides the global configuration. If a profile is not present, then the default global profile is used until you create a valid profile.

Examples

To set the strings describing LLDP:

```
device(conf-lldp)# description Extreme-LLDP
```

To set the strings describing LLDP for a specific LLDP profile, test2, enter the following:

```
device(conf-lldp)# profile test1
device(config-profile-test1)# description test2
```

description (STP)

Describes an xSTP configuration.

Syntax

description *description*

no description

Parameters

description

Characters describing the xSTP configuration. The string must be between 1 and 64 ASCII characters in length.

Modes

xSTP configuration mode

Usage Guidelines

Enter **no description** to remove the description.

Examples

To specify the bridge priority:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# description STP-S1

device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# description RSTP-S1

device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# description MSTP-S1
```

description (VRRP)

Describes a Virtual Router Redundancy Protocol extended (VRRP-E) interface.

Syntax

description *description*

no description

Parameters

description

Characters describing the VRRP-E interface. The string must be between 1 and 64 ASCII characters in length.

Modes

Virtual-router-group configuration mode

Usage Guidelines

Enter **no description** to remove the description.

Examples

To describe the VRRP-E group 10 interface:

```
device# configure terminal
device(config)# interface ve 25
device(config-ve-25)# vrrp-extended-group 10
device(config-vrrp-extended-group-10)# description vrrpe_group_10
```

designated-forwarder-hold-time

Configures the time in seconds to wait before electing a designated forwarder.

Syntax

designated-forwarder-hold-time *seconds*

designated-forwarder-hold-time

Command Default

The default setting is three seconds.

Parameters

seconds

Specifies the hold time in seconds. Enter an integer from 1 to 60.

Modes

Cluster configuration mode

Usage Guidelines

Use the **no** form of the command to reset the default setting of three seconds.

The designated forwarder is a PE in a set of multi-homing PEs connected to the same Ethernet segment that is responsible for sending BUM traffic to a client for a particular VLAN ID on an Ethernet segment.

DF election is not triggered unless at least one remote CCEP is configured. When a CCEP goes up or down, DF election is triggered as soon as the Ethernet route acknowledgment from remote peer is received.

When a client is deployed locally or remotely, or the BGP session comes up, the DF timer does not start and DF election is not performed until the timer expired.

Examples

The following example configures a 20-second hold time for DF election.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# designated-forwarder-hold-time 20
```

destination

Configures the destination address for the tunnel interface.

Syntax

destination *ip-address*

no destination *ip-address*

Command Default

No tunnel interface destination is configured.

Parameters

ip-address

Specifies the IPv4 address.

Modes

Interface tunnel configuration mode

Usage Guidelines

Use the **no tunnel destination** command to remove the destination configuration.

You must ensure that a route to the tunnel destination exists on the tunnel source device and create a static route if necessary.

Examples

This example configures the IP address 10.1.2.3 as the destination address.

```
device# configure terminal
device(config)# interface tunnel 5
device(config-intf-tunnel-5)# destination 10.1.2.3
```

dhcp ztp cancel

The Zero Touch Provisioning (ZTP) session indefinitely retries detecting the DHCP server to establish a network connection for firmware download. Once canceled, the ZTP session stops retrying.

Syntax

dhcp ztp cancel

Modes

Privileged EXEC mode

Usage Guidelines

By default, cancelling the ZTP session stops the session and stops all retry attempts, regardless of whether the process succeeds or not. If the firmware download has completed successfully, the device returns to Normal mode. The following limitations apply:

- If the firmware download has not started, you will need to reboot the switch manually to bring the switch back to normal mode.
- If the firmware download has already started, you must wait for firmware download to complete before running any other commands, power cycling the switch, starting a new firmware download, or starting a new ZTP session.
- If the firmware download completes and the switch fails to reboot, you must reboot the switch manually to bring the switch back to normal mode.

Examples

The following example cancels the ZTP retry.

```
device# dhcp ztp cancel
Warning: This command will terminate the existing ZTP session
Do you want to continue? [y/n] y
```

You can confirm that ZTP is canceled by running the **dhcp ztp cancel** command again. The output confirms that ZTP is disabled.

```
device# dhcp ztp cancel
ZTP is not enabled.
```

dhcp ztp log

Displays the Zero Touch Provisioning progress log.

Syntax

dhcp ztp log

Modes

Privileged EXEC mode

Usage Guidelines

The progress log displays if Zero Touch Provisioning is enabled.

Examples

The following example shows the ZTP progress log.

```
device# dhcp ztp log
ZTP, Wed Jun 29 17:32:36 2016, ========== ZTP start ==========
ZTP, Wed Jun 29 17:32:36 2016, disable raslog
ZTP, Wed Jun 29 17:32:36 2016, CLI is ready
ZTP, Wed Jun 29 17:33:11 2016, inband ports are enabled
ZTP, Wed Jun 29 17:33:11 2016, serial number = EXH3343L014
ZTP, Wed Jun 29 17:33:11 2016, model name = SLX9140
ZTP, Wed Jun 29 17:33:11 2016, use inband interfaces only
ZTP, Wed Jun 29 17:33:13 2016, get link down on all the interfaces
ZTP, Wed Jun 29 17:33:13 2016, retry in 10 seconds
ZTP, Wed Jun 29 17:33:23 2016, inband ports are enabled
ZTP, Wed Jun 29 17:33:24 2016, serial number = EXH3343L014
ZTP, Wed Jun 29 17:33:24 2016, model name = SLX9140
ZTP, Wed Jun 29 17:33:24 2016, use inband interfaces only
ZTP, Wed Jun 29 17:33:24 2016, get link down on all the interfaces
ZTP, Wed Jun 29 17:33:24 2016, retry in 10 seconds
ZTP, Wed Jun 29 17:33:34 2016, inband ports are enabled
ZTP, Wed Jun 29 17:33:34 2016, serial number = EXH3343L014
ZTP, Wed Jun 29 17:33:34 2016, model name = SLX9140
ZTP, Wed Jun 29 17:33:34 2016, use inband interfaces only
ZTP, Wed Jun 29 17:33:35 2016, checking inband interfaces link status
ZTP, Wed Jun 29 17:34:25 2016, find link up on intefaces: Eth0.6 Eth0.8
ZTP, Wed Jun 29 17:34:25 2016, start dhcp process on interfaces: Eth0.6 Eth0.8
ZTP, Wed Jun 29 17:34:34 2016, interface Eth0.8 receives dhcp response
ZTP, Wed Jun 29 17:34:34 2016, config ip address 192.169.0.147/24 on interface Eth0.8
ZTP, Wed Jun 29 17:34:39 2016, ping ftp server 192.169.0.2
ZTP, Wed Jun 29 17:34:40 2016, ping succeed
ZTP, Wed Jun 29 17:34:41 2016, download ZTP config file from ftp://192.169.0.2/config/
ztp.cfg
ZTP, Wed Jun 29 17:34:41 2016, receive ZTP configuration file [ztp.cfg]
ZTP, Wed Jun 29 17:34:41 2016, interface Eth0.8 connectivity test pass
ZTP, Wed Jun 29 17:34:41 2016, download script file [ztp.py]
ZTP, Wed Jun 29 17:34:41 2016, ZTP configuration sanity check pass
ZTP, Wed Jun 29 17:38:22 2016, ========== ZTP continue ==========
ZTP, Wed Jun 29 17:38:22 2016, disable raslog
ZTP, Wed Jun 29 17:38:22 2016, CLI is ready
ZTP, Wed Jun 29 17:38:58 2016, running configuration script [ztp.py]
```

```
ZTP, Wed Jun 29 17:39:25 2016, commit configuration
ZTP, Wed Jun 29 17:39:25 2016, ZTP succeed
ZTP, Wed Jun 29 17:39:25 2016, enable raslog
ZTP, Wed Jun 29 17:39:25 2016, ========== ZTP completed ==========
```

dir

Lists the contents of the device flash memory.

Syntax

dir

Modes

Privileged EXEC mode

Examples

The following example lists the contents of the flash memory.

```
device# dir
total 572
drwxr-xr-x 2  251 1011   4096 Jun  5 07:08 .
drwxr-xr-x 3  251 1011   4096 Mar 11 00:00 ..
-rw-r--r-- 1 root sys     410 Jun  3 00:56 defaultconfig.standalone
-rw-r--r-- 1 root sys     695 Jun  3 00:56 defaultconfig.cluster
-rw-r--r-- 1 root root 185650 Jun  5 09:38 startup-config
```

default-metric (IS-IS)

Sets the default redistribution metric value for the Intermediate System-to-Intermediate System (IS-IS) routing protocol.

Syntax

default-metric *value*

no default-metric

Command Default

The default metric value is 0.

Parameters

value

Specifies the default metric value. Valid values range from 0 through 65535. The default is 0.

Modes

IS-IS address-family IPv4 unicast configuration mode

IS-IS address-family IPv6 unicast configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command resets the default metric value to the default value of 0.

Examples

The following example sets the default metric value to 20 for the IPv4 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# default-metric 20
```

The following example sets the default metric value to 40 for the IPv6 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv6 unicast
device(config-router-isis-ipv6u)# default-metric 40
```

disable-adjacency-check

Disables Intermediate System-to-Intermediate System (IS-IS) IPv6 protocol-support consistency checks that are performed prior to forming adjacencies on hello packets.

Syntax

disable-adjacency-check

no disable-adjacency-check

Command Default

Disabled.

Modes

IS-IS address-family IPv6 unicast configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command re-enables the IS-IS IPv6 protocol-support consistency checks.

Examples

The following example disables the IS-IS IPv6 protocol-support consistency checks.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv6 unicast
device(config-router-isis-ipv6u)# disable-adjacency-check
```

The following example re-enables the IS-IS IPv6 protocol-support consistency checks.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv6 unicast
device(config-router-isis-ipv6u)# no disable-adjacency-check
```

disable-incremental-spf-opt

Disables incremental full SPF optimizations for Intermediate System-to-Intermediate System (IS-IS).

Syntax

disable-incremental-spf-opt

no disable-incremental-spf-opt

Command Default

Disabled.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

If you disable the partial SPF optimizations using the **disable-partial-spf-opt** command, IS-IS automatically disables the incremental SPF optimizations and always runs full SPF. However, if you disable incremental SPF optimizations using this command, IS-IS does not disable partial optimizations.

The **no** form of the command restores incremental SPF optimizations for IS-IS.

Examples

The following example disables incremental SPF optimizations for IS-IS.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# disable-incremental-spf-opt
```

The following example restores incremental SPF optimizations for IS-IS.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no disable-incremental-spf-opt
```

disable-inc-stct-spf-opt

Disables incremental shortcut LSP SPF optimization.

Syntax

disable-inc-stct-spf-opt

disable-inc-stct-spf-opt

Command Default

Disabled.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command restores incremental shortcut LSP SPF optimization.

Examples

The following example disables incremental shortcut LSP SPF optimization.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# disable-inc-stct-spf-opt
```

disable-partial-spf-opt

Disables partial SPF optimizations for Intermediate System-to-Intermediate System (IS-IS).

Syntax

disable-partial-spf-opt

no disable-partial-spf-opt

Command Default

Disabled.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

If you disable the partial SPF optimizations using this command, IS-IS automatically disables the incremental SPF optimizations and always runs full SPF. However, if you disable incremental SPF optimizations using the **disable-incremental-spf-opt** command, IS-IS does not disable partial optimizations.

The **no** form of the command restores partial SPF optimizations for IS-IS.

Examples

The following example disables partial SPF optimizations for IS-IS.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# disable-partial-spf-opt
```

The following example restores partial SPF optimizations for IS-IS.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no disable-partial-spf-opt
```

disallow-oar-ac

Allows multiple attachment circurit (AC) endpoints on a virtual router interface that is configured for a VPLS instance.

Syntax

disallow-oar-ac

no disallow-oar-ac

Command Default

A bridge domain created for a Virtual Private LAN Service (VPLS) application is also known as a VPLS instance. By default, multiple AC endpoints are allowed on a virtual router interface that is bound to a VPLS instance.

Modes

Router interface configuration mode.

Usage Guidelines

This feature is supported only on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

When multiple AC endpoints are not required on a VPLS instance and to help with system scaling of hardware resources, use this command to disallow multiple AC endpoints.

This command cannot be used when multiple AC endpoints already exist on the interface.

Use the **no** form of the command to restore the default configuration.

Examples

The following example shows how to bind a virtual router interface numbered 10 to a bridge domain numbered 5 and to then disallow multiple AC endpoints on router interface 10.

```
device# configure terminal
device(config)# bridge-domain 5
device(config-bridge-domain-5)# router interface 10
device(config-router-interface-10)# disallow-oar-ac
```

discard-packet

Configures the logging or monitoring interval for all Traffic Management (TM) discarded packets on the SLX-OS device.

Syntax

discard-packet { **logging-interval** *minutes* | **threshold** *discarded-packets* }

no discard-packet { **logging-interval** | **threshold** }

Command Default

The logging interval is 60 minutes.

The default threshold is zero (0) discarded packets.

Parameters

logging-interval *minutes*

Specifies the logging interval in minutes. Enter an integer from from 10 to 2880.

threshold *discarded-packets*

Specifies the threshold limit for all discarded packets of the TM device. Enter a value from 0 to 10000. The value of 0 disables the monitoring of the all TM device packets.

Modes

System monitor TM configuration mode

Usage Guidelines

Use the **no** version of this command to reset the default interval or threshold values.

A RASlog message for the TM device statistics is generated within the logging interval. The message consists of the time stamp, the number of discarded packets, and ingress slot, tower and core, similar to the following example:

```
device# show logging raslog reverse count 10
2017/01/05-10:56:58, [SYSD-1005], 788, M2 | Active | DCE, WARNING, SLX,  TM threshold,
Tail discarded packets 20734462 on device 3.1.1.
```

Examples

The following example configures the logging interval to 120 minutes.

```
device# configure terminal
device(config)# system-monitor tm
device(config-sys-mon-tm)# discard-packet logging-interval 120
```

The following example configures the threshold to 50 discarded packets.

```
device# configure terminal
device(config)# system-monitor tm
device(config-sys-mon-tm)# discard-packet threshold 50
```

discard-voq-packet

Configures the logging interval or threshold for all Virtual Output Queue (VOQ) discarded packets.

Syntax

discard-voq-packet { **logging-interval** *minutes* | **threshold** *discarded-packets* }

no discard-voq-packet { **logging-interval** | **threshold** }

Command Default

The logging interval is 60 minutes.

The default threshold is zero (0) discarded packets.

Parameters

logging-interval *minutes*

Specifies the logging interval in minutes. Enter an integer from from 10 to 2880.

threshold *discarded-packets*

Specifies the threshold limit for all VOQ discarded packets. Enter a value from 0 to 10000. The value of 0 disables the monitoring of the all VOQ packets.

Modes

System monitor TM configuration mode

Usage Guidelines

Use the **no** version of this command to reset the default interval or threshold values.

A RASlog message for the TM VOQ statistics is generated within the logging interval. The message consists of the time stamp, destination slot and port, priority, and ingress slot, tower and core, similar to the following example.

```
device# show logging raslog reverse count 100 | inc SYSD-1003
2017/01/05-11:03:59, [SYSD-1003], 793, M2 | Active | DCE, WARNING, SLX,  TM threshold
2017/01/05-11:00:34, Discarded packets 930587727, interface 3/2 prio 0 on device 3.1.0
```

The slot and port in the message determines the destination port that is congested at the ingress slot, tower, and core.

Examples

The following example configures the logging interval to 120 minutes.

```
device# configure terminal
device(config)# system-monitor tm
device(config-sys-mon-tm)# discard-voq-packet logging-interval 120
```

The following example configures the threshold to 50 discarded packets.

```
device# configure terminal
device(config)# system-monitor tm
device(config-sys-mon-tm)# discard-voq-packet threshold 50
```

distance (BGP)

Changes the default administrative distances for eBGP, iBGP, and local BGP.

Syntax

distance *external-distance internal-distance local-distance*

no distance

Parameters

external-distance

eBGP distance. Range is from 1 through 255.

internal-distance

iBGP distance. Range is from 1 through 255.

local-distance

Local BGP4 and BGP4+ distance. Range is from 1 through 255.

Modes

BGP configuration mode

Usage Guidelines

To select one route over another according to the source of the route information, the device can use the administrative distances assigned to the sources. The administrative distance is a protocol-independent metric that IP devices use to compare routes from different sources. Lower administrative distances are preferred over higher ones.

Examples

The following example configures the device to change the administrative distance.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# distance 100 150 200
```

distance (IS-IS)

Configures an administrative distance value for Intermediate System-to-Intermediate System (IS-IS) routes.

Syntax

distance *number*

no distance *number*

Command Default

The default is 115.

Parameters

value

Specifies the administrative distance. Valid values range from 1 through 255. The default is 115.

Modes

IS-IS address-family IPv4 unicast configuration mode

IS-IS address-family IPv6 unicast configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Routes with a distance value of 255 are not installed in the routing table.

The **no** form of the command resets the distance value to the default value of 115.

Examples

The following example sets an administrative distance of 40 for the IPv4 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# distance 40
```

The following example sets an administrative distance of 60 for the IPv6 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv6 unicast
device(config-router-isis-ipv6u)# distance 60
```

distance (OSPF)

Configures an administrative distance value for OSPFv2 and OSPFv3 routes.

Syntax

distance { **external** | **inter-area** | **intra-area** } *distance*

no distance

Command Default

The administrative distance value for OSPFv2 and OSPFv3 routes is 110.

Parameters

external

Sets the distance for routes learned by redistribution from other routing domains.

inter-area

Sets the distance for all routes from one area to another area.

intra-area

Sets the distance for all routes within an area.

distance

Administrative distance value assigned to OSPF routes. Valid values range from 1 through 255. The default is 110.

Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

You can configure a unique administrative distance for each type of OSPF route.

The distances you specify influence the choice of routes when the device has multiple routes from different protocols for the same network. The device prefers the route with the lower administrative distance. However, an OSPFv2 or OSPFv3 intra-area route is always preferred over an OSPFv2 or OSPFv3 inter-area route, even if the intra-area route's distance is greater than the inter-area route's distance.

The **no** form of the commands reverts to the default setting.

Examples

The following example sets the distance value for all external routes to 125.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# distance external 125
```

The following example sets the distance value for intra-area routes to 80.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# distance intra-area 80
```

The following example sets the distance value for inter-area routes to 90.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# distance inter-area 90
```

distribute

Enables advertisement of Border Gateway Protocol flow specification (BGP flowspec) rules that are configured under a route map.

Syntax

distribute *route-map-name*

no distribute *route-map-name*

Command Default

The advertisement of BGP flowspec rules is disabled.

Parameters

route-map-name

Name of a route map that is configured with the flowspec rules to be advertised.

Modes

BGP address-family IPv4 flowspec configuration mode

Usage Guidelines

The **no** form of the command disables advertisement of BGP flowspec rules.

Examples

The following example shows how to enable advertisement of flowspec rules configured under a route map named route_map_flowspec1 for the IPv4 address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 flowspec
device(config-bgp-ipv4fs)# distribute route_map_flowspec1
```

distribute-list prefix-list (OSPFv3)

Applies a prefix list to OSPF for IPv6 routing updates. Only routes permitted by the prefix-list can go into the routing table.

Syntax

distribute-list prefix-list *list-name* **in**

no distribute-list prefix-list

Command Default

Prefix lists are not applied to OSPFv3 for IPv6 routing updates.

Parameters

list-name

Name of a prefix-list. The list defines which OSPFv3 networks are to be accepted in incoming routing updates.

in

Applies the prefix list to incoming routing updates on the specified interface.

Modes

OSPFv3 router configuration mode

OSPFv3 VRF router configuration mode

Usage Guidelines

The **no** form of the command removes the prefix list.

Examples

The following example configures a distribution list that applies the filterOspfRoutes prefix list globally:

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# distribute-list prefix-list
filterOspfRoutes in
```

distribute-list route-map

Creates a route-map distribution list.

Syntax

distribute-list route-map *map* **in**

no distribute-list route-map

Parameters

map

Specifies a route map.

in

Creates a distribution list for an inbound route map.

Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The distribution list can filter Link State Advertisements (LSAs) received from other OSPF devices before adding the corresponding routes to the routing table.

The **no** form of the command removes the distribution list.

Examples

The following example creates a distribution list using a route map named filter1 that has already been configured.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# distribute-list route-map filter1 in
```

domain-name

Creates a maintenance domain at a specified level and name and enters the maintenance domain mode specified in the command argument.

Syntax

domain-name *name* **level** *level*

no domain-name *name* **level** *level*

Command Default

There is no domain configured.

Parameters

name

Specifies the domain name.

level *level*

Sets the domain level.

Modes

CFM protocol configuration mode

Usage Guidelines

The *name* parameter is case sensitive. The *level* parameter sets the domain level in the range 0 - 7. When the domain already exists, the level argument is optional. Typically, the levels are:

- Customer's Domain Levels: 5 - 7
- Provider Domain Levels: 3 - 4
- Operator Domain Levels: 0 – 2

The no form of the command removes the specified domain from the CFM protocol configuration mode.

Examples

```
device# configure terminal
device(config)# protocol cfm
device(config-cfm)# domain-name md1 level 4
device(config-cfm-md-md1)#
```

dot1ag-compliance

Enables IEEE 802.1ag (Dot1ag) compliance configuration mode to configure left and right interfaces, by associating MD name, MA name, MEP ID, and RMEP ID per interface for both ERP left and right interfaces for signal failure and recovery. This allows MDs, MAs, and MEPs to be configured as part of Dot1ag and to be associated with an Ethernet Ring Protection (ERP) instance to achieve faster convergence.

Syntax

dot1ag-compliance

no dot1ag-compliance

Command Default

IEEE 802.1ag compliance is not configured by default.

Modes

ERP configuration mode

Usage Guidelines

IEEE 802.1ag can be used to monitor ERP interfaces for signal failures. This command uses Dot1ag link status as a signal failure/recovery indication following a link status change on ERP ring interfaces, linking Dot1ag MEP status to ERP switching functionality.

Use the **no** form of this command to disable this feature.

Examples

The following example uses the **erp** command to enter Dot1ag compliance configuration mode. In this mode the user configures MD name, MA name, MEP ID, and RMEP ID per interface for both ERP left and right interfaces.

```
device# configure terminal
Entering configuration mode terminal
device(config-erp-2)# dot1ag-compliance
device(config-dot1ag-compliance)# left-interface domain-name md1 ma-name ma4 mep 2 remote-
mep 1
device(config-dot1ag-compliance)# right-interface domain-name md1 ma-name ma3 mep 1
remote-mep 2
```

The following example disables Dot1ag compliance.

```
device# configure terminal
device(config)# erp 1
device(config-erp-1)# no dot1ag-compliance
```

dot1x authentication

Enables 802.1x authentication on a port.

Syntax

dot1x authentication

no dot1x authentication

Command Default

802.1x authentication is disabled for ports.

Modes

Interface configuration mode

Usage Guidelines

Port control must be configured to activate authentication on an 802.1x-enabled interface using the **dot1x port-control auto** command from interface configuration mode.

Before activating the authentication using the **dot1x port-control auto** command on a port, you must remove configured static ACLs and static VLANs, if any, from the port.

Enter the **no dot1x authentication** command to disable dot1x on the port and remove the configuration from 802.1x management.

Examples

The following example enables 802.1x authentication on a specific port:

```
device# configure terminal
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x authentication
```

dot1x enable

Enables 802.1X authentication globally.

Syntax

dot1x enable

Command Default

802.1x authentication is not enabled.

Modes

Global configuration mode

Usage Guidelines

The **dot1x enable** command enables 802.1x authentication globally on all ports.

Note
802.1x port authentication is not supported by LAG (Link Aggregation Group) or interfaces that participate in a LAG.

Examples

The following example enables 802.1X authentication globally on all interfaces.

```
device(config)# dot1x enable
```

dot1x filter-strict-security

Enables or disables strict filter security for dot1x authentication on the interface.

Syntax

dot1x filter-strict-security

no dot1x filter-strict-security

Command Default

Strict filter security is enabled.

Modes

Interface configuration mode

Usage Guidelines

By default, strict security mode is enabled; that is the client is not authenticated if the Filter-Id attribute returned by RADIUS contains invalid information, or if insufficient system resources are available to implement the IP ACLs or MAC address filters.

When strict security mode is enabled:

- If the Filter-Id attribute in the Access-Accept message contains a value that does not refer to an existing filter (that is, a MAC address filter or IP ACL configured on the device), then the client will not be authenticated, regardless of any other information in the message (for example, if the Tunnel-Private-Group-ID attribute specifies a VLAN on which to assign the port).
- If the Vendor-Specific attribute specifies the syntax for a filter, but there are insufficient system resources to implement the filter, then the client will not be authenticated.
- If the device does not have the system resources available to dynamically apply a filter to a port, then the client will not be authenticated.

When strict security mode is disabled:

- If the Filter-Id attribute in the Access-Accept message contains a value that does not refer to an existing filter (that is, a MAC address filter or IP ACL configured on the device), then the client is still authenticated, but no filter is dynamically applied to it.
- If the Vendor-Specific attribute specifies the syntax for a filter, but there are insufficient system resources to implement the filter, then the client is still authenticated, but the filter specified in the Vendor-Specific attribute is not applied to the port.

The **no** form of the command disables strict filter security.

Examples

The following example enables strict filter security.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x filter-strict-security
```

dot1x max-req

Configures the retransmission parameter that defines the maximum number of times EAP request/challenge frames are retransmitted when EAP response/identity frame is not received from the client.

Syntax

dot1x max-req *count*

no dot1x max-req *count*

Command Default

The device retransmits the EAP-request/challenge twice.

Parameters

count

Specifies the number of EAP frame re-transmissions. Th range is from from 1 through 10. The default value is 2.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command disables this functionality.

Examples

The following example configures the device to retransmit an EAP-request/challenge frame to a client a maximum of three times.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x max-req 3
```

dot1x port-control

Controls port-state authorization and configures the port control type to activate authentication on an 802.1X-enabled interface.

Syntax

dot1x port-control { **auto** | **force-authorized** | **force-unauthorized** }

no dot1x port-control { **auto** | **force-authorized** | **force-unauthorized** }

Command Default

The default port state is auto.

Parameters

auto

Enables authentication on a port. It places the controlled port in the unauthorized state until authentication takes place between the client and authentication server. Once the client passes authentication, the port becomes authorized. This activates authentication on an 802.1X-enabled interface. The controlled port remains in the authorized state until the Client logs off.

force-authorized

Places the controlled port unconditionally in the authorized state, allowing all traffic to pass between the client and the authenticator. This also allows connection from multiple clients.

force-unauthorized

Places the controlled port unconditionally in the unauthorized state, denying any traffic to pass between the client and the authenticator.

Modes

Interface subtype configuration mode

Usage Guidelines

Before activating the authentication using the **dot1x port-control auto** command on a port, you must remove the configured static ACL and static VLANs, if any, from the port.

802.1x port authentication is not supported by LAG (Link Aggregation Group) or interfaces that participate in a LAG.

The **no** form of the command resets the port control type to the default state.

Examples

The following example configures the interface to place the port unconditionally in the unauthorized state until authentication takes place between the client and authentication server. Once the client passes authentication, the port becomes authorized.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x port-control auto
```

The following example configures the interface to place the controlled port unconditionally in the authorized state.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x port-control force-authorized
```

The following example configures the interface to place the controlled port unconditionally in the unauthorized state.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x port-control force-unauthorized
```

dot1x quiet-period

Configures the time interval that the device remains idle between a failed authentication and a reauthentication attempt.

Syntax

dot1x quiet-period *seconds*

no dot1x quiet-period

Command Default

The default quiet period is 60 seconds.

Parameters

seconds

Specifies the time between failed reauthentication and reauthentication attempt. Valid values range from 1 through 65535 seconds.

Modes

Interface configuration mode

Usage Guidelines

Changing the quiet-period interval time to a number lower than the default can result in a faster response time.

The **no dot1x quiet-period** command restores the default setting.

Examples

The following example sets the idle time as 200 seconds for the device before attempting reauthentication after an authentication failure.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x quiet-period 200
```

dot1x reauthenticate

Initiates 802.1X reauthentication on a specified interface.

Syntax

dot1x reauthenticate interface ethernet *slot/port*

Parameters

interface ethernet *slot/port*

Specifies a physical inteface ethernet port in terms of slot number and port nummber.

Modes

Privileged EXEC mode

Examples

The following example initiates reauthentication of a client connected to physical interface 1/1:

```
device# dot1x reauthenticate interface ethernet 1/1
```

dot1x reauthentication

Configures the device to periodically reauthenticate the clients connected to 802.1X-enabled interfaces at regular intervals.

Syntax

dot1x reauthentication

no dot1x reauthentication

Command Default

Periodic reauthentication is disabled.

Modes

Interface configuration mode

Usage Guidelines

When periodic reauthentication is enabled using the **dot1x reauthentication** command, the device reauthenticates the clients every 3,600 seconds by default.

The reauthentication interval is configurable using the **dot1x timeout re-authperiod** command. The reauthentication interval configured using the **dot1x timeout re-authperiod** command takes precedence.

The **no dot1x reauthentication** command disables periodic reauthentication.

Examples

The following example enables 802.1x reauthentication.

```
device# configure terminal
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x reauthentication
```

dot1x reauthMax

Sets the maximum number of times that a port attempts 802.1x reauthentication before the port changes to the unauthorized state.

Syntax

dot1x reauthMax *number*

no dot1x reauthMax

Command Default

The number of times that a port attempts 802.1x authentication is 2.

Parameters

number

Specifies the maximum number of reauthentication attempts before the port goes to the unauthorized state. Valid values range from 1 through 10.

Modes

Interface configuration mode

Usage Guidelines

The **no dot1x reauthMax** command restores the default setting.

Examples

The following example sets the maximum number of reauthentication attempts to 5.

```
device# configure terminal
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x reauthMax 5
```

dot1x test eapol-capable

Executes the 802.1x readiness check on the switch.

Syntax

dot1x test eapol-capable interface ethernet *slot/port*

Parameters

interface ethernet *slot/port*

Specifies a physical inteface ethernet port in terms of slot number and port nummber.

Modes

Privileged EXEC mode

Usage Guidelines

This command monitors 802.1x activity on all the switch ports and displays information about the devices connected to the ports that support 802.1x. You can use this feature to determine if the devices connected to the switch ports are 802.1x-capable. When you configure the **dot1x test eapol-capable** command on an 802.1x-enabled port, and the link comes up, the port queries the connected client about its 802.1x capability. When the client responds with a notification packet, it is designated as 802.1x-capable.

The readiness check can be sent on a port that handles multiple hosts (for example, a PC that is connected to an IP phone). The readiness check is not available on a port that is configured with the command **dot1x port-control force-unauthorized** .

The readiness check is typically used before 802.1x is enabled on the switch.

802.1x authentication cannot be initiated while the 802.1x readiness test is in progress.

The 802.1x readiness test cannot be initiated while 802.1x authentication is active.

802.1x readiness can be checked on a per-interface basis. Readiness check for all interfaces at once is not supported.

Examples

The following example configures readiness check on an interface to determine if the devices connected to the ports are 802.1x-capable.

```
device# dot1x test eapol-capable interface ethernet 1/1
device# 2016/07/18-00:49:03, [DOT1-1012], 5006, M2 | Active | DCE, INFO, sw0,
DOT1X_PORT_EAPOL_CAPABLE: Peer connected to port Ethernet 1/1 is EAPOL capable.
```

dot1x test timeout

Sets the 802.1X readiness test timeout.

Syntax

dot1x test timeout *timeout*

Command Default

The default readiness test interval is 10 seconds.

Parameters

timeout

Specifies the readiness test interval value in seconds. Valid values range from 1 through 65535.

Modes

Global configuration mode

Examples

The following example sets the test timeout to 30 seconds:

```
device(config)# dot1x test timeout 30
```

dot1x timeout

Configures the timeout parameters that determine the time interval for client reauthentication and EAP retransmissions.

Syntax

dot1x timeout {**re-authperiod** *seconds* | **supp-timeout** *seconds* | **tx-period** *seconds* }

no dot1x timeout {**re-authperiod** *seconds* | **supp-timeout** *seconds* | **tx-period** *seconds* }

Command Default

The timeout parameters are not applied to the device.

Parameters

re-authperiod *seconds*

Specifies the interval at which clients connected to 802.1X authentication enabled ports are periodically reauthenticated. When periodic reauthentication is enabled using the **dot1x reauthentication** command, the device reauthenticates the clients every 3,600 seconds by default. The re-authperiod option allows you to specify the time interval between reauthentication attempts. The reauthentication interval configured using the **dot1x timeout re-authperiod** command takes precedence.

supp-timeout *seconds*

Specifies the EAP response timeout for 802.1x authentication. By default, when the device relays an EAP-Request frame from the RADIUS server to the client, it expects to receive a response from the client within 30 seconds. If the client does not respond within the allotted time, the device retransmits the EAP-Request frame to the client. The timeout value for retransmission of EAP-Request frames to the client can be configured using the **supp-timeout** *seconds* parameters.

tx-period *seconds*

Specifies the EAP request retransmission interval, in seconds, with the client. By default, if the device does not receive an EAP-response/identity frame from a client, the device waits 30 seconds, then retransmits the EAP-request/identity frame. You can optionally change the amount of time the device waits before re-transmitting the EAP-request/identity frame to the client. If the client does not send back an EAP-response/identity frame within 60 seconds, the device will transmit another EAP-request/identity frame. The tx-period is a value from 1 through 4294967295. The default is 30 seconds.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of the command disables dot1x timeout.

Examples

The following example sets 25 seconds as the amount of time between reauthorization attempts on a specific interface.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x timeout re-authperiod 25
```

The following example sets 45 seconds as the switch-to-client retransmission time for the EAP request frame on a specific interface.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x timeout supp-timeout 45
```

The following example sets 34 seconds as the waiting period for a response to an EAP-request or identity frame from the client before retransmitting the request on a specific interface.

```
device(config)# interface Ethernet 1/1
device(conf-if-eth-1/1)# dot1x timeout tx-period 34
```

dpod

Manages Dynamic Ports on Demand (POD) assignments.

Syntax

dpod *slot/port* { **reserve** | **release** }

Parameters

slot

Specifies a slot number.

port

Specifies a port number.

reserve

Reserves a POD assignment for a port that is currently not able to come online but is expected to be viable in the future. A port license assignment that is reserved will be associated with the first port set that has a vacancy.

release

Removes a port from the port set to which it is currently assigned.

Modes

Global configuration mode

Usage Guidelines

A port POD assignment can only be released if the port is currently offline. Enter **shutdown** to take the port offline.

Do not release a port unless you plan to disconnect the optical link or disable the port persistently. If the link (server or optical) is left in a state where the port could be brought online, the Dynamic POD mechanism will detect this unassigned port and attempt to reassign it to a port set.

Examples

The following example reserves a POD assignment.

```
device# configure terminal
device(config)# dpod 8/15 reserve
device(config-dpod-8/15)# exit
```

The following example removes a port from a POD port set.

```
device# configure terminal
device(config)# dpod 8/15 release
```

```
device(config-dpod-8/15)# exit
```

dscp (QoS)

Defines the DSCP-to-EXP values for an MPLS QoS DSCP-to-EXP mutation map.

Syntax

dscp *dscp-value* **to exp** *exp-value*

no dscp *dscp-value*

Command Default

The default DSCP-EXP value.

```
dscp-exp map    'default' (dscp= d1d2)

 d1     : d2 0  1  2  3  4  5  6  7  8  9
 ------- --------------------------------
 0      :    0  0  0  0  0  0  0  0  1  1
 1      :    1  1  1  1  1  1  2  2  2  2
 2      :    2  2  2  2  3  3  3  3  3  3
 3      :    3  3  4  4  4  4  4  4  4  4
 4      :    5  5  5  5  5  5  5  5  6  6
 5      :    6  6  6  6  6  6  7  7  7  7
 6      :    7  7  7  7
```

Parameters

dscp-value

Specifies the DSCP value.

exp *exp-value*

Specifies the EXP value.

Modes

DSCP-EXP configuration mode

Usage Guidelines

After configuring the mutation mapping, you can apply the map globally.

Use the **no** form of the command to reset the DSCP value.

This command is supported on the Extreme 8820 and SLX 9740 devices only.

Examples

The following example defines the DSCP-to-EXP mutation map.

```
device# configure terminal
device(config)# qos-mpls map dscp-exp dscpExpMap
device(dscp-exp-dscpExpMap)# dscp 0 to exp 7
```

dscp (Tunnel)

Configures the tunnel differentiated services code point (DSCP).

Syntax

dscp *dscp-value*

no dscp

Parameters

dscp-value

Specifies the DSCP value. The range is from 0 to 63.

Command Default

The default value is 0.

Modes

Interface tunnel configuration mode

Usage Guidelines

Use the **no** form of this command to remove the DSCP configuration.

Examples

This example configures DSCP value for the tunnel interface.

```
device# configure terminal
device(config)# interface tunnel 5
device(config-intf-tunnel-5)# mode gre ip
device(config-intf-tunnel-5)# source 10.1.1.10
device(config-intf-tunnel-5)# source ve 4
device(config-intf-tunnel-5)# destination 10.1.1.11
device(config-intf-tunnel-5)# router-interface ve 3
device(config-intf-tunnel-5)# dscp-ttl-mode pipe
device(config-intf-tunnel-5)# dscp 10
```

dscp-ttl-mode

Configures tunnel differentiated services code point (DSCP) time to live (TTL) mode.

Syntax

dscp-ttl-mode { **pipe** | **uniform** }

no dscp-ttl-mode

Command Default

By default, set to pipe mode for all tunnels.

Parameters

pipe

Specifies pipe mode.

uniform

Specifies uniform mode.

Modes

Interface tunnel configuration mode

Usage Guidelines

Use the **no** form of this command to remove the QoS mode configuration.

Supporting the QoS mutation configuration on the VE is not supported.

Examples

This example shows how to configure the quality of service (QoS) mode.

```
device# configure terminal
device(config)# interface tunnel 5
device(config-intf-tunnel-5)# mode gre ip
device(config-intf-tunnel-5)# source 10.1.1.10
device(config-intf-tunnel-5)# source ve 4
device(config-intf-tunnel-5)# destination 10.1.1.11
device(config-intf-tunnel-5)# router-interface ve 3
device(config-intf-tunnel-5)# dscp-ttl-mode pipe
```

duplicate-mac-timer (EVPN default instance)

Configures a duplicate MAC detection timer for the detection of continuous MAC moves.

Syntax

duplicate-mac-timer *interval* **max-count** *interval*

no duplicate-mac-timer *interval* **max-count** *interval*

Parameters

interval

Specifies the duplicate MAC detection timer interval in seconds. Valid values range from 5 through 300. The default is 5.

max-count *value*

Specifies the maximum threshold of MAC moves that can occur within the configured time interval before the MAC address is treated as a duplicate address and further advertisements for that MAC address are blocked. Valid values range from 3 through 10. The default is 3.

Modes

EVPN instance configuration mode

Usage Guidelines

The **no** form of the command restores the default values.

Examples

The following example sets the duplicate MAC detection timer interval to 180 and the maximum count to 5 for the default EVPN instance.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# duplicate-mac-timer 180 max-count 5
```

The following example restores the default duplicate MAC detection timer and maximum count values.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# no duplicate-mac-timer
```

dynamic-bypass

The **dynamic-bypass** command enables dynamic bypass on a MPLS router or on an Ethernet interface.

Syntax

dynamic-bypass

no dynamic-bypass

Command Default

There is no dynamic bypass configuration in the default mode.

Modes

MPLS router configuration mode (config-router-mpls).

MPLS router MPLS interface dynamic bypass configuration mode (config-router-if-ethernet-*slot/port*).

Usage Guidelines

Dynamic bypass is enabled or disabled in the MPLS router using this command. Upon configuring this command, the configuration mode changes to dynamic bypass and enables dynamic bypass. If the dynamic bypass is already configured under router MPLS, then there is no change in the configured state of dynamic bypass.

Use the **dynamic-bypass** command to manually enable dynamic bypass on a MPLS interface.

A dynamic bypass LSP is created to protect an interface only when

1. The dynamic bypass is globally enabled AND
2. The global dynamic bypass **enable-all-interfaces** is configured OR interface level dynamic bypass is enabled.

The no form of the command in the MPLS router mode removes dynamic bypass from the MPLS router, and dynamic bypass is disabled in the system. The command deletes all configurations under the router mode dynamic bypass configuration block. This command brings down and deletes all the existing dynamic bypasses in the system.

The no form of the command in the interface mode deletes the dynamic bypass configuration from the MPLS interface and disables dynamic bypass on the interface when the MPLS router mode **enable-all-interfaces** is not configured.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

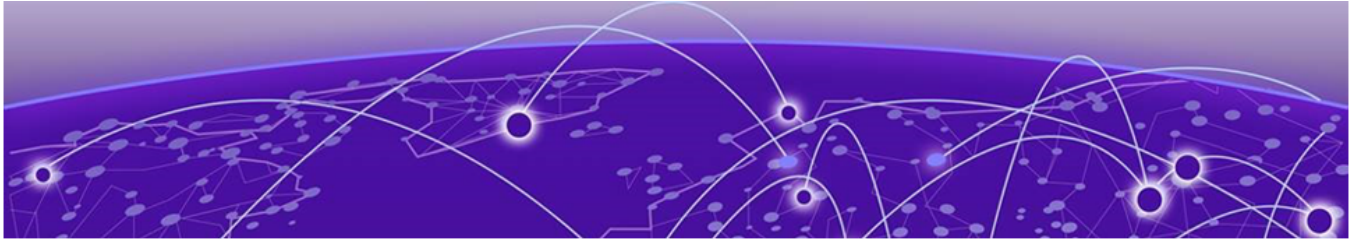
Examples

The following example enables dynamic bypass.

```
device>configure
device(config)# router-mpls
device(config-router-mpls)# dynamic-bypass
device(config-router-mpls-dynamic-bypass)#
```

The following example configures dynamic bypass on Ethernet interface *0/8*.

```
device>configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/8
device(config-router-mpls-if-ethernet-0/8)# dynamic-bypass
device(config-router-mpls-if-ethernet-0/8-dynamic-bypass)#
```



Commands E - F

efa deploy on page 541
enable on page 544
enable (ERP) on page 545
enable (GRUB) on page 546
enable (maintenance mode) on page 548
enable-on-reboot (maintenance mode) on page 549
enable (management-heartbeat) on page 550
encryption-level on page 552
enable-all-interfaces on page 553
enforce-first-as on page 554
eol on page 555
erp on page 556
error-disable-timeout enable on page 557
error-disable-timeout interval on page 558
esi on page 560
esi (BGP EVPN Multi-homing) on page 562
ethernet-segment on page 563
event on page 564
event-handler on page 566
event-handler abort action on page 568
event-handler activate on page 569
evpn on page 572
exclude-any on page 573
exclude-interface on page 575
exp on page 577
export-vrf-leaked-routes on page 579
export-map on page 580
extend bridge-domain on page 581
extend vlan on page 582
external-lsdb-limit (OSPFv2) on page 583
external-lsdb-limit (OSPFv3) on page 584
facility-backup on page 585
fast-convergence on page 587
fast-external-fallover on page 588

fast-flood on page 589
fastboot on page 590
fast-wtr-time on page 591
fec mode on page 592
fec (telemetry) on page 594
filter-change-update-delay on page 595
filter-fec-in on page 596
filter-fec-out on page 598
firmware activate on page 599
firmware commit on page 600
firmware download on page 601
firmware download ftp on page 604
firmware download fullinstall on page 606
firmware download interactive on page 609
firmware download scp on page 611
firmware download sftp on page 613
firmware download tftp on page 615
firmware download usb on page 617
firmware peripheral-update cpld on page 619
firmware peripheral-update fpga on page 620
firmware recover on page 621
firmware restore on page 622
flex-cli show link-fault-signaling on page 623
flex-cli show local-fault interface on page 624
flex-cli show local-fault slot on page 625
flex-cli show remote-fault interface on page 626
flex-cli show remote-fault slot on page 627
flow-label on page 628
flowspec validation on page 629
force-switch on page 631
format RFC-5424 on page 632
forward-delay on page 634
default-metric (IS-IS) on page 636
default-metric (IS-IS) on page 637

efa deploy

Deploys Extreme Fabric Automation (EFA) on TPVM. EFA can be deployed in one of *Graphics*, *No Graphics* or *Non Interactive* modes.

Syntax

efa deploy [**--graphics** | **nographics** | **non-interactive**]

efa deploy --graphics { *yes* | *no* [[**with-rollback**] **slx-peer-ip** *ipv4-address* **slx-peer-user** *user-name* **slx-peer-password** *user-password*] }

efa deploy nographics [**with-rollback**] **slx-peer-ip** *ipv4-address* **slx-peer-user** *user-name* **slx-peer-password** *user-password*

efa deploy non-interactive { **multi-node** | **single-node** | **with-rollback** }

efa deploy non-interactive multi-node package *path-to-efa-package-location* { **management-ip** | **peer-node** | **replacement-ip** }

efa deploy non-interactive multi-node package *path-to-efa-package-location* **management-ip sub-interface-name** *sub-interface-name* **sub-vlan-id** *sub-vlan-id* **external-subnet** *ipv4-address/mask* [**peer-node** | **replacement-ip**]

efa deploy non-interactive multi-node package *path-to-efa-package-location* **peer-node** *peer-tpvm-node-ipv4-address* **vip4** *virtual-ipv4-address* [**vip6** *virtual-ipv6-address*] [**management-ip** | **replacement-ip**]

efa deploy non-interactive multi-node package *path-to-efa-package-location* **replacement-ip** *replacement-ipv4-address* [**management-ip** | **peer-node**]

efa deploy non-interactive [**with-rollback**] **single-node package** *path-to-efa-package-location* **management-ip sub-interface-name** *sub-interface-name* **sub-vlan-id** *sub-vlan-id* **external-subnet** *ipv4-address/mask*

efa deploy non-interactive with-rollback slx-peer-ip *ipv4-address* **slx-peer-user** *user-name* **slx-peer-password** *user-password*

no efa deploy { **--graphics** | **nographics** }

Parameters

--graphics

yes

Deploy EFA in legacy mode with graphics support.

no

Deploy EFA in legacy mode without graphics support.

nographics

Deploy EFA using the no graphics mode.

non-interactive

Deploy EFA in the non interactive mode. In this mode EFA will be installed without any human interaction.

with-rollback

Enable rollback of deployment when deployment of EFA fails.

slx-peer-ip *ipv4-address*

The IPv4 address of the SLX peer device.

slx-peer-user *user-name*

The user name of the account used to access the peer SLX device.

slx-peer-password *user-password*

The password for the user account provided in the *slx-peer-user* field.

multi-node

Use this keyword when deploying EFA to more than one node.

package *path-to-efa-package-location*

The complete path to the EFA packager bundle.

peer-node *peer-tpvm-node-ipv4-address*

The IPv4 address of the peer TPVM node.

vip4 *virtual-ipv4-address*

The virtual IPv4 address of the peer TPVM node.

vip6 *virtual-ipv6-address*

The virtual IPv6 address of the peer TPVM node. This is an optional parameter.

management-ip

Use to configure additional Management IP related parameters.

sub-interface-name *sub-interface-name*

Configure the sub-interface within the management interface.

sub-vlan-id *sub-vlan-id*

Configure the sub VLAN ID for the management interface.

external-IP *ipv4-address/mask*

The IPv4 address and MASK for the external IP used to access the management interface.

replacement-ip *replacement-IP*

IP address of the peer node that will replace a faulty node in a Multi-Node deployment.

single-node

Deploy EFA to a single node.

Modes

Privileged EXEC mode

Usage Guidelines

The *no* form of this command removes a deployed EFA instance. You can choose between using the *Graphics* mode or the *No Graphics* mode.

Examples

The following example shows deploying or upgrading EFA on a Single node.

```
efa deploy non-interactive single-node package /efaboot/efa-2.7.0-16.tar.gz
```

The following example shows deploying or upgrading EFA on Multiple nodes.

```
efa deploy non-interactive multi-node package /efaboot/efa-2.7.0-16.tar.gz peer-node
10.20.246.102 vip4 10.20.246.103
```

The following example shows Multi node upgrade with replacement of a failed node.

```
efa deploy non-interactive multi-node package /efaboot/efa-2.7.0-16.tar.gz replacement-ip
10.200.246.155
```

enable

Enables the bypass LSP.

Syntax

enable

no enable

Command Default

The default value is disabled.

Modes

MPLS router bypass LSP configuration mode

Usage Guidelines

Enable the bypass LSP only after configuring the to-address and exclude-interface.

The **no** form of the command disables the bypass LSP.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example enables the bypass LSP with the name my-bypass-lsp.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# bypass-lsp my-bypass-lsp
device(config-router-mpls-bypass-lsp-my-bypass-lsp)# enable
```

enable (ERP)

Activates an Ethernet Ring Protection (ERP) instance by accepting the configurations and initializing protocol state machines.

Syntax

enable

no enable

Command Default

An ERP instance is not enabled by default.

Modes

ERP configuration mode

Usage Guidelines

Within an interconnected ring topology, in the major ring, you must first configure two interfaces. In a sub-ring, you must configure at least one interface before enabling the ERP instance.

Note
You must enable the major ring before enabling any sub-rings attached to the major ring (whose ERP ID is configured as parent-ring-id). Conversely, this order must be followed in reverse to disable an ERP instance.

Use the **no** form of this command to deactivate the ERP instance.

Examples

The following example configures a non-RPL node in a major ring.

```
device# configure terminal
device(config)# erp 1
device(config-erp-1)# right-interface vlan 2 e 1/2
device(config-erp-1)# left-interface vlan 2 e 1/1
device(config-erp-1)# enable
```

enable (GRUB)

Enables securing the GRUB bootloader with a password on the SLX device.

Syntax

enable

no enable

Command Default

By default, GRUB is not secured with a password. This command is used to explicitly enable this feature. Once enabled, the **username** command becomes available for configuring the username and password to secure GRUB.

Note
Reboot is required for this feature to take effect.

Modes

GRUB mode

Usage Guidelines

The `enable` command is executed to enable securing the GRUB with a username and password combination. When enabled, this username and password combination is applicable to the *ONIE* and *Offline Diagnostics* options of the GRUB menu and and GRUB environment “e” - edit the commands before booting and “c” - command-line. It is not applicable to the *SLX-OS* option of the GRUB menu. You can launch the SLX-OS without providing credentials.

When enabled, the password protection feature get enabled from the next reboot of the SLX device.

The **no** form of the command disables GRUB Password Protection. This is also applicable from the next reboot of the SLX device.

Examples

The following example enables the GRUB Password Protection.

```
SLX (config-grub)# enable
SLX (config-grub)#
```

GRUB Password Protection is enabled from the next reboot of the SLX device.

The following example disables GRUB Password Protection.

```
SLX (config-grub)# no enable
SLX (config-grub)#
```

enable (maintenance mode)

Enables the System Maintenance Mode.

Syntax

enable

no enable

Command Default

Maintenance Mode is not enabled by default.

Modes

System Maintenance mode

Usage Guidelines

The `no` form of the command disables maintenance mode.

Examples

This example navigates into the System Maintenance mode and forces the device into Maintenance Mode.

```
SLX # configure terminal
SLX (config) # system maintenance
SLX (config-system-maintenance)# enable
SLX (config-system-maintenance)#
```

enable-on-reboot (maintenance mode)

Configures the device to move into Maintenance Mode only when the device is rebooted.

Syntax

enable-on-reboot

no enable-on-reboot

Command Default

You must explicitly enable this option.

Modes

System Maintenance Mode

Usage Guidelines

When configured, the device will not enter into the System Maintenance Mode immediately. The device must be rebooted to enter into the maintenance mode.

Examples

This example show how to force the device to enter into System Maintenance Mode on being rebooted.

```
SLX # configure terminal
SLX (config) # system maintenance
SLX (config-system-maintenance)# convergence-time 250
SLX (config-system-maintenance)# enable-on-reboot
SLX (config-system-maintenance)# exit
SLX (config)#
```

This example shows how to remove the *enable-on-reboot* configuration.

```
 SLX # configure terminal
SLX (config) # system maintenance
SLX (config-system-maintenance)# no enable-on-reboot
SLX (config-system-maintenance)# exit
SLX (config)#
```

enable (management-heartbeat)

Enables Management Heartbeat mode on the SLX device.

Syntax

enable

no enable

Command Default

By default, Management Heartbeat mode is disabled. This command is used to explicitly enable this mode.

Modes

Management Heartbeat mode

Usage Guidelines

The `enable` command must only be executed after setting the desired threshold and action for the Management Heartbeat mode. This command can be executed immediately if you want to retain the default values for *threshold* and *action* for this mode. When this command is executed, the SLX device's *Admin* state becomes *UP*.

The **no** form of the command disables Management Heartbeat mode. However, the mode is not removed from the *running-config*.

Examples

The following example enables the Management Heartbeat mode.

```
SLX(config-management-heartbeat-manage) # enable
SLX(config-management-heartbeat-manage)# do show running-config management-heartbeat
manager
management-heartbeat manager
 enable
 threshold-timer 1
 action no-action

SLX(config-management-heartbeat-manage) #
```

The following example disables the Management Heartbeat mode.

```
SLX(config-management-heartbeat-manage) # no enable
SLX(config-management-heartbeat-manage)# do show running-config management-heartbeat
manager
management-heartbeat manager
 threshold-timer 1
 action no-action
```

```
SLX(config-management-heartbeat-manage) #
```

encryption-level

Configures the encryption level to use for communication with the Remote Authentication Dial-In User Service (RADIUS) server.

Syntax

encryption-level *encryption_level_value*

no encryption-level

Command Default

The default value is 7; the key is stored in encrypted format.

Parameters

encryption_level_value

Specifies the encryption level value for shared-secret key operation. Valid values are 0 and 7. A value of 0 sprecifies that the key is stored in cleartext format. A value of 7 specifies that the key is stored in encrypted format. The default value is 7.

Modes

RADIUS server host VRF configuration mode

Usage Guidelines

The **no** form of the command restores the command default value.

Note
Before downgrading to a software version that does not support the **encryption-level** command, set the encryption level value to 0. Otherwise, the firmware download displays an error requesting that the encryption level value be set to 0.

Examples

The following example shows how to specify an encryption level of 0; the shared secret key is stored in cleartext format

```
device# configure terminal
device(config)# radius-server host 10.37.73.180 use-vrf green-vrf
device(config-host-10.37.73.180/green-vrf)# encryption-level 0
```

enable-all-interfaces

Use the enable-all-interfaces command to enable dynamic bypass on all the MPLS interfaces. This command disables dynamic bypass on all interfaces where dynamic bypass is not disabled using the interface level commands. MPLS interface specific dynamic bypass configurations take precedence over this configuration.

Syntax

enable-all-interfaces

no enable-all-interfaces

Command Default

Disabled on all interfaces unless the user enables dynamic bypass on the MPLS interfaces.

Modes

MPLS router dynamic bypass configuration mode (config-router-mpls-dynamic-bypass).

Usage Guidelines

The **no** form of the command disables dynamic bypass on all interfaces where dynamic bypass is not enabled using the interface level commands.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example enables dynamic bypass on all interfaces.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# dynamic-bypass
device(config-router-mpls-dynamic-bypass)# enable-all-interfaces
```

enforce-first-as

Enforces the use of the first autonomous system (AS) path for external BGP (eBGP) routes.

Syntax

enforce-first-as

no enforce-first-as

Command Default

The device does not require the first AS listed in the AS_SEQUENCE field of an AS path update message from eBGP neighbors be the AS of the neighbor that sent the update.

Modes

BGP configuration mode

Usage Guidelines

The **no** form of the command disables this feature.

This command causes the router to discard updates received from eBGP peers that do not list their AS number as the first AS path segment in the AS_PATH attribute of the incoming route.

The device accepts the update only if the AS numbers match. If the AS numbers do not match, the device sends a notification message to the neighbor and closes the session. This requirement applies to all updates received from eBGP neighbors.

Examples

The following example configures the device to enforce the use of the first AS path.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# enforce-first-as
```

eol

Enables the end-of-lib configuration mode.

Syntax

eol

no eol

Modes

MPLS LDP configuration mode

Usage Guidelines

Use the **no** form of this command to remove this mode and attribute under it.

The end-of-lib mode contains all the attributes of the end of lib capability and notification. Also, when you enable the end-of-lib mode, you can determine whether the two RFCs 5561 and 5919 are enabled by the LSR.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example enables the end-of-lib configuration mode.

```
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# eol
device(config-router-mpls-ldp-eol)#
```

erp

Asigns an an Ethernet Ring Protection (ERP) ID and creates an ERP instance.

Syntax

erp *erp_id*

no erp *erp_id*

Command Default

An ERP instance is not configured by default.

Parameters

erp_id

Specifies an ERP instance. Range is from 1 through 255.

Modes

Global configuration mode

Usage Guidelines

You must assign an ERP ID. This ID number is used to do the following:

- Filter and clear statistics associated with a particular ERP ID
- Delete the nonrevertive mode in the case of an RPL owner
- Clear WTR and WTB timers

Use the **no** form of this command to delete the instance.

Examples

The following example specifies ERP instance 1 and enters ERP configuration mode.

```
device# configure terminal
device(config)# erp 1
device(config-erp-1)#
```

error-disable-timeout enable

Enables the timer to bring the interface out of the error-disabled state.

Syntax

error-disable-timeout enable

Modes

Spanning tree configuration mode

Usage Guidelines

When the Spanning Tree Protocol (STP) Bridge Protocol Data Unit (BPDU) guard disables a port, the port remains in the disabled state unless the port is enabled manually. This command allows you to enable the interface from the disabled state.

The command is the same regardless of which type of STP is enabled.

Examples

To bring the interface out of the disabled state:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# error-disable-timeout enable

device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# error-disable-timeout enable

device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# error-disable-timeout enable

device# configure terminal
device(config)# protocol spanning-tree pvst
device(conf-pvst)# error-disable-timeout enable

device# configure terminal
device(config)# protocol spanning-tree rpvst
device(conf-rpvst)# error-disable-timeout enable
```

error-disable-timeout interval

Sets the timeout interval for errors on an interface.

Syntax

error-disable-timeout interval *seconds*

no error-disable-timeout interval

Command Default

300 seconds

The timeout feature is disabled.

Parameters

seconds

Specifies the time for the interface to time out. Valid values range from 10 through 1000000 seconds.

Modes

Spanning tree configuration mode

Usage Guidelines

Enter **no error-disable-timeout interval** to return to the default setting.

The command is the same regardless of which type of STP is enabled.

Examples

Follow these examples to set the timeout interval.

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# error-disable-timeout interval 100

device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# error-disable-timeout interval 100

device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# error-disable-timeout interval 100

device# configure terminal
device(config)# protocol spanning-tree pvst
device(conf-pvst)# error-disable-timeout interval 100
```

```
device# configure terminal
device(config)# protocol spanning-tree rpvst
device(conf-rpvst)# error-disable-timeout interval 100
```

esi

Sets the Ethernet Segment ID (ESI) value, which is used to uniquely identify the client for the MCT client, or configures an auto-generated ESI value for a port channel client interface running LACP.

Syntax

esi {*HH:HH:HH:HH:HH:HH:HH:HH:HH:HH* | **auto lacp** }

no esi

Parameters

HH:HH:HH:HH:HH:HH:HH:HH:HH:HH

Specifies the 9-octect ESI value. Enter *HH* in hexadecimal format.

auto lacp

Configures an auto-generated ESI value for a port channel client interface running LACP.

Modes

Cluster client configuration mode

Cluster client PW configuration mode (SLX 9540 and SLX 9640 devices only)

Usage Guidelines

Use the **no** form of the command to delete the ESI setting for the client.

Only one ESI is allowed under a client.

You must configure the same ESI value on both devices in an MCT cluster.

For an MCT client, the configuration of the ESI value creates the MCT client LAG.

The same ESI cannot be added under multiple client entries.

The **esi auto lacp** command is available only in cluster client configuration mode. When a client interface is a port channel and LACP is running on the port channel, MCT supports an automatically-generated ESI value, as defined in RFC 7432. This ESI is encoded as type 1, as follows:

- 1-byte ESI type = 1
- 9-byte ESI value = 6-byte LACP system MAC address of the client followed by the 2-byte LACP port key, and then a 1-byte 0x00

The manually configured ESI uses type 0.

Examples

The following example shows the setting of the ESI value for the cluster client.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# client MCT1-client 200
device(config-cluster-client-200)# esi 00.a1.b2.c3.d4.e5.f6.89.00
```

The following example shows the configuration of an auto-generated ESI for the cluster client.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# client MCT1-client 200
device(config-cluster-client-200)# esi auto lacp
```

On the SLX 9540 and SLX 9640 devices, the following example shows the setting of the ESI for the cluster PW client.

```
device(config)# cluster MCT1 1
device(config-cluster-1)# client-pw
device(config-cluster-client-pw)# esi 01:02:03:04:05:06:07:08:0a
```

esi (BGP EVPN Multi-homing)

Ethernet Segment Identifier (ESI) is a 10-octet identifier value that denotes an Ethernet Segment. It is used to discover and group the various interfaces of a multi-homed client. This command is used to manually assign Ethernet Segment Identifier (ESI) value to the segment. The same local port-channel id should be used by the multi-homed leaf peers on links connected to the same host.

Syntax

esi *es-id*

[no] esi *es-id*

Parameters

es-id

The 10 digit ESI value. Manually assigned ESI values must be in Hexadecimal and should always start with *0x00*.

Modes

Ethernet Segment mode within Ethernet and Port-channel interface modes.

Usage Guidelines

Ethernet Segment Identifier is a 10-octet identifier value that denotes an Ethernet Segment. It is used to discover and group the various interfaces of a multi-homed client.

The [no] format of the command removes the Ethernet Segment Identifier value mapped to ethernet segment of the selected interface.

Examples

The following example shows the configuration of a leaf node with connections to two different multi-homed hosts.

```
SLX(config)# interface Ethernet 0/1
SLX(conf-if-eth-0/1)#ethernet-segment
SLX(conf-if-eth-0/1-es)# esi 00:11:22:33:44:55:66:77:88:99
SLX(config)# interface Port-channel 1
SLX(config-Port-channel-1)# ethernet-segment
SLX(config-Port-channel-1-es)# esi 00:11:11:22:22:33:33:44:44:55
```

ethernet-segment

When a host device connects to multiple leaf nodes in a fabric through its interfaces, the aggregation of these links is termed as an Ethernet Segment (ES). Each host is assigned an unique 10-octet Ethernet Segment Identifier (ESI) that identifies this aggregation of connected ports. The assigned ESI value is used to discover other leaf nodes within the same ESI. This command navigates into a new configuration mode within which all ES configuration must be done.
ESI values are not assigned to single homed nodes.

Syntax

ethernet-segment

[no] ethernet-segment

Modes

Ethernet and Port-Channel modes. Navigates into the Ethernet Segment configuration mode.

Usage Guidelines

The command indicates that the current interface is a part of an Ethernet Segment and an Ethernet Segment Identifier (ESI) value must be assigned to it.

The [no] function removes the current interface from the ES.

Examples

The following example creates the Ethernet-Segment for configuring and generating the Ethernet Segment Identifier (ESI) value for a multi-homed client. In this example, two different interfaces are configured. For each interface, the Ethernet Segment mode is enabled.

```
SLX(config)# interface Ethernet 0/1
SLX(conf-if-eth-0/1)#ethernet-segment
SLX(conf-if-eth-0/1-es)#
SLX(config)# interface Port-channel 1
SLX(config-Port-channel-1)# ethernet-segment
SLX(config-Port-channel-1-es)#
```

event

Configures an event and action.

Syntax

event{ *average-threshold* | *max-threshold* | *ccm-down* | *ccm-up* } **actions** { *interface-down* | *event-handler* | *all* }

no event

Parameters

average-threshold

Specifies average thereshold.

max-threshold

Specifies maximum thereshold.

ccm-down

Specifies CCM is down

ccm-up

Specifies CCM is up.

actions

Specifies the actions.

interface-down

Specifies interface down.

event-handler

Specifies event handler.

all

Specifies all.

Modes

Y1731 configuration mode

Usage Guidelines

Use the **no** form of the command delete the corresponding configured action profile also corresponding associations with Source and Target MEP pair.

Examples

This example shows how to create an action profile.

```
device# configure terminal
device(config)# protocol cfm
device(config-cfm)# y1731
```

```
device(config-cfm-y1731)# action-profile action-prof-act1
device((protocol-cfm)# event max-threshold actions all
```

event-handler

Creates or accesses an event-handler profile, which can execute a Python script when a specified trigger occurs.

Syntax

event-handler *event-handler-name* [**action python-script** *file-name*]

event-handler *event-handler-name* [**description** *description-text*]

event-handler *event-handler-name* [**trigger** *trigger-id* **raslog** *raslog-id* [**pattern** *posix-ext-regex*]]

no event-handler *event-handler-name*

Command Default

No event-handler profile is enabled.

Parameters

event-handler-name

Specifies the name of the event-handler profile. Valid values can have from 1 through 32 characters. The first character must be alphabetic.

action python-script *file-name*

Specifies a Python file that runs when a trigger-condition occurs. Valid values range from 4 through 32 characters (including the **.py** extension). The first character must be alphanumeric.

description *description-text*

Specifies a string describing the event-handler profile. The string can be 1 through 128 ASCII characters in length. Do not use the ? character. If you need to use ! or \, precede each with \.

trigger *trigger-id*

Defines an event-handler trigger and specifies an ID number for the trigger. Valid values are 1 through 100, and must be unique per event-handler profile. When the trigger-condition occurs, a Python script is run.

raslog *raslog-id*

Specifies a RASlog message ID as the trigger.

pattern *posix-ext-regex*

Specifies a POSIX extended regular expression to search for a match within the specified RASlog message ID. For examples, refer to the "trigger" topic.

Modes

Global configuration mode

Event-handler configuration mode for an existing event handler. (There is no need to enter the **exit** command to return to global configuration mode.)

Usage Guidelines

You can create multiple event-handler profiles.

You can optionally specify a description, a trigger, or the Python script with this command; or specify them later.

An **event-handler** command creates or accesses an event-handler profile and can also define one of the following parameters:

- Description
- One trigger
- The Python-script action that runs on any trigger

You can also define the above parameters—including one or more triggers—from event-handler configuration mode.

A Python event-handler script runs only if all of the following occur:

- Using the **copy** command, copy the Python file to the `flash://` location on the device.
- Using the **event-handler** command, create an event-handler profile.
- Either using the **event-handler** command or in configuration mode for that profile:
  - Using the **trigger** command, create one or more triggers.
  - Using the **action** command, specify the Python script that will be triggered.
- Using the **event-handler activate** command, activate an instance of the event handler.
- The trigger event occurs.

If an event-handler profile is not activated, the **no** form of this command deletes it.

Examples

The following example creates an event-handler profile and accesses its configuration mode.

```
device# configure terminal
device(config)# event-handler eventHandler1
device(config-event-handler-eventHandler1)#
```

event-handler abort action

Under Python event-management, aborts a specified event handler that is currently running.

Syntax

event-handler abort action *event-handler-name*

Parameters

event-handler-name

Specifies the name of the event-handler profile.

Modes

Privileged EXEC mode

Examples

The following command successfully aborted event-handler action "eh1".

```
device# event-handler abort action eh1
This operation will abort an event handler action that is currently running and may leave
the switch in an inconsistent state.  Do you want to continue? [y/n]:y
Operation completed successfully.
```

event-handler activate

Activates an event handler and accesses event-handler activation mode, from which you can enter advanced configuration commands. You can also append the advanced commands to **event-handler activate**.

Syntax

event-handler activate *event-handler-name*

event-handler activate *event-handler-name* [**action-timeout** *minutes*] [**delay** *seconds*] [**iterations** *num-iterations*] [**interval** *seconds*] [**trigger-mode** *mode*] [**trigger-function** { **OR** | **AND** [**time-window** *seconds*] }]

no event-handler activate *event-handler-name*

Command Default

No event handler is activated on the device.

Parameters

event-handler-name

Specifies the name of the event-handler profile.

action-timeout *minutes*

Specifies the number of minutes to wait for an action-script to complete execution. If you specify "0", no timeout is set. Valid timeout values are any positive integer.

delay *seconds*

Specifies a number of seconds from when a trigger is received until the execution of the specified action begins. Valid values are 0 or a positive integer.

iterations *num-iterations*

Specifies the number of times an event-handler action is run, when triggered. Valid values are any positive integer. The default value is 1.

interval *seconds*

Specifies the number of seconds between iterations of an event-handler action, if triggered. Valid values are 0 or a positive integer. The default is 0.

trigger-mode *mode*

Specifies if an event-handler action can be triggered only once or more than once. The default is each time the trigger condition occurs, the event-handler action is launched.

each-instance

The event-handler action is launched on each trigger instance received.

on-first-instance

As long as the device is running, the event-handler action is launched only once. Following a device restart, the event-handler action can be triggered again.

only-once

For the duration of a device's configuration, the event-handler action is launched only once.

trigger-function

For an implementation of an event-handler profile, if multiple triggers are defined for an event-handler action, specifies if the action runs only if all of the triggers occur; or if one is sufficient.

OR

The event-handler action runs if any of the triggers occur.

AND

The event-handler action runs only if all of the triggers occur.

time-window *seconds*

In seconds, specify the time window within which all of the triggers must occur in order that the event-handler action runs. Once all triggers have been received and on each subsequent trigger received, the action will be launched when the time difference between the latest trigger and the oldest trigger is less than or equal to the configured time-window.

Modes

Global configuration mode

Event-handler activation mode for an existing event handler. (There is no need to enter the **exit** command.)

Usage Guidelines

You can activate up to 10 different event-handler profiles on a device.

A Python event-handler script runs only if all of the following occur:

- Using the **copy** command, copy the Python file to the `flash://` location on the device.
- Using the **event-handler** command, create an event-handler profile.
- In configuration mode for that profile:
  - Using the **trigger** command, create one or more triggers.
  - Using the **action** command, specify the Python script that will be triggered.
- Using the **event-handler activate** command, activate an instance of the event handler.
- The trigger event occurs.

Following an initial triggering of an event-handler action, any subsequent trigger launches the action an additional time if the following conditions are true:

- The **trigger-mode** parameter is set to the default **each-instance**.

- The subsequent trigger occurs within the specified **time-window**.

For additional usage guidelines regarding the advanced configuration commands, see the following topics:

- **action-timeout**
- **delay**
- **iterations**
- **interval**
- **trigger-mode**
- **trigger-function**

To inactivate an event-handler instance on a device, use the **no** form of this command. If an event-handler Python script is running, it is executed to completion before inactivation of the event handler.

Examples

This example activates eventHandler1 on the device.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)#
```

evpn

Creates an EVPN instance and enables EVPN instance configuration mode.

Syntax

evpn [*name*]

no evpn { **default** |*name* }

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to remove the EVPN instance.

When you enter the **evpn** command without a name, a default EVPN instance is created.

The device allows only one EVPN instance.

Examples

The following example configures the default EVPN instance.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)#
```

The following example creates an EVPN instance named myinstance.

```
device# configure terminal
device(config)# evpn myinstance
device(config-evpn-myinstance)#
```

exclude-any

Interfaces that are not part of these groups, as well as interfaces that are not part of any group, are eliminated from consideration.

Syntax

exclude-any *admin_group_name* | *admin_group_name* [*admin_group_name* | *admin_group_name*]

no exclude-any *admin_group_name* | *admin_group_name* [*admin_group_name* | *admin_group_name*]

Command Default

There are no excluded interfaces in the command default mode.

Parameters

name

Specifies the group, by name, the interface must be a member of. The name can be the name of the administrative group to which an administrative group number is associated by configuration in router MPLS mode. More than one parameter can be provided.

number

Specifies the group, by number, the interface must be a member of. Number can be from 0 to 31 representing 32 admin groups. More than one parameter can be provided.

Modes

MPLS LSP configuration mode (config-router-mpls lsp-*lsp_name*)

MPLS router Bypass LSP configuration mode (config-router-mpls-bypass-lsp-*lsp_name*)

MPLS router MPLS interface dynamic bypass configuration mode (config-router-mpls-if-ethernet-*slot/port*-dynamic-bypass)

Usage Guidelines

More than one group may be configured at a time.

Use the interface level **exclude-any** command to configure administrative groups for dynamic bypass LSPs to be created corresponding to a protected link.

The **no** form of the command removes the interface administrative group configuration.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example eliminates interfaces in either administrative group *gold* or *silver* when the path for LSP *tunnel1* is calculated.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp tunnel1
device(config-router-mpls-lsp-tunnel1)# exclude-any gold silver
```

The following example eliminates bypass LSP administration groups *15* and *16* .

```
device# configure
device(config)# router mpls
device(config-router-mpls)# bypass-lsp my-bypass-lsp
device(config-router-mpls-bypass-lsp-my-bypass-lsp)#  exclude any 15 16
```

The following example eliminates groups *10* and *11* from consideration for dynamic bypass MPLS Ethernet interface *0/8*.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/8
device(config-router-mpls-if-ethernet-0/8)# dynamic-bypass
device(config-router-mpls-if-ethernet-0/8-dynamic-bypass)# exclude-any 10 11
```

exclude-interface

Configures one or more exclude interfaces for the bypass LSP.

Syntax

exclude-interface { [**ethernet** *slot/port* | **port-channel** *number* | **ve** *ve-num*] }

no exclude-interface { [**ethernet** *slot/port* | **port-channel** *number* | **ve** *ve_num*] }

Command Default

There is no default value. This is a mandatory parameter.

Parameters

ethernet *slot/port*

Specifies the physical slot and port on the Ethernet interface.

port-channel *number*

Specifies a port-channel interface.

ve *ve_num*

Specifies the Virtual Ethernet (VE) number on the VE interface.

Modes

MPLS router Bypass LSP configuration mode.

Usage Guidelines

The **no** form of this command removes an exclude interface of the bypass LSP.

The user can configure one or more exclude interfaces for the bypass LSP. The interface can be an Ethernet or a virtual Ethernet type. To enable a bypass LSP, the system requires at least one exclude interface configuration.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example excludes Ethernet interface *2/8* on bypass LSP *my-bypass-lsp*.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# bypass-lsp my-bypass-lsp
device(config-router-mpls-bypass-lsp-my-bypass-lsp)# exclude-interface Ethernet 0/8
```

The following example excludes VE interface 108 on bypass LSP *my-bypass-lsp*.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# bypass-lsp my-bypass-lsp
device(config-router-mpls-bypass-lsp-my-bypass-lsp)# exclude-interface ve 108
```

exp

Defines the QoS MPLS EXP-to-DSCP or EXP-to-traffic class mutation mapping.

Syntax

exp *exp-value* **to** { **dscp** *dscp-value* } | { **traffic class** *traffic-class-value* **drop-precedence** *drop-precedence-value* }

no exp *exp-value*

Command Default

The default EXP-to-DSCP mapping is as follows:

```
Exp      :   0   1   2   3   4   5   6   7
-------- --------------------------------
Dscp     :   0   8  16  24  32  40  48  56
```

The default EXP-to-traffic class mapping with the drop precedence is as follows:

```
Exp             :   0  1  2  3  4  5  6  7
--------------- ------------------------
traffic-class   :   0  1  2  3  4  5  6  7
drop-precedence :   0  0  0  0  0  0  0  0
```

Parameters

exp-value

Specifies the EXP value. Enter an integer from 0 through 7.

dscp *dscp-value*

Specifies the DSCP value. Enter an integer from 0 through 63.

traffic class *traffic-class-value*

Specifies the traffic class value. Enter an integer from 0 through 7.

drop-precedence *drop-precedence-value*

Specifies the drop precedence for the traffic class. Enter an integer from 0 through 3.

Modes

QoS-MPLS map EXP-DSCP and EXP-traffic-class configuration mode

Usage Guidelines

After configuring the mutation mapping, you can apply the map globally.

Use the **no** form of this command to reset the default mapping.

This command is supported on the Extreme 8820 and SLX 9740 devices only.

Examples

The following example is an MPLS QoS EXP-to-DSCP mutation map configuration.

```
device# configure terminal
device(config)# qos-mpls map exp-dscp expDscpMap
device(exp-dscp-expDscpMap)# exp 0 to dscp 7
device(exp-dscp-expDscpMap)# exp 1 to dscp 23
device(exp-dscp-expDscpMap)# exp 3 to dscp 31
```

The following example is an MPLS QoS EXP-to-traffic class mutation map configuration.

```
device# configure terminal
device(config)# qos-mpls map exp-traffic-class expTcMap
device(exp-traffic-class-expTcMap)# exp 0 to traffic-class 7 drop-precedence 0
```

export-vrf-leaked-routes

Allows exporting VRF leaked routes to Layer VPN.

Syntax

export-vrf-leaked-routes

no export-vrf-leaked-routes

Modes

BGP address-family IPv4 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command disables exporting VRF leaked routes to Layer VPN.

Examples

This example shows how to export VRF leaked routes to Layer VPN.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family vpnv4 unicast
device(config-bgp-vpnv4u)# export-vrf-leaked-routes
```

export-map

Exports the target-VPN community.

Syntax

export-map *route-map*

no export-map *route-map*

Parameters

route-map

Specifies the route-map name.

Modes

VRF configuration mode

Usage Guidelines

The **no** form of the command to apply a route-map filter on the routes to be exported.

Examples

The following example shows how to export the target-VPN community.

```
device# configure terminal
device(config)# vrf vpn1
device#(config-vrf-vpn1)# rd 1:2
device#(config-vrf-vpn1)# vpn-statistics
device#(config-vrf-vpn1)# address-familin ipv4 unicast
device#(config-vrf-vpn1-ipv4-unicast)# route-target-import 100:1
device#(config-vrf-vpn1-ipv4-unicast)# export-map import-route-map1
```

extend bridge-domain

Configures a bridge domain (BD) to a site for a VXLAN Layer 2 gateway.

Syntax

extend bridge-domain { **add** | **remove** } *bridge_domain_id*

Parameters

add

Adds a bridge-domain ID to a tunnel.

remove

Removes a bridge-domain ID from a tunnel.

bridge_domain_id

Specifies the configured bridge domain ID.

Modes

Site configuration mode

Examples

The following example configures the bridge domain to the site of the VXLAN Layer 2 gateway.

```
device# configure terminal
device(config)# overlay-gateway gateway1
device(config-overlay-gw-gateway1)# site mysite
device(config-overlay-gw-gateway1-site-mysite)# extend bridge-domain add 10
```

extend vlan

Configures switchport VLANs for the tunnels to the containing site in VXLAN overlay gateway configurations.

Syntax

extend vlan { **add** | **remove** } *vlan_id*

no extend vlan

Parameters

add

Specifies a VLAN ID or range of VLAN IDs to be added to a tunnel.

remove

Specifies a VLAN ID or range of VLAN IDs to be removed from a tunnel.

vlan_id

A VLAN ID or range of VLAN IDs. See the Usage Guidelines.

Modes

VXLAN overlay gateway site configuration mode

Usage Guidelines

The VXLAN Network Identifier (VNI) classification is derived from the "map vlan" configuration of the parent overlay gateway. This command results in the provisioning or unprovisioning of the VLANs. Use the **no extend vlan** *vlan_id* command to unprovision a VLAN.

All of the VLAN IDs that are specified must be VLANs that have been mapped by means of the **map vlan** *vlan_id* **vni** *vni* command on the parent overlay gateway, unless automatic VNI mapping has been enabled by means of the **map vlan vni auto** command.

Use the **no attach vlan** *vlan_id* command to remove all switchport configurations from the tunnels to the containing site.

Examples

To configure a switchport VLAN and range of VLANs:

```
device# configure terminal
device(config)# overlay-gateway gateway1
device(config-overlay-gw-gateway1)# site mysite
device(config-overlay-gw-gateway1-site-mysite)# extend vlan add 10,20-30
```

external-lsdb-limit (OSPFv2)

Configures the maximum size of the external link state database (LSDB).

Syntax

external-lsdb-limit *value*

no external-lsdb-limit

Parameters

value

Maximum size of the external LSDB. Valid values range from 1 through 14913080. The default is 14913080.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

If you change the value, make sure to save the running-config file and reload the software. The change does not take effect until you reload or reboot the software.

The **no** form of the command restores the default setting.

Examples

The following example sets the limit of the LSDB to 20000.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# external-lsdb-limit 20000
```

external-lsdb-limit (OSPFv3)

Configures the maximum size of the external link state database (LSDB).

Syntax

external-lsdb-limit *value*

no external-lsdb-limit

Parameters

value

Maximum size of the external LSDB. Valid values range from 1 through 250000. The default is 250000.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

If you change the value, you must save the running-config file and reload the software. The change does not take effect until you reload or reboot the software.

The **no** form of command reverts to the default setting.

Examples

The following example sets the limit of the external LSDB to 15000.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# external-lsdb-limit 15000
```

facility-backup

Enables facility backup (many-to-one) Fast Reroute (FRR) on a Label Switched Path (LSP).

Syntax

facility-backup [**bandwidth** | **exclude-any** *name* | **hop-limit** *name* | **include-all** | **include-any** | **link-protection** | **priority** | **revertive**]

no facility-backup [**bandwidth** | **exclude-any** *name* | **hop-limit** *name* | **include-all** | **include-any** | **link-protection** | **priority** | **revertive**]

Command Default

By default, a FRR LSP is a one-to-one (detour) protection LSP with the desired node protection.

Parameters

bandwidth

Specifies the bandwidth for the detour or backup LSP.

exclude-any *name*

Excludes any of the specified administrative groups.

hop-limit *num*

Specifies the limit of hops the detour or backup LSP can traverse.

include-all

Specifies to include all of the administrative groups.

include-any

Specifies to include any of the administrative groups.

link-protection

Requests link protection for the LSP.

priority

Requests setup and hold priorities.

revertive

Activates FRR revertiveness.

Modes

MPLS router LSP FRR configuration mode.

Usage Guidelines

When enabled at every Point of Local Repair (PLR), the LSP outgoing interface is expected to be protected by a bypass LSP. The user can create bypass LSPs manually or they can be created automatically using dynamic bypass.

The **no** form of the command sets the FRR LSP to the detour (one-to-one) mode.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example enables facility backup on LSP named *my-fbkup-lsp*.

```
device# kconfigure
device(config)# router mpls
device(config-router-mpls)#lsp my-fbkup-lsp
device(config-router-mpls-lsp-my-fbkup-lsp)# frr
device(config-router-mpls-lsp-my-fbkup-lsp-frr)# facility-backup
```

fast-convergence

Enables fast convergence of devices in the Ethernet Ring Protection (ERP) ring.

Syntax

fast-convergence

no fast-convergence

Command Default

Fast convergence is disabled by default.

Modes

ERP configuration mode

Usage Guidelines

A convergence time of less than 50-msec can be achieved with 4-device ring topology on 1-RU devices. If the number of nodes in the topology increases, a small linear increase in convergence time occurs accordingly.

The **no** form of the command disables fast-convergence.

Examples

The following example enables fast convergence in the ERP instance 1.

```
device# configure terminal
device(config)# erp 1
device(config-erp-1) fast-convergence
```

fast-external-fallover

Resets the session if a link to an eBGP peer goes down.

Syntax

fast-external-fallover

no fast-external-fallover

Modes

BGP configuration mode

Usage Guidelines

Use this command to terminate and reset external BGP sessions of a directly adjacent peer if the link to the peer goes down, without waiting for the timer, set by the BGP **timers** command, to expire. This can improve BGP conversion time, but can also lead to instability in the BGP routing table as a result of a flapping interface.

Examples

The following example configures the device to reset the session if a link to an eBGP peer goes down.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# fast-external-fallover
```

fast-flood

Configures Intermediate System-to-Intermediate System (IS-IS) to flood Link State PDUs to other devices in the network before running SPF.

Syntax

fast-flood *lsp-count*

no fast-flood *sp-count*

Command Default

Four LSPs are flooded before running SPF.

Parameters

lsp-count

Specifies the number of LSPs that must be flooded before running SPF. Valid values range from 1 through 15. The default value is 4.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command resets the LSP count to the default value of 4.

Examples

The following example configures IS-IS to flood 10 LSPs before running SPF.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# fast-flood 10
```

fastboot

Reboots the device without a power-on self-test (POST).

Syntax

fastboot

Modes

Privileged EXEC mode

Usage Guidelines

All reboot operations are disruptive, and the commands prompt for confirmation before executing. When you reboot a device, all traffic to and from it stops. All ports on that device remain inactive until the device comes back online.

Any unsaved configurations are lost.

Examples

The following example shows the use of the **fastboot** command.

```
device# fastboot
```

fast-wtr-time

Sets the Wait to Restore (WTR) time for Ethernet Ring Protection (ERP) from minutes to seconds.

Syntax

fast-wtr-time

no fast-wtr-time

Command Default

The WTR value is in minutes by default.

Modes

ERP configuration mode

Usage Guidelines

Use the **no** form of this command to restore the WTR value to minutes.

Examples

The following example configures a WTR time value to seconds.

```
device# configure terminal
device(config)# erp 1
device(config-erp-1)# fast-wtr-time
```

fec mode

Configures the various Forward Error Corrections (FEC) parameters for the interface.

Syntax

fec mode { **FC-FEC** | **RS-FEC** | **auto-negotiation** | **disable** }

no fec mode

Command Default

By default, SLX-OS selects one of *FC-FEC*, *RS-FEC* or *disable* based on port type, configured speed, and the optic inserted in that port.

Parameters

FC-FEC

Set the FEC mode to FC-FEC in manual mode.

RS-FEC

Set the FEC mode to use RS-FEC in manual mode.

auto-negotiation

Set the FEC mode to *auto-negotiation*. This setting is only applicable for 25G DAC cables.

disable

Disable FEC on the interface.

Modes

Interface Ethernet mode

Usage Guidelines

The *no* format of this command resets the FEC configuration on the interface to the default configuration.

Examples

The following example configures the ethernet port 0/1 with RS-FEC.

```
SLX # config terminal
SLX (config)# interface Ethernet 0/1
SLX (conf-if-eth-0/1)# fec mode RS-FEC

2021/12/15-08:42:19, [NSM-1002], 3190, DCE, INFO, SLX9250-32C,  interface Ethernet 0/1 is
protocol down.
2021/12/15-08:42:19, [NSM-1003], 3191, DCE, INFO, SLX9250-32C,  interface Ethernet 0/1 is
link down.
SLX (conf-if-eth-0/1)# 2021/12/15-08:42:19, [ONMD-1010], 3192, DCE, INFO, SLX9250-32C,
```

```
LLDP Neighbor Delete: Local info:Eth 0/1,f46e.95a3.780b, Remote info:Ethernet
0/1,887e.25d3.1211,Eth 0/1, , ,887e.25d3.120a,SLX, .
2021/12/15-08:42:21, [NSM-1001], 3193, DCE, INFO, SLX9250-32C,  interface Ethernet 0/1 is
online.
```

fec (telemetry)

Indicates the MPLS FEC address to be used for the mpls-traffic-fec profile.

Syntax

fec *fec-address*

no fec *fec-address*

Parameters

fec-address

Specifies the address of the target FEC for the profile.

Modes

Telemetry profile configuration mode

Usage Guidelines

The *fec-address* variable must be unique.

The **no** form of the command deletes the FEC address from the profile.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example selects *20.10.3.4* as the FEC address for the profile.

```
device(config)# telemetry profile mpls-traffic-fec default_mpls_traffic_fec_statistics
device(config-telemetry-profile)# fec 20.10.3.4
```

filter-change-update-delay

Configures the delay period before application of a change to a Border Gateway Protocol flow specification (BGP flowspec) route-map rule.

Syntax

filter-change-update-delay *delay*

no filter-change-update-delay

Command Default

By default, changes to BGP flowspec route-map rules are applied after a delay of 10 seconds.

Parameters

delay

Delay period (in seconds) before changes to BGP flowspec route-map rules are applied.

Modes

Global configuration mode

Usage Guidelines

The **no** from of the command restores the default configuration.

Examples

The following example shows how to set (to 500 seconds) the delay period for application of changes to BGP flowspec route-map rules.

```
device# configure terminal
device(config)# filter-change-update-delay 500
```

filter-fec-in

Configures LDP inbound or outbound FEC filtering to filter inbound label bindings on a MPLS router.

Syntax

filter-fec-in *prefix-list-name*

no filter-fec-in *prefix-list-name*

Command Default

By default, LDP distributes all FECs that are learned locally or from LDP neighbors to all other LDP neighbors.

Parameters

prefix-list-name

Specifies the prefix-list name.

Modes

MPLS LDP configuration mode

Usage Guidelines

Use the **no** form of this command to remove the FEC filtering configuration.

LDP inbound-FEC filtering allows the control the amount of memory and CPU processing involved in installing and advertising label bindings not used for forwarding. It also serves as a tool to avoid DOS attack. For inbound FEC filter, consider the following:

- The FECs filtered by the LDP inbound-FEC filter do not install in the forwarding plane or advertise to the upstream neighbors. The FEC remains in the retained state.
- The LDP inbound-FEC filter are changed directly without deleting the one previously configured. The change automatically applies and triggers the filtering of inbound FECs.
- Changes to a referenced prefix-list automatically applies to LDP inbound-FEC filtering. This triggers filtering by way of the new configuration, filtering any existing FECs which violate the filter.
- To allow multiple route filter updates, the device waits for default 10 seconds before notifying the application of the filter change. The time for notification is configurable.
- When the LDP inbound-FEC filter is not configured, LDP does not filter any inbound FECs.

- By default, when the prefix-list referenced by the LDP inbound-FEC filter has no configuration, it is an implicit deny. All inbound FECs are filtered out and retained. The behavior is the same when the prefix list is deleted after setting it in the inbound FEC filter configuration. This behavior is consistent with other protocols which use device filters and also with the use of the **advertise-fec** command for LDP route injection.
- Inbound FEC filtering is applicable only for Layer 3 FECs and not for VC FECs. Inbound FEC filtering is not applicable for Layer 2 VPNs.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures the LDP inbound-FEC filter.

```
device# configure terminal
device(config)# ip prefix-list list-abc permit 10.20.20.0/24
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# filter-fec-in list-abc
```

filter-fec-out

Configures LDP outbound FEC filtering to filter outbound label bindings on a MPLS router.

Syntax

filter-fec-out *prefix-list-name*

no filter-fec-out *prefix-list-name*

Command Default

By default, LDP distributes all FECs that are learned locally or from LDP neighbors to all other LDP neighbors.

Parameters

prefix-list-name

Specifies the prefix-list name.

Modes

MPLS LDP configuration mode

Usage Guidelines

Use the **no** form of this command to remove the FEC filtering configuration.

LDP outbound FEC filtering gives you the ability to control which FECs can be advertised and to which LDP neighbors. It also reduces the number of labels distributed to neighbors and the number of messages exchanged with peers. Through this filtering, LDP scalability and convergence, security, and performance are improved.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures the LDP outbound-FEC filter.

```
device# configure terminal
device(config)# ip prefix-list list-out deny 10.40.40.0/24
device(config)# ip prefix-list list-out permit 0.0.0.0/0 ge 32
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# filter-fec-out list-out
```

firmware activate

Activates the firmware that was downloaded with firmware download noactivate command.

Syntax

firmware activate

Command Default

Activation of the firmware is performed manually by default after a download.

Modes

Privileged EXEC mode

Usage Guidelines

By default, the **firmware download** command downloads the firmware to the system, reboots the system, and commits the firmware automatically. You can specify the **noactivate** parameter to download the firmware to the system without activating it (the node is not rebooted). The user can run the **firmware activate** command later to activate the firmware.

Examples

To activate firmware on the device:

```
device# firmware activate
```

firmware commit

Commits a firmware upgrade.

Syntax

firmware commit

Modes

Privileged EXEC mode

Usage Guidelines

The **firmware download** command updates the secondary partitions only. When the **firmware download** command completes successfully and the device reboots, the system swaps partitions. The primary partition (with the previous firmware) becomes the secondary partition, and the secondary partition (with the new firmware) becomes the primary partition.

By default, **firmware download** automatically commits the firmware after the device reboots. If you disable auto-commit mode when running **firmware download**, you must execute **firmware commit** to commit the new firmware to the secondary partition.

You must run the **firmware download** command with the **nocommit** parameter set for the following firmware commit operation to succeed.

Examples

To commit the firmware:

```
device# firmware commit

Validating primary partition...
Doing firmwarecommit now.
Please wait ...
Replicating kernel image
..............
FirmwareCommit completes successfully.
```

firmware download

Downloads the firmware on the device, reboots the system, and commits the firmware.

Syntax

```
firmware download { default-config | ftp | scp | sftp | tftp | usb
   | interactive | migrate } [ manual ] [ nocommit ] [ noreboot ]
   [ noactivate ] [ coldboot ] host { hostname | host_ip_address } user
   username password password directory directory [ file file_name ]
   [ use-vrf vrf-name] ]
```

Command Default

By default, **firmware download** downloads the firmware to the system, reboots the system, and commits the firmware automatically. The user can specify **noactivate** to download the firmware to the system without activating it (the node is not rebooted). You can run the **firmware activate** command later to activate the firmware.

BMC firmware image is bundled with the SLX-OS firmware image. When the SLX-OS firmware image is updated, the update process checks the version of the BMC installed on the device. If the installed BMC version is found to be older than the bundled BMC version, the upgrade process automatically installs the bundled BMC version replacing the installed BMC version.

Parameters

default-config

Sets the configuration back to default.

ftp | scp | sftp | usb

Valid protocols are **ftp** (File Transfer Protocol), **scp** (Secure Copy), **sftp** (SSH File Transfer Protocol), **tftp** (Trivial File Transfer Protocol), or **usb** (Universal Serial Bus). The values are not case-sensitive.

interactive

Runs firmware download in interactive mode. You are prompted for input.

migrate

Runs *full-install* to install a new compatible NOS. The installed SLX-OS will be over written and will be erased.

manual

Currently, this keyword has no effect.

nocommit

Disables auto-commit mode. When auto-commit mode is disabled, firmware is downloaded only to the primary partition. You must execute the firmware **commit** command manually to propagate the new image to the secondary partition.

noreboot

Disables auto-reboot mode. When auto-reboot mode is disabled, you must reboot the device manually.

noactivate

Downloads the firmware to the system without activating it, so the device is not automatically rebooted. You can run the **firmware activate** command later to activate the firmware.

coldboot

Downloads the firmware to the system and reboots the device.

host

Specifies the host by DNS name or IP address.

hostname

Specifies an IPv4 DNS host name.

host_ip_address

Specifies the host IP address. IPv4 and IPv6 addresses are supported.

directory *directory*

Specifies a fully qualified path to the directory where the firmware is located.

file *file_name*

Specifies the firmware .plist file. This parameter is optional; if unspecified, the default file, release.plist, is used.

user *username*

Specifies the user login name for the host.

password *password*

Specifies the account password.

use-vrf *vrf-id*

Use this option to specify the name of the VRF where the host is located. If this option is not set, mgmt-vrf is used by default.

Modes

Privileged EXEC mode

Usage Guidelines

Unless you specify **noactivate**, the upgrade or downgrade involves system reboots that disrupt traffic.

If the **firmware download** command is interrupted because of an unexpected reboot, such as a result of a software error or power failure, the command automatically recovers the corrupted secondary partition. Wait for the recovery to complete before beginning another firmware download.

Examples

Example of firmware download with the **coldboot** option:

```
device# firmware download ftp directory /buildsjc/sre/SQA/slxos/17r.1.00/17r.1.00 host
10.31.2.27 user releaseuser password releaseuser coldboot

Performing system sanity check...

This command will cause a cold/disruptive reboot and will require that existing telnet,
secure telnet or SSH sessions be restarted.


Do you want to continue? [y/n]y
```

Example of firmware download with the **default-config** option:

```
device# firmware download default-config ftp directory /buildsjc/sre/SQA/slxos/
17r.1.00/17r.1.00 host 10.31.2.27 user releaseuser password releaseuser

Performing system sanity check...



This command will cause a cold/disruptive reboot and will require that existing telnet,
secure telnet or SSH sessions be restarted.



Do you want to continue? [y/n]y
```

firmware download ftp

Specifies FTP as the protocol used to perform a firmware download.

Syntax

firmware download ftp [**coldboot**] [**manual**] [**noactivate**] [**nocommit**] [**noreboot**] **host** { *hostname* | *host_ip_address* } **use-vrf** *vrf-name* **user** *username* **password** *password* **directory** *directory* [**file** *file_name*]

Command Default

By default, downloads the firmware to the system, reboots the system, and commits the firmware automatically. The user can specify **noactivate firmware download** to download the firmware to the system without activating it (the node is not rebooted). The user can run **firmware activate** later to activate the firmware.

Parameters

coldboot

Downloads the firmware to the system and reboots the device.

directory *directory*

Specifies a fully qualified path to the directory where the firmware is located.

file *file_name*

Specifies the firmware .plist file. This parameter is optional; if unspecified, the default file, release.plist, is used.

host

Specifies the host by DNS name or IP address.

hostname

Specifies an IPv4 DNS host name.

host_ip_address

Specifies the host IP address. IPv4 and IPv6 addresses are supported.

manual

Currently, this keyword has no effect.

noactivate

Performs a firmware download without activation on the local device.

nocommit

Disables auto-commit mode. When auto-commit mode is disabled, firmware is downloaded only to the primary partition. You must execute the firmware **commit** command manually to propagate the new image to the secondary partition.

noreboot

Disables auto-reboot mode. When auto-reboot mode is disabled, you must reboot the device manually. If auto-commit mode was disabled, you must perform a manual firmware **commit** operation after the device comes back up.

password *password*

Specifies the account password.

use-vrf *vrf-name*

Specifies a VRF.

user *username*

Specifies the user login name for the host.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to download firmware from an external host.

Unless you specify **noactivate**, the upgrade or downgrade involves system reboots that disrupt traffic.

If the **firmware download** command is interrupted because of an unexpected reboot, such as a result of a software error or power failure, the command automatically recovers the corrupted secondary partition. Wait for the recovery to complete before beginning another firmware download.

This command does not support pagination.

Examples

This example downloads firmware by means of FTP and specifies a path to the directory where the firmware is located. A user login name is specified for the host and an account password is specified.

```
device# firmware download ftp directory /buildsjc/sre/SQA/slxos/17r.1.00/17r.1.00 host
10.31.2.27 user releaseuser password releaseuser
```

firmware download fullinstall

Downloads the firmware on the local device.

Syntax

```
firmware download [ fullinstall ] { ftp | scp | sftp | tftp | usb }
   [ manual ] [ nocommit ] [ noreboot ] [ noactivate ] [ coldboot ]
   host { hostname | host_ip_address } user username password password
   directory directory [ file file_name ] [ use-vrf vrf-name ]
```

Command Default

By default, **firmware download** downloads the firmware to the system, reboots the system, and commits the firmware automatically. The user can specify **noactivate** to download the firmware to the system without activating it (the node is not rebooted). You can run the **firmware activate** command later to activate the firmware.

Parameters

fullinstall

This is an optional parameter. Downloads a larger install file that converts between 32-bit and 64-bit firmware when upgrading or downgrading the device.

ftp | scp | sftp | usb

Valid protocols are **ftp** (File Transfer Protocol), **scp** (Secure Copy), **sftp** (SSH File Transfer Protocol), **tftp** (Trivial File Transfer Protocol), or **usb** (Universal Serial Bus).

The parameters are not case-sensitive.

manual

This parameter performs no action.

nocommit

This is an optional keyword. This keyword disables auto-commit mode. When auto-commit mode is disabled, firmware is downloaded only to the primary partition. You must execute the firmware **commit** command manually to propagate the new image to the secondary partition.

noreboot

This is an optional keyword. This keyword disables auto-reboot mode. When auto-reboot mode is disabled, you must reboot the device manually.

noactivate

This is an optional keyword. This keyword downloads the firmware to the system without activating it, so the device is not automatically rebooted. You can then run the **firmware activate** command to activate the firmware later.

coldboot

host

Specifies the host by DNS name or IP address.

hostname

Specifies an IPv4 DNS host name.

host_ip_address

Specifies the host IP address. IPv4 and IPv6 addresses are supported.

directory *directory*

Specifies a fully qualified path to the directory where the firmware is located.

file *file_name*

Specifies the firmware .plist file. This parameter is optional; if unspecified, the default file, release.plist, is used.

user *username*

Specifies the user login name for the host.

password *password*

Specifies the account password.

use-vrf *vrf-id*

Use this option to specify the name of the VRF where the host is located. If this option is not set, mgmt-vrf is used by default.

Modes

Privileged EXEC mode

Usage Guidelines

Unless you specify **noactivate**, the upgrade or downgrade involves system reboots that disrupt traffic.

If the **firmware download** command is interrupted because of an unexpected reboot, such as a result of a software error or power failure, the command automatically recovers the corrupted secondary partition. Wait for the recovery to complete before beginning another firmware download.

The **fullinstall** option enables upgrading the firmware from a 32-bit version to a 64-bit version. Additionally, the **fullinstall** option enables downgrading the firmware from a 64-bit version to a 32-bit version. This feature assumes the device hardware is capable of supporting 64-bit architecture.

The **fullinstall** option preserves startup-config, SSH host keys, and licenses. However, though the startup-config is preserved, the system is designed to boot with the default-config. You must manually apply the configs that were preserved, if configurations are compatible. Manually copying the config file uses the **copy flash://startup-config running-config** command or the **copy <file> running-config** command.

It is recommended that you back up your running configuration before running the *fullinstall* command. Use one of the following commands to do so:

- **copy flash://<config> startup-config**
- **copy scp/ftp/tftp:://<config> startup-config**
- **copy running-config startup-config** .

The system then can use the backed up configuration file to restore your configuration during full install.

firmware download interactive

Allows the user to select firmware download parameters interactively before starting a firmware download.

Syntax

firmware download interactive

Command Default

By default, **firmware download** downloads the firmware to the system, reboots the system, and commits the firmware automatically.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to download firmware from an external host or from an attached USB device. You can run this command interactively or provide the parameters on the command line.

Unless you specify **noactivate**, the upgrade or downgrade involves system reboots that disrupt traffic.

If the **firmware download** command is interrupted because of an unexpected reboot, such as a result of a software error or power failure, the command automatically recovers the corrupted secondary partition. Wait for the recovery to complete before beginning another firmware download.

This command does not support pagination.

Examples

To perform a firmware download in interactive mode using default parameters:

```
device# firmware download interactive
Server name or IP address: 10.70.4.106
File name: dist
Protocol (ftp, scp, sftp, tftp) [ftp]: scp
User: fvt
Password: **********
Enter VRF name[mgmt-vrf]:
Select procedure (1=ISSU, 2=coldboot, 3=default-config) [1]:1

Performing system sanity check...

This command will cause a cold/disruptive reboot and will require that existing telnet,
secure telnet or SSH sessions be restarted.
```

```
Do you want to continue? [y/n]y
```

firmware download scp

Specifies Secure Copy (SCP) as the protocol used to perform a firmware download.

Syntax

firmware download scp [**coldboot**] [**manual**] [**nocommit**] [**noreboot**] **host** { *hostname* | *host_ip_address* } **user** *username* **password** *password* **directory** *directory* [**file** *file_name*] [**noactivate**] [**use-vrf** *vrf-name*]

Command Default

A filename is optional. If no filename is specified, release.plist, is used.

Parameters

coldboot

Downloads the firmware to the system and reboots the device.

manual

Currently, this keyword has no effect.

nocommit

Disables auto-commit mode. When auto-commit mode is disabled, firmware is downloaded only to the primary partition. You must execute the firmware **commit** command manually to propagate the new image to the secondary partition. (Skips auto-commit after firmware download.)

noreboot

Disables auto-reboot mode. When auto-reboot mode is disabled, you must reboot the device manually. If auto-commit mode was disabled, you must perform a manual firmware **commit** operation after the device comes back up.

host

Specifies the host by DNS name or IP address.
hostname

Specifies an IPv4 DNS host name.

host_ip_address

Specifies the host IP address. IPv4 and IPv6 addresses are supported.

user *username*

Specifies the user login name for the host.

password *password*

Specifies the account password.

directory *directory*

Specifies a fully qualified path to the directory where the firmware is located.

file *file_name*

Specifies the firmware .plist file. This parameter is optional.

noactivate

Performs a firmware download without activation on the local device.

use-vrf *vrf-id*

Use this option to specify the name of the VRF where the host is located. If this option is not set, mgmt-vrf is used by default.

Modes

Privileged EXEC mode.

Usage Guidelines

Use this command to download firmware from an external host or from an attached USB device. You can run this command interactively or provide the parameters on the command line.

Unless you specify **noactivate**, the upgrade or downgrade involves system reboots that disrupt traffic.

If the **firmware download** command is interrupted because of an unexpected reboot, such as a result of a software error or power failure, the command automatically recovers the corrupted secondary partition. Wait for the recovery to complete before beginning another firmware download.

This command does not support pagination.

If the **firmware download** is interrupted because of an unexpected reboot as a result of a software error or power failure, the command automatically recovers the corrupted secondary partition. Wait for the recovery to complete before starting another firmware download.

Examples

This example downloads firmware by means of SCP and specifies a path to the directory where the firmware is located. A user login name is specified for the host and an account password is specified.

```
device# firmware download scp directory /buildsjc/sre/SQA/nos/slx17r.1.00/slx17r.1.00
host 10.31.2.27 user releaseuser password releaseuser
```

firmware download sftp

Specifies Secure FTP (SFTP) as the protocol used to perform a firmware download.

Syntax

firmware download sftp [**coldboot**] **directory** *directory* [**manual**] [**nocommit**] [**noreboot**] **host** { *hostname* | *host_ip_address* } **user** *username* **password** *password* **directory** *directory* [**file** *file_name*] [**noactivate**] [**use-vrf** *vrf-name*]

Parameters

coldboot

Downloads the firmware to the system and reboots both the device.

directory *directory*

Specifies a fully qualified path to the directory where the firmware is located.

file *filename*

Specifies the firmware .plist file. This parameter is optional; if unspecified, the default file, release.plist, is used.

host

Specifies the host by DNS name or IP address.

hostname

Specifies an IPv4 DNS host name.

host_ip_address

Specifies the host IP address. IPv4 and IPv6 addresses are supported.

manual

Currently, this keyword has no effect.

noactivate

Performs a firmware download without activation on the local switch.

nocommit

Disables auto-commit mode. When auto-commit mode is disabled, firmware is downloaded only to the primary partition. You must execute the firmware **commit** command manually to propagate the new image to the secondary partition. (Skips auto-commit after firmware download.)

noreboot

Disables auto-reboot mode. When auto-reboot mode is disabled, you must reboot the switch manually. If auto-commit mode was disabled, you must perform a manual firmware **commit** operation after the switch comes back up.

password *password*

Specifies the account password.

user *username*

Specifies the user login name for the host.

use-vrf *vrf-id*

Use this option to specify the name of the VRF where the host is located. If this option is not set, mgmt-vrf is used by default.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to download firmware from an external host or from an attached USB device. You can run this command interactively or provide the parameters on the command line.

Unless you specify **noactivate**, the upgrade or downgrade involves system reboots that disrupt traffic.

In addition, default-config causes the loss of configuration because it resets the configuration back to the default settings during the firmware upgrade process.

If the **firmware download** command is interrupted because of an unexpected reboot, such as a result of a software error or power failure, the command automatically recovers the corrupted secondary partition. Wait for the recovery to complete before beginning another firmware download.

This command does not support pagination.

If the **firmware download** is interrupted because of an unexpected reboot as a result of a software error or power failure, the command automatically recovers the corrupted secondary partition. Wait for the recovery to complete before starting another firmware download.

Examples

This example downloads firmware by means of SFTP and specifies a path to the directory where the firmware is located. A user login name is specified for the host and an account password is specified.

```
switch# firmware download sftp directory /buildsjc/sre/SQA/sxlos/slx17r.1.00/slx17r.1.00
host 10.31.2.27 user releaseuser password releaseuser
```

firmware download tftp

Specifies Trivial FTP (TFTP) as the protocol used to perform a firmware download.

Syntax

firmware download tftp [**coldboot**] **directory** *directory* [**manual**] [**nocommit**] [**noreboot**] **host** { *hostname* | *host_ip_address* } **user** *username* **password** *password* **directory** *directory* [**file** *file_name*] [**noactivate**] [**use-vrf** *vrf-name*]

Parameters

coldboot

Downloads the firmware to the system and reboots both the active and standby MMs.

directory *directory*

Specifies a fully qualified path to the directory where the firmware is located.

file *filename*

Specifies the firmware .plist file. This parameter is optional; if unspecified, the default file, release.plist, is used.

host

Specifies the host by DNS name or IP address.

hostname

Specifies an IPv4 DNS host name.

host_ip_address

Specifies the host IP address. IPv4 and IPv6 addresses are supported.

manual

Currently, this keyword has no effect.

noactivate

Performs a firmware download without activation on the local device.

nocommit

Disables auto-commit mode. When auto-commit mode is disabled, firmware is downloaded only to the primary partition. You must execute the firmware **commit** command manually to propagate the new image to the secondary partition. (Skips auto-commit after firmware download.)

noreboot

Disables auto-reboot mode. When auto-reboot mode is disabled, you must reboot the device manually. If auto-commit mode was disabled, you must perform a manual firmware **commit** operation after the device comes back up.

password *password*

Specifies the account password.

user *username*

Specifies the user login name for the host.

use-vrf *vrf-id*

Use this option to specify the name of the VRF where the host is located. If this option is not set, mgmt-vrf is used by default.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to download firmware from an external host or from an attached USB device. You can run this command interactively or provide the parameters on the command line.

Unless you specify **noactivate**, the upgrade or downgrade involves system reboots that disrupt traffic.

In addition, default-config causes the loss of configuration because it resets the configuration back to the default settings during the firmware upgrade process.

If the **firmware download** command is interrupted because of an unexpected reboot, such as a result of a software error or power failure, the command automatically recovers the corrupted secondary partition. Wait for the recovery to complete before beginning another firmware download.

This command does not support pagination.

If the **firmware download** is interrupted because of an unexpected reboot as a result of a software error or power failure, the command automatically recovers the corrupted secondary partition. Wait for the recovery to complete before starting another firmware download.

Examples

This example downloads firmware by means of TFTP and specifies a path to the directory where the firmware is located. The host is specified by IP address and a firmware .plist file is specified.

```
device# firmware download tftp directory /buildsjc/sre/SQA/slx/slx17r.1.00/slx17r.1.00
host 10.31.2.27 file release.plist
```

firmware download usb

Specifies USB as the protocol used to perform a firmware download.

Syntax

firmware download usb [**coldboot**] [**noactivate**] [**nocommit**] [**noreboot**] [**manual**] **directory** *directory*

Command Default

By default, the **firmware download** process reboots the system and activates the new image. Finally, the process performs a **firmware commit** operation to copy the new image to the other partition.

Parameters

coldboot

Downloads the firmware to the system and reboots both the active and standby MMs. Caution: Do not use this option unless instructed to do so by Extreme Networks Technical Support.

directory *directory*

Specifies a fully qualified path to the directory where the firmware is located.

manual

Currently, this keyword has no effect.

noactivate

Performs a firmware download without activation on the local device.

nocommit

Disables auto-commit mode. When auto-commit mode is disabled, firmware is downloaded only to the primary partition. You must execute the firmware **commit** command manually to propagate the new image to the secondary partition.

noreboot

Disables auto-reboot mode. When auto-reboot mode is disabled, you must reboot the device manually. If auto-commit mode was disabled, you must perform a manual firmware **commit** operation after the device comes back up.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to download firmware from an external host or from an attached USB device. You can run this command interactively or provide the parameters on the command line.

Unless you specify **noactivate**, the upgrade or downgrade involves system reboots that disrupt traffic.

In addition, default-config causes the loss of configuration because it resets the configuration back to the default settings during the firmware upgrade process.

If the **firmware download** command is interrupted because of an unexpected reboot, such as a result of a software error or power failure, the command automatically recovers the corrupted secondary partition. Wait for the recovery to complete before beginning another firmware download.

This command does not support pagination.

If the **firmware download** is interrupted because of an unexpected reboot as a result of a software error or power failure, the command automatically recovers the corrupted secondary partition. Wait for the recovery to complete before starting another firmware download.

Examples

To download firmware from an attached USB device using the command line:

```
device# firmware download usb directory slx_17r.1.00
```

firmware peripheral-update cpld

Updates the Complex Programmable Logic Device (CPLD) flash memory with the latest image from the installation package.

Syntax

firmware peripheral-update cpld

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on SLX 9540 and SLX 9640 devices.

The following message appears when this command is executed:

```
WARNING: Hardware image will be upgraded and followed with a board-level power cycling.
Do you want to continue?[y/n]:
```

After the CPLD is updated, the entire board is power-cycled.

Examples

The following example upgrades the firmware on an SLX 9540.

```
device# firmware peripheral-update cpld
WARNING: Hardware image will be upgraded and followed with a board-level power cycling.
Do you want to continue?[y/n]: y

for cpld0:
erasing ........done
programming ........................... 25% ........................
50% ........................... 75% ........................... 100%

for cpld1:
erasing ........done
programming ........................... 25% ........................
50% ........................... 75% ........................... 100%
```

firmware peripheral-update fpga

Updates the Field Programmable Gate Array (FPGA) flash memory with the latest image from the installation package.

Syntax

firmware peripheral-update fpga

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on SLX 9540 and SLX 9640 devices.

The following message appears when this command is executed:

```
WARNING: Hardware image will be upgraded and followed with a board-level power cycling.
Do you want to continue?[y/n]:
```

After the FPGA is updated, the entire board is power-cycled.

Examples

The following example upgrades the firmware on an SLX 9540.

```
device# firmware peripheral-update fpga
WARNING: Hardware image will be upgraded and followed with a board-level power cycling.
Do you want to continue?[y/n]: y

erasing  \ …..
erasing .. ... done
programming ........................... 25% .......
programming ........................... 25% ..........................
50% ........................... 75% ........................... 100%
sysfpga image is upgraded successfully.
device#
```

firmware recover

Recovers the previous firmware version on the device if a firmware upgrade was unsuccessful.

Syntax

firmware recover

Modes

Privileged EXEC mode

Usage Guidelines

This command reverts the operation that was performed using the firmware download "noactivate" option.

If you invoke a noactivate firmware download, the firmware is loaded to the secondary node without swapping partitions. If firmware recover is executed, it performs a forceful commit.

This command does not reboot the node.

Examples

To recover firmware on the device:

```
device# firmware recover
```

firmware restore

Swaps the partition and reboots the device.

Syntax

firmware restore

Modes

Privileged EXEC mode

Usage Guidelines

Caution
Do not use this command unless instructed by Extreme Networks Technical Support.

Use this command to restore the previously active firmware image. You can run this command only if auto-commit mode was disabled during the firmware download. After a firmware download and a reboot (with auto-commit mode disabled), the downloaded firmware becomes active. If you do not want to commit the firmware, use the **firmware restore** command.

This command reboots the device and reactivates the previous firmware. After reboot, all primary and secondary partitions restore the previous firmware image.

This command causes the device to boot up with its older firmware. Later, the image in the primary partition is automatically committed to the secondary partition.

The **firmware download** command must have been run with the **nocommit** parameter for the **firmware restore** operation to succeed.

Examples

To restore the previous firmware:

```
device# firmware restore

Restore old image to be active ...
Restore both primary and secondary image after reboot.
The system is going down for reboot NOW !!
Broadcast message from root (ttyS0) Fri Oct 26 23:48:54 2016...
Doing firmwarecommit now.
Please wait ...
```

flex-cli show link-fault-signaling

Displays information pertaining to link fault signaling (LFS).

Syntax

flex-cli show link-fault-signaling

Modes

Privileged EXEC mode

Output

The **flex-cli show link-fault-signaling** command displays the following information:

Output field	Description
Port	Port number
Rx-Link-Fault	Displays rx link fault
Tx-Link-Fault	Displays tx link fault

Examples

This example displays information pertaining to LFS.

```
device# flex-cli show link-fault-signaling
Port    Rx-Link-Fault    Tx-Link-Fault
0/1     ON               ON
0/2     ON               ON
0/3     ON               ON
0/4     ON               ON
0/5     ON               ON
0/6     ON               ON
0/7     ON               ON
0/8     ON               ON
0/9     ON               ON
0/10    ON               ON
0/11    ON               ON
0/12    ON               ON
0/13    ON               ON
0/14    ON               ON
0/15    ON               ON
0/16    ON               ON
0/17    ON               ON
0/18    ON               ON
0/19    ON               ON
0/20    ON               ON
0/21    ON               ON
0/22    ON               ON
```

flex-cli show local-fault interface

Displays the local faults of an interface.

Syntax

flex-cli show local-fault interface [**ethernet** *slot/port* | **port-channel** *port-chnnel-number*]

Parameters

ethernet

Specifies Ethernet interface.

slot-number

Specifies the slot number.

port-channel

Specifies port-channel.

port-channel numbe

Specifies the port-channel number.

Modes

Privileged EXEC mode

Examples

This example displays the local faults of an interface.

```
device# flex-cli show local-fault interface ethernet 0/9
Port    Local-Fault-Detected      Local-Fault-Count  Time-Last-Local-Fault-Dete
ted
0/9     No                                      0  N/A
dutC-Aval#
0/4     No                                      0  N/A
0/5     No                                      0  N/A
0/6     No                                      0  N/A
0/7     No                                      0  N/A
0/8     No                                      0  N/A
0/9     No                                      0  N/A
0/10    No                                      0  N/A
0/11    No                                      0  N/A
0/12    No                                      0  N/A
0/13    No                                      0  N/A
0/14    No                                      0  N/A
0/15    No                                      0  N/A
0/16    No                                      0  N/A
0/17    No                                      0  N/A
0/18    No                                      0  N/A
0/19    No                                      0  N/A
0/20    No                                      0  N/A
0/21    No                                      0  N/A
```

flex-cli show local-fault slot

Displays the local faults of a slot.

Syntax

flex-cli show local-fault slot *slot-number*

Parameters

slot-number

Specifies the slot number.

Modes

Privileged EXEC mode

Examples

This example displays the local faults of a slot.

```
device# flex-cli show local-fault slot 1
Port    Local-Fault-Detected      Local-Fault-Count  Time-Last-Local-Fault-Deteted
0/1     No                                      0  N/A
0/2     No                                      0  N/A
0/3     No                                      0  N/A
```

flex-cli show remote-fault interface

Displays the remote faults of an interface.

Syntax

flex-cli show remote-fault interface [**ethernet** *slot/port* | **port-channel** *port-channel-number*]

Parameters

ethernet

Specifies an Ethernet interface.

slot/port number

Specifies the slot or port number.

port-channel

Specifies a port-channel.

port-channel-number

Specifies the port-channel number.

Modes

Privileged EXEC mode

Examples

This example displays the remote faults of an interface.

```
device# flex-cli show remote-fault interface ethernet 0/10
Port    RFN-Detected      Remote-fault-count  Time-last-RFN-Detected
0/10    No                                0  N/A
```

flex-cli show remote-fault slot

Displays the remote faults of a slot.

Syntax

flex-cli show remote-fault slot *slot-number*

Parameters

slot-number

Specifies the slot number.

Modes

Privileged EXEC mode

Examples

This example displays the remote faults of a slot.

```
device# flex-cli show remote-fault slot 1
Port    RFN-Detected      Remote-fault-count  Time-last-RFN-Detected
0/1     No                                 0  N/A
0/2     No                                 0  N/A
0/3     No                                 0  N/A
0/4     No                                 0  N/A
0/5     No                                 0  N/A
0/6     No                                 0  N/A
0/7     No                                 0  N/A
0/8     No                                 0  N/A
0/9     No                                 0  N/A
0/10    No                                 0  N/A
0/11    No                                 0  N/A
0/12    No                                 0  N/A
0/13    No                                 0  N/A
0/14    No                                 0  N/A
0/15    No                                 0  N/A
0/16    No                                 0  N/A
0/17    No                                 0  N/A
0/18    No                                 0  N/A
0/19    No                                 0  N/A
0/20    No                                 0  N/A
0/21    No                                 0  N/A
0/22    No                                 0  N/A
```

flow-label

Enables flow label for a pseudowire (PW) profile.

Syntax

flow-label

no flow-label

Command Default

By default, control word is disabled for PW profiles.

Modes

Pseudowire profile configuration mode

Usage Guidelines

The **no** form of the command disables flow label for a PW profile.

Flow label configuration improves load balancing of PW traffic over an MPLS network, particularly in the context of PWs that transport high volumes of traffic that are comprised of multiple individual traffic flows (for example, the same source-destination pair for a Transport Control Protocol (TCP) connection is an individual traffic flow).

Examples

The following example shows how to enable flow label for a PW profile named pw_example

```
device# configure terminal
device(config)# pw-profile pw_example
device(config-pw-pw_example)# flow-label
```

The following example shows how to disable flow label for a PW profile named pw_example

```
device# configure terminal
device(config)# pw-profile pw_example
device(config-pw-pw_example)# no flow-label
```

flowspec validation

Configures Border Gateway Protocol flow specification (BGP flowspec) route validation at address-family level.

Syntax

flowspec validation [**redirect**]

no flowspec validation [**redirect**]

Command Default

Flowspec validation is enabled.

Parameters

redirect

Specifies only validation of the redirect IP nexthop address.

Modes

BGP address-family IPv4 flowspec configuration mode

Usage Guidelines

Flowspec validation can be configured at neighbor, peer-group, or address-family level with the neighbor-level configuration prioritized over peer-group level configuration and the peer-group level configuration prioritized over the address-family level configuration.

Use the **flowspec validation** command to configure flowspec validation at address-family level. To configure flowspec validation at neighbor or peer-group level, refer to the **neighbor flowspec validation** command.

By default, flowspec validation is enabled. Use the **no** form of the **flowspec validation** command to completely disable flowspec validation at address-family level. To only disable redirect IP nexthop validation at address-family level, use the **no** form of the **flowspec validation** command specifying the **redirect** opton.

Only one flowspec validation configuration is allowed at a time. Configuration operates as follows:

- When complete flowspec validation is aleady disabled, issuing the **no flowspec validation** command specifying the **redirect** option has no impact; complete flowspec validation remains disabled.
- When the **redirect** option is already disabled, issuing the **no flowspec validation** command without the **redirect** option changes the configuration to complete flowspec validation disabled.

Examples

The following example shows how to disable IPv4 flowspec validation. In this example and because the **redirect** option is specified, only redirect IP nexthop validation is disabled for the IPv4 address-family in the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 flowspec
device(config-bgp-ipv4fs)# no flowspec validation redirect
```

When flowspec validation is already completely disabled, issuing the **no flowspec validation** specifying the **redirect** option does not change the configuration. The following example shows how to completely disable flowspec validation for the IPv4 address family in a VRF named red and to verify the configuration. The **no flowspec validation** command is then issued specifying the **redirect** option, and the configuration is again displayed to show that flowspec validation remains completely disabled.

```
device(config)# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 flowspec vrf red
device(config-bgp-ipv4fs-vrf)# no flowspec validation        !completely disables
flowspec validation!
device(config-bgp-ipv4fs-vrf)# end
device(config)# show running-configuration router bgp address-family ipv4 flowspec vrf
red
!
router bgp
  address-family ipv4 flowspec vrf red
  no flowspec validation
!
device(config)# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 flowspec vrf red
device(config-bgp-ipv4fs-vrf)# no flowspec validation redirect
device(config-bgp-ipv4fs-vrf)# end
device(config)# show running-configuration router bgp address-family ipv4 flowspec vrf
red
!
router bgp
  address-family ipv4 flowspec vrf red
  no flowspec validation                        !flowspec validation remains completely
disabled!
!
```

force-switch

Forces the blocking of a specified link for Ethernet Ring Protection (ERP).

Syntax

force-switch { **vlan** *vlan_id* **ethernet** *slot/port* | **port-channel** *number* }

no force-switch { **vlan***vlan_id* **ethernet** *slot/port* | **port-channel** *number* }

Command Default

This feature is not configured by default.

Parameters

vlan *vlan_id*

Specifies a VLAN. Range is from 1 through 4090.

ethernet *slot/port*

Specifies an Ethernet interface.

port-channel *number*

Specifies a port-channel.

Modes

ERP configuration mode

Usage Guidelines

An operator can use the forced switch (FS) mechanism when no errors, a single error, or multiple errors are present in the topology. You can enter this command multiple times. You need to explicitly specify the VLAN and Ethernet slot and port.

Use the **no** form of this command to remove the configuration.

Examples

The following example configures FS for a specified interface.

```
device# configure terminal
device(config)# erp 100
device(config-erp-100)# force-switch vlan 100 ethernet 0/10
device(config-erp-100)#
```

format RFC-5424

Configures a specified syslog server to log messages using the RFC-5424 format.

Syntax

format RFC-5424

no format RFC-5424

Parameters

RFC-5424

Syslog message format defined in RFC-5424.

Modes

Syslog server configuration mode

Usage Guidelines

Use this command to configure the router to generate log messages with the RFC-5424 format.

The RFC-5424 syslog message header consists of the following fields:

<*prival*><*version*><space>< *time-stamp*><space><*host-name*><space><*app name*><space><*process id*><space><*Msg Id*>

Where:

- *prival* is the priority field. This is always <190> for SLXOS 17r.2.00.
- *version* is the version number of the syslog protocol standard. Currently, this can only be 1.
- *time-stamp* is the ISO 8601 compatible standard timestamp format (yyyy-mm-ddThh:mm:ss+-ZONE).
- *host-name* is the machine that originally sent the message, or if no hostname, a "–" is present instead.
- *app name* is the device or application that generated the message, or if no application, a "–" is present instead.
- *process id* is the process name or PID (process ID) of the syslog application that sent the message, or if no PID, a "–" is present instead. This is always – in the SLX-OS 17r.2.00 release.
- *Msg Id* is the ID number of the message, or if no Message ID, a "–" is present instead. This is always – in the SLX-OS 17r.2.00 release.

For example:

```
<190>1 2017-06-19T09:19:52.000003+00:00 SLX raslogd - -
```

Note
In the SLX-OS 17r.2.00 release, the *process id* and *Msg Id* fields are not filled and are replaced with - -.

Use the **no format RFC-5424** command to remove the RFC-5424 log message format from the syslog server configuration.

Examples

First, access the global configuration level of the CLI and configure the IP address for the syslog server. Then, enter the **format RFC-5424** command to configure the router to use the RFC-5424 format as shown in the following example.

```
device# configure terminal
device(config)# logging syslog-server 192.168.163.233
device(config-syslog-server-192.168.163.233)# format RFC-5424
```

To verify the syslog server log message format, enter the **show running-config logging syslog-server** command as shown in the following example.

```
device# running-config logging syslog-server
logging syslog-server 192.168.163.233
format RFC-5424
```

To remove the RFC-5424 format from the configured syslog server, enter the **no format RFC-5424** command as shown in the following example.

```
device(config)# logging syslog-server 192.168.163.233
device(config-syslog-server-192.168.163.233)# no format RFC-5424
```

forward-delay

Specifies the time an interface spends in each of the listening and learning states.

Syntax

forward-delay *seconds*

no forward-delay

Command Default

15 seconds

Parameters

seconds

Specifies the time that an interface spends in the Spanning Tree Protocol (STP) learning and listening states. Valid values range from 4 through 30 seconds.

Modes

Spanning tree configuration mode

Usage Guidelines

This command specifies how long the listening and learning states last before the interface begins the forwarding of all spanning-tree instances.

STP interface states:

- Listening - The interface processes the Bridge Protocol Data Units (BPDUs) and awaits possible new information that might cause it to return to the blocking state.
- Learning - The interface does not yet forward frames (packets), instead it learns source addresses from frames received and adds them to the filtering database (switching database).
- Forwarding - An interface receiving and sending data, normal operation. STP still monitors incoming BPDUs that can indicate it should return to the blocking state to prevent a loop.
- Blocking - An interface that can cause a switching loop, no user data is sent or received, but it might go to the forwarding state if the other links in use fail and the STP determines that the interface may transition to the forwarding state. BPDU data continues to be received in the blocking state.

When you change the spanning-tree forward-delay time, it affects all spanning-tree instances. When configuring the forward-delay, the following relationship should be kept:

```
(2 × (forward-delay - 1)) >= max-age >= (2 × (hello-time + 1))
```

Enter **no forward-delay** to return to the default settings.

The command is the same regardless of which type of STP is enabled.

Examples

To configure the forward-delay time to 18 seconds:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# forward-delay 18

device# configure terminal
device(config)## protocol spanning-tree rstp
device(conf-rstp)# forward-delay 18

device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# forward-delay 18

device# configure terminal
device(config)# protocol spanning-tree pvst
device(conf-pvst)# forward-delay 18

device# configure terminal
device(config)# protocol spanning-tree rpvst
device(conf-rpvst)# forward-delay 18
```

default-metric (IS-IS)

Sets the default redistribution metric value for the Intermediate System-to-Intermediate System (IS-IS) routing protocol.

Syntax

default-metric *value*

no default-metric

Command Default

The default metric value is 0.

Parameters

value

Specifies the default metric value. Valid values range from 0 through 65535. The default is 0.

Modes

IS-IS address-family IPv4 unicast configuration mode

IS-IS address-family IPv6 unicast configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command resets the default metric value to the default value of 0.

Examples

The following example sets the default metric value to 20 for the IPv4 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# default-metric 20
```

The following example sets the default metric value to 40 for the IPv6 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv6 unicast
device(config-router-isis-ipv6u)# default-metric 40
```

default-metric (IS-IS)

Sets the default redistribution metric value for the Intermediate System-to-Intermediate System (IS-IS) routing protocol.

Syntax

default-metric *value*

no default-metric

Command Default

The default metric value is 0.

Parameters

value

Specifies the default metric value. Valid values range from 0 through 65535. The default is 0.

Modes

IS-IS address-family IPv4 unicast configuration mode

IS-IS address-family IPv6 unicast configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command resets the default metric value to the default value of 0.

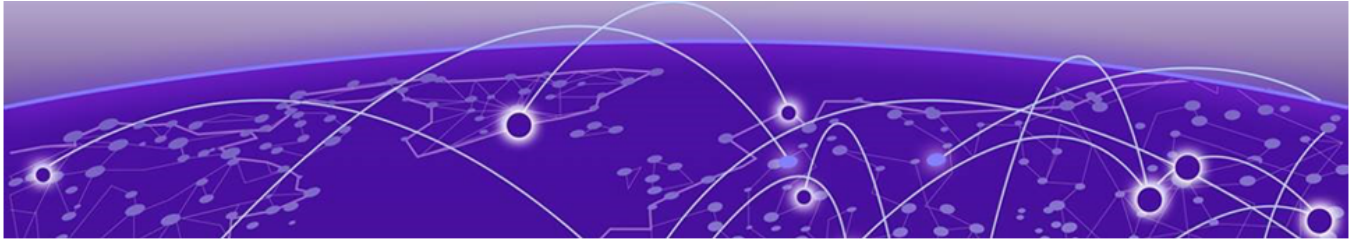
Examples

The following example sets the default metric value to 20 for the IPv4 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# default-metric 20
```

The following example sets the default metric value to 40 for the IPv6 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv6 unicast
device(config-router-isis-ipv6u)# default-metric 40
```



Commands G - J

gNMI Server Configuration on page 644
graceful-restart (BGP) on page 645
graceful-restart (LDP) on page 648
graceful-restart (OSPFv2) on page 649
graceful-restart (OSPFv3) on page 651
graceful-restart helper (OSPFv3) on page 652
graceful-restart helper-disable (IS-IS) on page 653
graceful-shutdown on page 654
grub on page 656
guard-time on page 657
handle-isis-neighbor-down on page 658
hardware on page 660
hardware media-database activate on page 661
hardware smt on page 662
hello (LLDP) on page 663
hello (MPLS RSVP) on page 665
hello (UDLD) on page 667
hello padding on page 668
hello-acknowledgements on page 670
hello-interval (LD) on page 671
hello-interval (LDP) on page 672
hello-interval (PIM) on page 673
hello-interval-link on page 674
hello-interval-target on page 675
hello-time on page 676
hello-timeout (LDP) on page 678
hello-timeout-link on page 680
hello-timeout-target on page 681
helper-only on page 682
hold-time on page 683
holdoff-time on page 684
hop-limit on page 685
host-table aging-mode conversational on page 687
host-table aging-time conversational on page 688

hostname disable on page 689
http server on page 690
implicit-commit on page 692
import l2vpn evpn reoriginate on page 694
import vpnv4 unicast reoriginate on page 695
import vpnv6 unicast reoriginate on page 696
import-map on page 697
inactivity-timer on page 698
include-all on page 699
include-any on page 701
ingress-tunnel-accounting on page 703
ingress-vlan-mapped-ve-counter on page 704
init-route-calc-delay on page 705
insight enable on page 707
insight mode on page 709
install-igp-cost on page 710
instance on page 711
interface ethernet on page 713
interface loopback on page 715
interface management on page 716
interface port-channel on page 717
interface (telemetry) on page 720
interface management on page 721
interface ve on page 723
interval on page 724
interval (telemetry) on page 725
ip access-group on page 727
ip access-list on page 729
ip address on page 731
ip address (site) on page 733
ip anycast-address on page 734
ip arp gratuitous none on page 735
ip arp inspection on page 736
ip arp inspection filter on page 737
ip arp inspection trust on page 738
ip arp learn-any on page 739
ip arp-aging-timeout on page 740
ip dhcp relay on page 742
ip dhcp relay address on page 743
ip dhcp relay gateway on page 744
ip dhcp snooping on page 745
ip dhcp snooping enable on page 746

ip dhcp snooping information option on page 747
ip dhcp snooping trust on page 748
ip directed-broadcast on page 749
ip dns on page 750
ip extcommunity-list on page 753
ip flowspec rules statistics on page 755
ip forward on page 757
ip global-subnet-broadcast-acl on page 758
ip icmp-fragment enable on page 759
ip icmp rate-limiting on page 760
ip icmp redirect on page 761
ip icmp unreachable on page 762
ip igmp immediate-leave on page 763
ip igmp last-member-query-interval on page 764
ip igmp query-interval on page 765
ip igmp query-max-response-time on page 766
ip igmp router-alert-check-disable on page 767
ip igmp snooping enable on page 768
ip igmp snooping fast-leave on page 769
ip igmp snooping last-member-query-interval on page 770
ip igmp snooping mrouter interface on page 771
ip igmp snooping querier enable on page 772
ip igmp snooping query-interval on page 773
ip igmp snooping query-max-response-time on page 774
ip igmp snooping static-group on page 775
ip igmp snooping version on page 776
ip igmp ssm-map on page 777
ip igmp static-group on page 779
ip igmp version on page 780
ip interface loopback (overlay gateway) on page 781
ip irdp on page 782
ip large-community-list extended on page 783
ip large-community-list standard on page 785
ip mtu on page 787
ip option on page 789
ip ospf active on page 791
ip ospf area on page 792
ip ospf auth-change-wait-time on page 794
ip ospf authentication-key on page 796
ip ospf bfd on page 797
ip ospf cost on page 798
ip ospf database-filter on page 799

ip ospf dead-interval on page 801
ip ospf hello-interval on page 803
ip ospf ldp-sync on page 804
ip ospf md5-authentication on page 805
ip ospf mtu-ignore on page 807
ip ospf network on page 808
ip ospf passive on page 810
ip ospf priority on page 811
ip ospf retransmit-interval on page 812
ip ospf transmit-delay on page 813
ip pim dr-priority on page 814
ip pim snooping enable on page 815
ip pim-sparse on page 816
ip pim ttl-threshold on page 817
ip port (telemetry) on page 818
ip policy route-map on page 819
ip prefix-list on page 820
ip proxy-arp on page 822
ip receive access-group on page 823
ip route on page 825
ip route next-hop-recursion on page 828
ip route static bfd on page 829
ip route static bfd holdover-interval on page 831
ip router-id on page 832
ip router isis on page 833
ip source-guard enable on page 834
ip subnet-broadcast-acl on page 835
ip subnet-rate-limit on page 836
ip vrrp-extended auth-type on page 838
ip on page 840
ipv6 access-group on page 842
ipv6 access-list on page 844
ipv6 address on page 846
ipv6 anycast-address on page 848
show ipv6 dhcp relay on page 849
ipv6 dhcp relay distance on page 850
ipv6 dhcp relay address on page 851
ipv6 dhcp relay distance on page 853
ipv6 dhcp relay maximum-delegated-prefixes on page 854
ipv6 dns on page 855
ipv6 icmpv6 redirect on page 856
ipv6 icmpv6 rate-limiting on page 857

ipv6 icmpv6 unreachable on page 858
ipv6 mld snooping enable on page 859
ipv6 mld snooping fast-leave on page 860
ipv6 mld snooping last-member-query-interval on page 861
ipv6 mld snooping mrouter interface on page 862
ipv6 mld snooping mrouter logical-interface on page 864
ipv6 mld snooping querier enable on page 866
ipv6 mld snooping query-interval on page 868
ipv6 mld snooping query-max-response-time on page 870
ipv6 mld snooping static-group on page 871
ipv6 mld snooping version on page 873
ipv6 mld ssm-map enable on page 874
ipv6 nd cache expire on page 875
ipv6 nd cache interface-limit on page 876
ipv6 option disable on page 878
ipv6 ospf active on page 879
ipv6 ospf area on page 880
ipv6 ospf authentication ipsec on page 882
ipv6 ospf authentication ipsec disable on page 883
ipv6 ospf authentication spi on page 884
ipv6 ospf bfd on page 886
ipv6 ospf cost on page 887
ipv6 ospf dead-interval on page 888
ipv6 ospf hello-interval on page 890
ipv6 ospf hello-jitter on page 892
ipv6 ospf instance on page 893
ipv6 ospf mtu-ignore on page 894
ipv6 ospf network on page 895
ipv6 ospf passive on page 897
ipv6 ospf priority on page 898
ipv6 ospf retransmit-interval on page 899
ipv6 ospf suppress-linklsa on page 900
ipv6 ospf transmit-delay on page 901
ipv6 pim dr-priority on page 902
ipv6 pim snooping enable on page 903
ipv6 pim ttl-threshold on page 904
ipv6 pim-sparse on page 905
ipv6 policy route-map on page 906
ipv6 prefix-list on page 907
ipv6 protocol vrrp on page 909
ipv6 protocol vrrp-extended on page 910
ipv6 receive access-group on page 911

ipv6 route on page 913
ipv6 route next-hop-recursion on page 916
ipv6 route null on page 917
ipv6 route next-hop-vrf on page 919
ipv6 route static bfd on page 921
ipv6 route static bfd holdover-interval on page 923
ipv6 router isis on page 924
ipv6 router ospf on page 925
ipv6 router pim on page 926
ipv6 prefix-list on page 927
ipv6 subnet-zero drop on page 929
ipv6 vrrp-extended auth-type on page 930
ipv6 vrrp-extended-group on page 931
ipv6 vrrp-group on page 932
ipv6 vrrp-suppress-interface-ra on page 933
is-type on page 934
isis auth-check on page 936
isis auth-key on page 937
isis auth-mode on page 939
isis bfd on page 940
isis circut-type on page 941
isis hello-interval on page 942
isis hello-multiplier on page 943
isis hello padding on page 945
isis ipv6 metric on page 946
isis ldp-sync on page 948
isis metric on page 949
isis passive on page 951
isis point-to-point on page 952
isis priority on page 953
isis reverse-metric on page 955
iterations on page 957

gNMI Server Configuration

Configures the secure gNMI server.

Syntax

gNMI server

no gNMI server

Command Default

By default, non TLS gNMI server runs on port 9339.

Examples

This configures a secure-port for TLS gNMI server. Choose a unique port in the range of 1024 to 49151. TLS certificates are to be imported for gNMI server should be imported before configuring the secure-port. For importing TLS server certificate, refer to *crypto ca import-pkcs* section.

```
SLX# configure terminal
Entering configuration mode terminal
SLX(config)# gNMI server
SLX(config-gNMI-server)# secure-port ?
Possible completions:
<NUMBER:1024-49151>   Port range from 1024 to 49151
SLX(config-gNMI-server)# secure-port <NUMBER>
```

Example.

```
SLX(config-gNMI-server)# secure-port 9449
```

Use the *show running-config gNMI* command to view the configuration.

Unconfigures the secure gNMI server. Henceforth, non-TLS gNMI server will be running.

```
SLX(config-gNMI-server)# no secure-port
```

graceful-restart (BGP)

Enables the BGP graceful restart capability.

Syntax

graceful-restart [**purge-time** *seconds* | **restart-time** *seconds* | **stale-routes-time** *seconds*]

no graceful-restart

Command Default

Disabled.

Parameters

purge-time

Specifies the maximum period of time, in seconds, for which a restarting device maintains stale routes in the BGP routing table before purging them. The default value is 600 seconds. The configurable range of values is from 1 to 3600 seconds.

restart-time

Specifies the restart-time, in seconds, advertised to graceful restart-capable neighbors. The default value is 120 seconds. The configurable range of values is from 1 to 3600 seconds.

stale-routes-time

Specifies the maximum period of time, in seconds, that a helper device will wait for an End-of-RIB (EOR) message from a peer. All stale paths are deleted when this time period expires. The default value is 360 seconds. The configurable range of values is from 1 to 3600 seconds.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

BGP address-family L2VPN EVPN configuration mode

Usage Guidelines

Use this command under a BGP address-family configuration mode to enable or disable the graceful-restart capability for all BGP neighbors in the address family. When this command is enabled, graceful-restart capability is negotiated with neighbors in

the BGP OPEN message when a session is established. If the neighbor advertises support for graceful restart, that function is activated for that neighbor session. Otherwise, graceful restart is not activated for that session, even though it is enabled locally. If the neighbor has not sent graceful-restart parameters, the restarting device will not wait for the neighbor to start route calculation, but graceful restart will be enabled.

If the graceful-restart capability is enabled after a BGP session has been established, the neighbor session must be cleared for graceful restart to take effect.

The **purge-time** parameter is applicable for both restarting and helper devices. The timer starts when a BGP connection is closed. The timer ends when an EOR is received from all nodes, downloaded into BGP and an EOR sent to all neighbors. The configured purge-time timer value is effective only on the configured node.

The **restart-time** parameter is applicable only for helper devices. The timer starts at the time the BGP connection is closed by the remote peer and ends when the Peer connection is established. The configured restart-time timer value is effective only on the peer node, and not in the configured node. During negotiation time, the timer value is exchanged.

The **stale-routes-time** parameter is applicable only for helper devices. The timer starts when the peer connection is established after the HA-failover. The timer ends at the time an EOR is received from the peer. The configured stale-time timer value is effective only on the configured node.

For non-default VRF instances, graceful restart timers are inherited from the default VRF. The **purge-time**, **restart-time**, and **stale-routes-time** parameters are not available in BGP address-family IPv4 unicast VRF configuration mode and BGP address-family IPv6 unicast VRF configuration mode.

Use the **clear ip bgp neighbor** command with the **all** parameter for the changes to the graceful-restart parameters to take effect immediately.

The **no** form of the command disables the BGP graceful-restart capability globally for all BGP neighbors in the address family.

Examples

The following example enables the BGP graceful restart capability.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 1
device(config-bgp-router)# neighbor 1.1.1.1 remote-as 2
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# graceful-restart
```

The following example sets the purge time to 240 seconds.

```
device# configure terminal
device(config)# router bgp
```

```
device(config-bgp-router)# local-as 1
device(config-bgp-router)# neighbor 1.1.1.1 remote-as 2
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# graceful-restart
%Warning: Please clear the neighbor session for the parameter change to take effect!
device(config-bgp-ipv4u)# graceful-restart purge-time 240
```

The following example sets the restart time to 60 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 1
device(config-bgp-router)# neighbor 1.1.1.1 remote-as 2
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# graceful-restart
%Warning: Please clear the neighbor session for the parameter change to take effect!
device(config-bgp-ipv4u)# graceful-restart restart-time 60
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

The following example sets the stale-routes time to 180 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 1
device(config-bgp-router)# neighbor 1000::1 remote-as 2
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 1000::1 activate
device(config-bgp-ipv6u)# graceful-restart
%Warning: Please clear the neighbor session for the parameter change to take effect!
device(config-bgp-ipv6u)# graceful-restart stale-routes-time 180
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

The following example enables the BGP graceful restart capability and sets the purge time to 220 seconds in L2VPN EVPN configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# graceful-restart purge-time 220
```

graceful-restart (LDP)

Enables the MPLS LDP graceful restart capability for all LDP sessions and accesses the graceful restart (GR) configuration mode .

Syntax

graceful-restart

no graceful-restart

Command Default

Disabled.

Modes

MPLS LDP configuration mode

Usage Guidelines

When you enable LDP GR, the router waits until it receives an LDP Initialization message from its neighbor to know whether it must delete its states or start the LDP GR recovery procedure. It is applicable to all LDP sessions regardless of the adjacency type exists between the neighbors.

The **no** form of the command disables the LDP graceful-restart capability globally for all LDP sessions and removed the configuration.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example enables the BGP graceful restart capability.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# graceful-restart
```

graceful-restart (OSPFv2)

Enables the OSPF Graceful Restart (GR) capability.

Syntax

graceful-restart [**helper-disable** | **restart-time** *seconds*]

no graceful-restart

Command Default

Graceful restart and graceful restart helper capabilities are enabled.

Parameters

helper-disable

Disables the GR helper capability.

restart-time

Specifies the maximum restart wait time, in seconds, advertised to neighbors. The default value is 120 seconds. The configurable range of values is from 10 through 1800 seconds.

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

Use **no graceful-restart helper-disable** to re-enable the GR helper capability.

The **no** form of the command disables the graceful restart capability.

Examples

The following example disables the GR helper capability.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# graceful-restart helper-disable
```

The following example re-enables the GR helper capability.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# no graceful-restart helper-disable
```

The following example re-enables the GR capability and changes the maximum restart wait time from the default value to 240 seconds.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# graceful-restart restart-time 240
```

graceful-restart (OSPFv3)

Enables the OSPFv3 Graceful Restart capability.

Syntax

graceful-restart [**helper** | **restart-time** *seconds*]

no graceful-restart [**helper** | **restart-time** *seconds*]

Command Default

By default, graceful restart and graceful restart helper capabilities are enabled.

Parameters

helper

Sets graceful restart helper options.

restart-time *seconds*

Specifies the maximum restart wait time, in seconds, advertised to neighbors. The default value is 120 seconds. Valid values range from 10 through 1800 seconds.

Modes

OSPF IPv6 router configuration mode

OSPFIPv6 router VRF configuration mode

Usage Guidelines

Use the **no graceful-restart** command to disable graceful restart mode.

Use the **no graceful-restart helper** command to disable the graceful restart helper capability.

Examples

This example disables the graceful restart helper capability.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# no graceful-restart helper
```

This example sets the graceful restart interval to 130 seconds.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# graceful-restart restart-time 130
```

graceful-restart helper (OSPFv3)

Enables the OSPFv3 graceful restart (GR) helper capability.

Syntax

graceful-restart helper { **disable** | **strict-lsa-checking** }

no graceful-restart helper

Command Default

GR helper is enabled.

Parameters

disable

Disables the OSPFv3 GR helper capability.

strict-lsa-checking

Enables the OSPFv3 GR helper mode with strict link-state advertisement (LSA) checking.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The **no** form of the command disables the GR helper capability on a device.

Examples

The following example enables GR helper and sets strict LSA checking.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# graceful-restart helper strict-lsa-
checking
```

graceful-restart helper-disable (IS-IS)

Disables and enables Intermediate System-to-Intermediate System (IS-IS) graceful restart helper mode.

Syntax

graceful-restart helper-disable

no graceful-restart helper-disable

Command Default

The graceful restart helper is enabled by default.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command re-enables the graceful restart helper if it has been disabled.

Examples

The following example disables the IS-IS graceful restart helper.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# graceful-restart helper-disable
```

The following example re-enables the IS-IS graceful restart helper.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no graceful-restart helper-disable
```

graceful-shutdown

Gracefully shuts down all BGP neighbors.

Syntax

graceful-shutdown *seconds* [**community** *value* [**local-preference** *value*] | **local-preference** *value* [**community** *value*] | **route-map** *route-map-name*]

no graceful-shutdown *seconds* [**community** *value* [**local-preference** *value*] | **local-preference** *value* [**community** *value*] | **route-map** *route-map-name*]

Command Default

Default graceful shutdown parameters are applied.

Parameters

seconds

Specifies the number of seconds in which the BGP graceful shutdown will occur. Valid values range from 30 through 600 seconds.

community *value*

Sets the community attribute for graceful shutdown. Valid values range from 1 through 4294967295.

local-preference *value*

Sets the local preference attribute for graceful shutdown. Valid values range from 0 through 4294967295.

route-map *route-map-name*

Specifies the route map for graceful shutdown attributes.

Modes

BGP configuration mode

Usage Guidelines

The **no** form of the command de-activates graceful shutdown.

Examples

The following example gracefully shuts down all BGP neighbors and sets the graceful shutdown timer to 180 seconds.

```
device# configure terminal
```

```
device(config)# router bgp
device(config-bgp-router)# graceful-shutdown 180
```

The following example gracefully shuts down all BGP neighbors and sets the graceful shutdown timer to 600 seconds. The route map “myroutemap” is specified for graceful shutdown attributes.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# graceful-shutdown 600 route-map myroutemap
```

The following example gracefully shuts down all BGP neighbors and sets the graceful shutdown timer to 600 seconds. The community attribute is set to 10.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# graceful-shutdown 600 community 10
```

grub

This command navigates into the GRUB configuration mode.

Syntax

grub

Modes

Global Configuration mode

Usage Guidelines

The GRUB configuration mode is used to configure a password for securing GRUB from unauthorized changes.

Examples

The following example navigates into the GRUB configuration mode.

```
SLX # configure terminal
SLX (config)# grub
SLX (config-grub) #
```

guard-time

Specifies a value for the Ethernet Ring Protection (ERP) guard timer.

Syntax

guard-time *time*

no guard-time

Command Default

The guard timer is configured at 1500 milliseconds (ms) by default.

Parameters

time

Time in ms. Range is from 1200 through 4000, in intervals of 100.

Modes

ERP configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

The following example configures a guard timer value of 1400 ms.

```
device# configure terminal
device(config)# erp 1
device(config-erp-1)# guard-time 1400
```

handle-isis-neighbor-down

Globally enables the handling of an IGP neighbor down event by MPLS. This command takes effect immediately and you can run it as needed.

Syntax

handle-isis-neighbor-down

no handle-isis-neighbor-down

Command Default

By default, RSVP does not handle IGP neighbor down events. RSVP IGP synchronization must be enabled to handle an IGP neighbor down event.

Modes

MPLS policy mode (config-router-mpls-policy)

Usage Guidelines

The **handle-isis-neighbor-down** command is independent of MPLS traffic engineering configurations. The **handle-isis-neighbor-down** command allows MPLS (RSVP) to handle IGP neighbor down events and take action, such as tearing down the associated RSVP sessions. For example, when IS-IS is configured as MPLS TE protocol, the user can still configure MPLS to handle an OSPF neighbor down event (and vice versa).

An IGP neighbor down event is handled only by the RSVP sub-component of MPLS by tearing down the associated sessions. This event is not handled by LDP sub-component of MPLS.

MPLS RSVP does not keep track of the current state of IGP neighbor. That is, when an IGP neighbor goes down, RSVP tears down all the associated sessions. But RSVP does not prevent bringing up any session while the IGP neighbor to RSVP next-hop is down (or not yet available). That is, the RSVP session is brought up even when the IGP neighbor to the next-hop does not exist.

An IGP neighbor down is treated as upstream neighbor down or downstream neighbor down event by RSVP, depending upon the direction of the LSP. When a downstream IGP neighbor goes down, it results in an LSP tear down or FRR switchover, whichever is applicable.

MPLS receives and processes an IGP neighbor down event only for the cases when an IGP neighbor goes down because of hellos not received from the peer.

When an IGP neighbor goes down because of an underlying interface down, MPLS does not react to an IGP neighbor down event as RSVP would also receive the interface

down event and tears down associated LSP sessions. Handling an IGP neighbor down event is redundant in such situations.

When BFD is configured on IGP interfaces, an IGP neighbor down is detected quickly and may help RSVP converge faster.

When an IGP neighbor is Nonstop Routing or Graceful Restart capable, MPLS does not receive a neighbor down event when NSR is performed on the peer IGP router.

Faster FRR feature is not be triggered when MPLS detects that IGP neighbor is down. Instead, each FRR LSP is processed individually to perform local repair.

It is highly recommended to observe extreme caution when implementing this feature when BFD is enabled for the underlying IGP. Under some circumstances, unnecessary flapping for RSVP sessions/LSPs can occur with this combination.

The **no** version of the command does not handle IGP neighbor down events.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example shows how to enable the RSVP to handle IGP neighbor down events for IS-IS.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# handle-isis-neighbor-down
```

hardware

Accesses hardware configuration mode, from which you can also access the connector and the profile configuration modes.

Syntax

hardware

Modes

Global configuration mode

Examples

The following example shows the accessing of hardware configuration mode.

```
device# configure terminal
device(config)# hardware
device(config-hardware)#
```

hardware media-database activate

Activates the media-database, which contains a list of the port media that the device supports.

Syntax

hardware media-database activate

Command Default

By default, the media-database is not activated.

Modes

Privileged EXEC mode

Usage Guidelines

The media-database contains the list of port media supported on the device. This information is saved in an .xml file on the device.

The default version of the file is provided in the release package. You can also download your own version or upload the file to a remote server for modification. After a new media-database is downloaded to the device, it needs to be activated to take effect.

You can use the **show hardware media-database** command to see the supported media types in the media-database file.

After the media-database is activated, the device sends RASLOG to warn against incompatible media that is detected on the ports. You can use this information to help identify the cause of links that do not come online.

Examples

This example activates the media-database file.

```
device# hardware media-database activate
device#
```

hardware smt

Enables or disables simultaneous multithreading (SMT).

Syntax

hardware smt { **enable** | **disable** }

Command Default

By default, SMT is enabled.

Parameters

enable

Enables SMT.

disable

Disables SMT.

Modes

Privileged EXEC mode

Usage Guidelines

SMT is a performance optimization mechanism deployed by Intel processors. To help mitigate security vulnerabilities related to SMT, use the **hardware smt** command to enable or disable SMT.

By enabling SMT, you disable the security mitigation in favor of better performance. By disabling SMT, you enable the security mitigation.

You need to restart the device to enable changes. A warning message in the CLI reminds you to do so.

This command is supported on the Broadcom Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

This example enables SMT.

```
device# hardware smt enable
Warning: Please reload the switch to activate the new SMT setting.
```

This example disables SMT.

```
device# hardware smt disable
Warning: Performance will be impacted with SMT disabled.
Warning: Please reload the switch to activate the new SMT setting.
```

hello (LLDP)

Sets the interval between LLDP hello messages.

Syntax

hello *seconds*

no hello

Command Default

30 seconds

Parameters

seconds

Valid values range from 4 through 180 seconds.

Modes

LLDP protocol and profile configuration modes

Usage Guidelines

The LLDP hello messages can also be configured for a specific LLDP profile. When you apply an LLDP profile on an interface using the **lldp profile** command, it overrides the global configuration. If a profile is not present, then the default global profile is used until you create a valid profile.

Enter **no hello** to return to the default setting.

Examples

To set the time interval to 10 seconds between the transmissions:

```
device# configure terminal
device (config)# protocol lldp
device(conf-lldp)# hello ?
Possible completions:
<4-180>   Seconds[30 seconds]
device(conf-lldp)# hello 10
```

To set the time interval to 8 seconds between the transmissions for a specific LLDP profile:

```
device(conf-lldp)# profile test1
device(config-profile-test1)# hello 8
device(config-profile-test1)#
```

hello (MPLS RSVP)

Enables RSVP Hello on all RSVP interfaces and configure the interval and tolerance.

Syntax

hello [**interval** *seconds*] [**tolerance** *number*]

no hello [**interval**] [**tolerance**]

Command Default

RSVP Hello is disabled on the device.

The default interval is 9 seconds.

The default tolerance is 3 unacknowledged RSVP Hello requests before timeout.

Parameters

interval *seconds*

Specifies the interval in seconds between two RSVP Hello requests. Enter an integer from 1 to 60.

tolerance *number*

Specifies the number of unacknowledged RSVP Hello requests before timeout. Enter a number from 1 to 255.

Modes

MPLS RSVP configuration mode

MPLS interface RSVP configuration mode

Usage Guidelines

When you configure the interval and tolerance for the RSVP-TE Hello protocol globally, they are pushed to all MPLS interfaces when MPLS interface configurations are not present. In addition to these two parameters, you can configure the acknowledgments globally.

You can configure RSVP-TE Hello interval and tolerance on an MPLS interface. The interface configurations take precedence over global configurations.

By default, acknowledgments are not sent on the MPLS interface supporting RSVP Hello when no sessions are taken on the interface.

Caution

When disabling RSVP hello, disable it on both sides of the link at the same time to avoid bringing down all the RSVP sessions going over that link.

Use the **no** command to disable RSVP Hello, or to reset the default interval or tolerance settings.

The **no hello** command on the MPLS interface sets the RSVP-TE Hello parameters to the globally configured RSVP Hello parameter values. If RSVP Hello is not configured globally, it disables the RSVP Hello on the MPLS interface. Executing this removes the configuration from the interface.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example enables RSVP hello globally and configures the interval at 15 seconds and a tolerance of 8.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# rsvp
device(config-router-mpls-rsvp)# hello interval 15 tolerance 8
```

The following example enables RSVP hello on an MPLS interface and configures the interval at 20 seconds and a tolerance of 10.

```
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/12
device(config-router-mpls-interface-0/12)# rsvp
device(config-router-mpls-interface-0/12-rsvp)# hello interval 20 tolerance 10
```

hello (UDLD)

Sets the hello transmit interval.

Syntax

hello *hundred_milliseconds*

no hello

Command Default

5 is the default value (500 milliseconds).

Parameters

hundred_milliseconds

Valid values range from 1 through 60 (in counts of 100 milliseconds).

Modes

Unidirectional link detection (UDLD) protocol configuration mode

Usage Guidelines

Use this command to set the time interval between the transmission of hello UDLD PDUs from UDLD-enabled ports.

Enter **no hello** to return to the default setting.

Examples

To set the time interval to 2,000 milliseconds between hello UDLD PDU transmissions:

```
device# configure terminal
device(config)# protocol udld
 device(config-udld)# hello 20
```

hello padding

Re-enables the padding of Intermediate System-to-Intermediate System (IS-IS) hello Protocol Data Units (PDUs) globally.

Syntax

hello padding [**disable**] [**point-to-point**]

no hello padding [**disable**] [**point-to-point**]

Command Default

Enabled.

Parameters

disable

Disables the padding of IS-IS hello PDUs.

point-to-point

Specifies point-to-point interfaces.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Generally, you do not need to disable padding unless a link is experiencing slow performance. If you enable or disable padding on an interface using the **isis hello padding** command, the interface setting overrides the global setting.

The **no** form of the command disables the padding of IS-IS hello PDUs.

Examples

The following example globally disables padding of IS-IS hello PDUs.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# hello padding disable
```

The following example globally disables padding of IS-IS hello PDUs for point-to-point interfaces.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# hello padding disable point-to-point
```

The following example globally re-enables padding of IS-IS hello PDUs.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# hello padding
```

The following example globally re-enables padding of IS-IS hello PDUs for Point-to-Point interfaces.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# hello padding point-to-point
```

hello-acknowledgements

Configures the MPLS RSVP-TE Hello to respond back with Hello ACKs to neighbors not carrying any RSVP sessions.

Syntax

hello-acknowledgements

no hello-acknowledgements

Command Default

By default, RSVP Hello acknowledgements are disabled.

Modes

MPLS RSVP configuration mode

Usage Guidelines

Use the **no** form of this command to reset the default behavior.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only..

Examples

The following example enables RSVP Hello acknowledgements.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# rsvp
device(config-router-mpls-rsvp)# hello-acknowledgements
```

hello-interval (LD)

Configures a global hello interval for the loop-detection (LD) protocol.

Syntax

hello-interval *milliseconds*

no hello-interval

Command Default

The default interval is 1000 milliseconds.

Parameters

milliseconds

Range is from 100 through 5000 milliseconds. The default is 1000 milliseconds.

Modes

Protocol Loop Detection configuration mode

Usage Guidelines

Use the no form of this command to revert to the default hello interval.

Examples

To configure a hello interval of 2000 milliseconds:

```
device# configure terminal
device(config)# protocol loop-detection
device(config-loop-detect)# hello-interval 2000
```

To revert to the default hello interval:

```
device# configure terminal
device(config)# protocol loop-detection
device(config-loop-detect)# no hello-interval
```

hello-interval (LDP)

Sets the interval between LDP Hello messages for LDP sessions for LDP interfaces. These messages maintain LDP sessions between the device and its LDP peers.

Syntax

hello-interval *interval*

no hello-interval *interval*

Command Default

For an LDP interface configuration, the default value is the interval for the configured global LDP Hello messages.

Parameters

interval

Specifies the interval in seconds. Enter an integer from 1 through 32767.

Modes

MPLS interface LDP configuration mode

Usage Guidelines

Use this command to set the interval for LDP Link Hello messages that are multicast to all routers on the subnet.

When you configure the LDP link interval for an interface, it overrides the global interval.

When a Hello Adjacency already exists, the adjacency remains up and any new configured interval takes effect upon the expiration of the current Hello Interval timer. Consequently, the next and subsequent Hello messages are sent at the new interval.

Use the **no** for this command to reset the default interval.

Examples

The following example sets the link Hello message interval for the interface to 30 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 1/2
device(config-router-mpls-interface-1/2)# ldp-params
device(config-router-mpls-interface-1/2-ldp-params)# hello-interval 30
```

hello-interval (PIM)

Configures the frequency with which the device sends PIM hello messages to its neighbors.

Syntax

hello-interval *seconds*

no hello-interval

Command Default

By default, the hello-interval is 30 seconds.

Parameters

seconds

Specifies the hello interval in seconds. The range is 10 through 3600 seconds.

Modes

PIM Router configuration mode

Usage Guidelines

Use the **no hello-interval** form of this command to reset the default interval.

Devices use PIM hello messages to advertise themselves as PIM routing devices to their neighbors. At the beginning of an interval, a device sends a hello message, and the timer is reset. The device drops any neighbor that doesn't respond to the message in a period that is 3.5 times the hello interval.

Examples

The following example configures the IPv4 PIM hello interval.

```
device(config)# router pim
device(config-pim-router)# hello-interval 50
```

The following example configures the IPv6 PIM hello interval.

```
device(config)# ipv6 router pim
device(config-ipv6-router-pim-vrf-default-vrf)# hello-interval 50
```

hello-interval-link

Sets the interval between LDP link Hello messages globally which applies to all LDP interfaces. These messages are used to maintain LDP sessions between the device and its LDP peers.

Syntax

hello-interval-link *interval*

no hello-interval-link

Command Default

The default is 5 seconds.

Parameters

interval

Specifies the interval in seconds. Enter an integer from 1 through 32767.

Modes

MPLS LDP configuration mode

Usage Guidelines

Use this command to globally set the interval for LDP Link Hello messages that multicast to all routers on the subnet.

When you configure the LDP link interval for an interface, it overrides the global interval for the interface.

When a Hello Adjacency already exists, the adjacency remains up and any new configured interval takes effect upon the expiration of the current Hello Interval timer. Consequently, the next and subsequent hello messages are sent at the new interval.

Use the **no** for this command to reset the default interval.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example sets the global interval to 10 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# hello-interval-link 10
```

hello-interval-target

Sets the interval between LDP Targeted Hello messages globally for all LDP interfaces. These messages are used to maintain LDP sessions between the device and its LDP peers.

Syntax

hello-interval-target *interval*

no hello-interval-target

Command Default

The default is 15 seconds.

Parameters

interval

Specifies the interval in seconds. Enter an integer from 1 through 32767.

Modes

MPLS LDP configuration mode

Usage Guidelines

Use this command to set the interval for LDP Targeted Hello messages that are unicast to a specific address, such as a VLL peer.

For targeted LDP sessions, the LDP Hello Interval can only be set globally.

Use the **no** for this command to reset the default interval.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example sets the interval for LDP Targeted Hello messages to 10 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# hello-interval-target 10
```

hello-time

Sets the interval between the hello Bridge Protocol Data Units (BPDUs) sent on an interface.

Syntax

hello-time *seconds*

no hello-time

Command Default

2 seconds

Parameters

seconds

Specifies the time interval between the hello BPDUs sent on an interface. Valid values range from 1 through 10 seconds.

Modes

Spanning tree configuration mode

Usage Guidelines

This command configures the spanning-tree bridge hello time, which determines how often the device broadcasts hello messages to other devices.

If the VLAN parameter is not provided, the **hello-time** value is applied globally for all per-VLAN instances. But for the VLANs which have been configured explicitly, the per-VLAN configuration takes precedence over the global configuration. When configuring the **hello-time**, the **max-age** command setting must be greater than the **hello-time** setting. The following relationship should be kept:

```
(2 × (forward-delay - 1)) >= max-age >= (2 × (hello-time + 1))
```

Enter **no hello-time** to return to the default settings.

The command is the same regardless of which type of STP is enabled.

Examples

To configure spanning tree bridge hello time to 5 seconds:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# hello-time 5
```

```
device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# hello-time 5

device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# hello-time 5

device# configure terminal
device(config)# protocol spanning-tree pvst
device(conf-pvst)# hello-time 5

device# configure terminal
device(config)# protocol spanning-tree rpvst
device(conf-rpvst)# hello-time 5
```

hello-timeout (LDP)

Sets how long the device waits for its LDP peers for LDP sessions to send a Hello message for LDP interfaces.

Syntax

hello-timeout *seconds*

no hello-timeout *seconds*

Command Default

For an LDP interface configuration, the default value is the hold time for the configured global LDP Hello messages.

Parameters

seconds

Specifies the hold time in seconds. Enter an integer from 2 through 65335. The minimum value that can be configured for the hold time is two times the value set for the Hello interval.

Modes

MPLS interface LDP configuration mode

Usage Guidelines

When the device does not receive a Hello message within this time, the LDP session with the peer can be terminated. The device includes the hold time in the Hello messages it sends out to its LDP peers.

The new time takes effect immediately and goes in the next Hello message sent. This hold time applies to only the hold time that the device sends to its peers. It does not affect the hold time the device uses to time out those peers. The latter is determined from the hold time that peers send to the device.

Use the **no** for this command to reset the default interval.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example sets the link Hello hold time for the interface to 30 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/2
```

```
device(config-router-mpls-interface-0/2)# ldp-params
device(config-router-mpls-interface-0/2-ldp-params)# hello-timeout 30
```

hello-timeout-link

Sets how long the device waits for its LDP peers for link LDP sessions to send a Hello message.

Syntax

hello-timeout-link *seconds*

no hello-timeout-link

Command Default

The default is 15 seconds.

Parameters

seconds

Specifies the hold time in seconds. Enter an integer from 2 through 65335.

Modes

MPLS LDP configuration mode

Usage Guidelines

When the device does not receive a Hello message within this time, the LDP session with the peer can be terminated. The device includes the hold time in the Hello messages it sends out to its LDP peers.

The new time takes effect immediately and goes in the next Hello message sent. This hold time applies to only the hold time that the device sends to its peers. It does not affect the hold time the device uses to time out those peers. The latter is determined from the hold time that peers send to the device.

Use the **no** for this command to reset the default hold time.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example sets the global hold time to 10 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# hello-timeout-link 10
```

hello-timeout-target

Sets how long the device waits for its LDP peers for targeted LDP sessions to send a Hello message.

Syntax

hello-timeout-target *seconds*

no hello-timeout-target

Command Default

The default is 45 seconds.

Parameters

seconds

Specifies the hold time in seconds. Enter an integer from 2 through 65335.

Modes

MPLS LDP configuration mode

Usage Guidelines

When the device does not receive a Hello message within this time, the LDP session with the peer can be terminated. The device includes the hold time in the Hello messages it sends out to its LDP peers.

The new time takes effect immediately and goes in the next Hello message sent. This hold time applies to only the hold time that the device sends to its peers. It does not affect the hold time the device uses to time out those peers. The latter is determined from the hold time that peers send to the device.

Use the **no** for this command to reset the default timeout.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example sets the global hold time to 10 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# hello-timeout-target 10
```

helper-only

Specifies that the LSR acts as a helper only for LDP graceful restart (GR).

Syntax

helper-only

no helper-only

Command Default

Full LDP GR mode with the router acting either as a restarting router or a GR helper.

Modes

MPLS LDP GR configuration mode

Usage Guidelines

A GR helper is an LSR whose neighbor is restarting its LDP component.

In helper mode, a router does not preserve its forwarding entries on a LDP GR restart. It indicates to its peers that forwarding state is not preserved by sending an initialization message with the Reconnect Time and the Recovery Time set to zero (0) in FT session TLV. The configuration commands for reconnect-time and recovery-time are rejected with informational messages. However, it can help a neighboring router recover its forwarding entries when the neighbor is going through restart.

The **no** form of the command removes the LDP GR helper mode and revert back to full LDP GR mode with the router acting either as a restarting router or a GR helper.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures the LSR for LDP GR helper mode only.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# graceful-restart
device(config-router-mpls-ldp-gr)# helper-only
```

hold-time

Sets the time that a previously down backup VRRP router, which also must have a higher priority than the current master VRRP router, will wait before assuming mastership of the virtual router.

Syntax

hold-time *range*

Command Default

0 seconds

Parameters

range

A value between 1 and 3600 seconds that specifies the time a formerly down backup router waits before assuming mastership of the virtual router.

Modes

Virtual-router-group configuration mode

Usage Guidelines

The hold-time must be set to a number greater than the default of 0 seconds for this command to take effect.

This command can be used for both VRRP and VRRP-E.

Examples

To set the hold time to 60 seconds for backup routers in a specific virtual router:

```
device# configure terminal
device(config)# interface ve 25
device(config-ve-25)# vrrp-extended-group 1
device(config-vrrp-extended-group-1)# hold-time 60
```

holdoff-time

Specifies a value for the Ethernet Ring Protection (ERP) holdoff timer.

Syntax

holdoff-time *time*

no holdoff-time

Command Default

The default holdoff-time value is 0 milliseconds (ms).

Parameters

time

Time in ms. Range is from 0 through 10000, in intervals of 100.

Modes

ERP configuration mode

Usage Guidelines

To prevent unnecessary Signal Fail events resulting from port flapping, when a link error occurs the event is not reported immediately. When the hold-off timer expires, ERP checks to see whether the error still exists.

Use the **no** form of this command to restore the default value.

Examples

The following example configures a holdoff-time of 100 ms.

```
device# configure terminal
device(config)# erp 1
device(config-erp-1)# holdoff-time 100
```

hop-limit

Gives the ability to change the hop limit to a lower number.

Syntax

hop-limit *number*

hop-limit *number*

Command Default

By default, there is no hop-limit configuration .

Parameters

number

Specifies the selected number of hops in the path. The range for the number of hops is 0 - 255 with a default number of 255.

Modes

MPLS LSP configuration mode (config-router-mpls-lsp-*lsp_name*).

MPLS router bypass LSP configuration mode (config-router-mpls-bypass-lsp-*bypass_name*).

MPLS router MPLS interface dynamic bypass configuration mode (config-router-mpls-if-ethernet-*slot/port*-dynamic-bypass)

Usage Guidelines

The **no** form of the command removes the specified number of hops and returns to the default hop number of 255 hops.

The user can configure an interface level hop-limit for dynamic Bypass LSPs to be created corresponding to a protected link.

Compute the dynamic bypass path, so the hop-limit is the minimum number of the backup requested hop limit and the interface mode configured hop limit. This computed hop limit sets as the dynamic bypass LSP hop limit during the initial creation of dynamic bypass.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example limits the CSPF to choosing a path consisting of no more than *20* hops for LSP *tunnel1* .

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp tunnel1
device(config-router-mpls-lsp-tunnel1)# hop-limit 20
```

The following example configures the bypass LSP hop limit to *6*.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# bypass-lsp my-bypass-lsp
device(config-router-mpls-bypass-lsp-my-bypass-lsp)#  hop-limit 6
```

The following example configures dynamic bypass MPLS Ethernet interface *0/8* s hop-limit to *5* .

```
device# configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/8
device(config-router-mpls-if-ethernet-0/8)# dynamic bypass
device(config-router-mpls-if-ethernet-0/8-dynamic-bypass)# hop-limit 5
```

host-table aging-mode conversational

Enables conversational address-resolution protocol (ARP) and conversational neighbor discovery (ND). Such enablement improves hardware utilization by programming only active flows into the forwarding plane.

Syntax

host-table aging-mode conversational

no host-table aging-mode conversational

Command Default

Conversational ARP/ND is disabled.

Modes

Global configuration mode

Usage Guidelines

You can change the aging-time value from the 300 second default—either before or during enablement—by entering the **host-table aging-time conversational** command.

Conversational ARP/ND can be CPU-intensive.

If conversational ARP/ND is not enabled, make sure that the software ARP/ND cache size is less than the hardware profile limit.

To disable conversational ARP/ND, enter the **no** form of this command.

Upon disablement, the conversational ARP/ND timers no longer apply: All current entries become permanent as do all new entries.

Examples

The following example enables conversational ARP/ND.

```
device# configure terminal
device(config)# host-table aging-mode conversational
```

host-table aging-time conversational

Specifies a non-default aging-time value for conversational ARP/ND.

Syntax

host-table aging-time conversational *seconds*

no host-table aging-time conversational

Command Default

If conversational ARP/ND is enabled (by entering the **host-table aging-mode conversational** command), the default aging-time value is 300 seconds.

Parameters

seconds

Specifes the aging-time value for conversational ARP/ND. Values range from 60 through 100000 seconds. The default is 300.

Modes

Global configuration mode

Usage Guidelines

You can modify the aging-time value either before or after enabling conversational ARP/ND.

Pre-existing entries age out using the old configured value. A changed age-time configuration applies only entries added following the change.

To restore the default aging-time value of 300 seconds, enter the **no** form of this command.

Examples

The following example sets the aging-time value to 600 seconds and then enables conversational ARP/ND.

```
device# configure terminal
device(config)# host-table aging-time conversational 600
device(config)# host-table aging-mode conversational
```

hostname disable

Disables Intermediate System-to-Intermediate System (IS-IS) name mapping on a device.

Syntax

hostname disable

no hostname disable

Command Default

Disabled.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The implementation of IS-IS supports RFC 2763, which describes a mechanism for mapping IS-IS system IDs to the host names of the devices with those IDs. For example, if you set the host name on the device to "IS-IS Router 1", the mapping capability uses this name instead of the IS-IS system ID of the device in the output of the following commands:

- show isis database
- show isis interface
- show isis neighbor

The **no** form of the command re-enables IS-IS name mapping on a device.

Examples

The following example disables IS-IS name mapping.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# hostname disable
```

The following example re-enables IS-IS name mapping.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no hostname disable
```

http server

Configures HTTP or HTTPS service on a device.

Syntax

http server use-vrf *vrf-name* **shutdown**

no http server use-vrf *vrf-name* **shutdown**

Parameters

use-vrf *vrf-name*

Specifies a user-defined VRF.

shutdown

Disables HTTP or HTTPS service.

Modes

Global configuration mode

Usage Guidelines

Use the **http server** command with the **use-vrf** parameter to enable HTTP or HTTPS service and associate it with the specified VRF. The **use-vrf** parameter configures HTTP or HTTPS service for the specified VRF only. Service for that VRF is enabled or disabled with no effect on service for other VRFs.

Use the **http server** command with the **use-vrf** and **shutdown** parameters to disable HTTP or HTTPS service for the specified VRF.

Use the **no http server** command with the **use-vrf** parameter to disable HTTP or HTTPS service and remove its association with the specified VRF. You can disable service for any VRF, including the management VRF. Disabling service for the management VRF is allowed, but removing the server's association with the management VRF is not allowed.

HTTPS crypto certificates are required to enable HTTPS mode. HTTPS crypto certificates determine whether the service is HTTP or HTTPS.

Examples

The following example creates and enables HTTP or HTTPS service on a device and specifies using a user-defined VRF (myvrf).

```
device# configure terminal
device(config)# http server use-vrf myvrf
```

The following example disables HTTP or HTTPS service (or both HTTP and HTTPS services when both are enabled) on a device for a user-defined VRF.

```
device# configure terminal
device(config)# http server use-vrf myvrf shutdown
```

The following example enables HTTP or HTTPS service on an device for a user-defined VRF when service is disabled.

```
device# configure terminal
device(config)# no http server use-vrf myvrf shutdown
```

The following example disables HTTP or HTTPS service on a device for a user-defined VRF and removes its association with that VRF.

```
device# configure terminal
device(config)# no http server use-vrf myvrf
```

implicit-commit

MPLS allows the user to modify the configurable parameters for RSVP LSPs while the LSP is operational.

Syntax

implicit-commit { **all** | **lsp-reoptimize-timer** }

no implicit-commit

Command Default

The is no implicit commit, by default.

Parameters

all

Enables an implicit commit for all triggers.

lsp-reoptimize-timer

Enables an implicit commit for reoptimizations.

Modes

MPLS policy configuration mode (config-router-mpls-policy)

Usage Guidelines

The **no** form of the command removes the implicit commit.

After modifying the parameters for an operational LSP, the user must execute the **commit** command to apply the changes. Applying these configuration changes requires a new instance of the LSP to be signaled with a modified or new set of parameters, also known as make-before-break. Once the new instance of the LSP is up, the old instance is removed.

By default, if the adaptive parameters of an LSP have changed, but the changes are not yet committed, any system-initiated make-before-break, such as an LSP re-optimization event, is ignored. To allow changes to be automatically applied, the user can use the **implicit-commit lsp-reoptimize-timer** command under the router MPLS policy command to enable certain types of events to trigger implicit commit.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example enable the LSP re-optimize timer to trigger an implicit commit.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# implicit-commit lsp-reoptimize-timer
```

import l2vpn evpn reoriginate

This CLI when configured on DC BL enables import of EVPN Type-5 prefix routes from EVPN VXLAN peers into BGP VPNv4/VPNv6 . The imported prefixes are re-originated as L3VPN NLRI to L3VPN peers.

Syntax

import l2vpn evpn reoriginate

no import l2vpn evpn reoriginate

Modes

Router BGP mode

- Address Family VPNv4 Unicast
- Address Family VPNv6 Unicast

Usage Guidelines

The **no** form of the command disables import of EVPN type-5 prefixes into VPNv4/ VPNV6 and withdraw the prefixes from the L3VPN peers.

Examples

The following example shows how to enable import of BGP type-5 prefixes(IPv6) from EVPN VXLAN peers into BGP VPNv6.

```
device# configure terminal
device(config)# router BGP
device(config-bgp-router)# address-family vpnv6 unicast
device(config-bgp-vpnv6u)# import l2vpn evpn reoriginate
```

import vpnv4 unicast reoriginate

This CLI when configured on DC BL enables import of VPNv4 prefixes from L3VPN peers into BGP EVPN . The imported prefixes are re-originated as EVPN Type-5 prefixes to EVPN VXLAN peers.

Syntax

import vpnv4 unicast reoriginate

no import vpnv4 unicast re-originate

Modes

BGP address-family L2VPN EVPN configuration mode

Usage Guidelines

The **no** form of the command disables import of L3VPN VPNv4 prefixes into EVPN and withdraw the prefixes from EVPN VXLAN peers.

Examples

The following example shows how to enable import of VPNv4 prefixes from L3VPN peers into BGP EVPN.

```
device# configure terminal
device(config)# router BGP
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# import vpnv4 unicast reoriginate
```

import vpnv6 unicast reoriginate

This CLI when configured on DC BL enables import of VPNv6 prefixes from L3VPN peers into BGP EVPN . The imported prefixes are re-originated as EVPN Type-5 prefixes to EVPN VXLAN peers.

Syntax

import vpnv6 unicast reoriginate

no import vpnv6 unicast re-originate

Modes

BGP address-family L2VPN EVPN configuration mode

Usage Guidelines

The **no** form of the command disables import of L3VPN VPNv6 prefixes into EVPN and withdraw the prefixes from EVPN VXLAN peers.

Examples

The following example shows how to enable import of VPNv6 prefixes from L3VPN peers into BGP EVPN.

```
device# configure terminal
device(config)# router BGP
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# import vpnv6 unicast reoriginate
```

import-map

Imports the target-VPN community.

Syntax

import-map *route-map*

no import-map *route-map*

Parameters

route-map

Specifies the route-map name.

Modes

VRF configuration mode

Usage Guidelines

The **no** form of the command removes a route-map filter.

Examples

The following example shows how to import target-VPN community.

```
device# configure terminal
device(config)# vrf vpn1
device(config-vrf-vpn1)# rd 1:2
device(config-vrf-vpn1)# vpn-statistics
device(config-vrf-vpn1)# address-family ipv4 unicast
device(config-vrf-vpn1-ipv4-unicast)# route-target-import 100:1
device(config-vrf-vpn1-ipv4-unicast)# import-map immport-route-map1
```

```
device# configure terminal
device(config)# vrf vpn1
device#(config-vrf-vpn1)# rd 1:2
device#(config-vrf-vpn1)# vpn-statistics
device#(config-vrf-vpn1)# address-familin ipv6 unicast
device#(config-vrf-vpn1-ipv6-unicast)# route-target-import 100:1
device#(config-vrf-vpn1-ipv6-unicast)# import-map immport-route-map1
```

inactivity-timer

Configures the amount of time a forwarding entry can remain unused before the device deletes it.

Syntax

inactivity-timer *seconds*

no inactivity-timer *seconds*

Command Default

The default inactive time is 180 seconds.

Parameters

seconds

Specifies the inactivity period in seconds. Valid values range from 60 through 3600 seconds.

Modes

PIM router configuration mode

Usage Guidelines

A device deletes a forwarding entry if the entry is not used to send multicast packets. The PIM inactivity timer defines how long a forwarding entry can remain unused before the device deletes it.

The **no inactivity-timer** form of this command restores the default inactive time of 180 seconds.

Examples

This example configures an inactive timer of 90 seconds for IPv4 PIM.

```
device# configure terminal
device(config)# router pim
device(config-pim-router)# inactivity-timer 90
```

This example configures an inactive timer of 90 seconds for IPv6 PIM.

```
device# configure terminal
device(config)# ipv6 router pim
device(config-ipv6-router-pim-vrf-default-vrf)# inactivity-timer 90
```

include-all

When a device uses CSPF to calculate the path for an LSP, it takes into account the administrative group to which an interface belongs. The user can specify which administrative groups the device can include or exclude for this calculation.

Syntax

include-all *admin_group_name* | *admin_group_number* [*admin_group_name* |] *admin_group_number*

no include-all *admin_group_name* | *admin_group_number* [*admin_group_name* |] *admin_group_number*

Command Default

No interfaces are assigned to the administrative groups in the default mode.

Parameters

admin_group_name

Specifies the group, by name, the interface must be a member of. The name can be the name of the administrative group to which an administrative group number is associated by configuration in router MPLS mode. More than one parameter can be provided.

admin_group_number

Specifies the group, by number, the interface must be a member of. Number can be from 0 to 31 representing 32 admin groups. More than one parameter can be provided.

Modes

MPLS LSP configuration mode (config-router-mpls-lsp-*lsp_name*).

MPLS router bypass LSP configuration mode (config-router-mpls-bypass-lsp-*lsp_name*)

MPLS router MPLS interface dynamic bypass configuration mode (config-router-mpls-if-ethernet-*slot/port*-dynamic-bypass)

Usage Guidelines

Several administrative groups may be assigned to the LSP at the same time. The interface then must be a member of both groups.

Use the interface level **include-all** command to configure administrative groups for dynamic bypass LSPs to be created corresponding to a protected link.

The **no** form of the command removes the assigned interface.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example specifies that the interface must be a member of both the "*gold* " and "*silver* " administrative groups to included in the path calculations for LSP *tunnel1*.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp tunnel1
device(config-router-mpls-lsp-tunnel1)# include-all gold silver
```

The following example includes administrative groups 4, 5, and 6.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# bypass-lsp by-bypass-lsp
device(config-router-mpls-bypass-lsp-by-bypass-lsp)# include-all 4 5 6
```

The following example includes administrative groups 4 and 5 on MPLS Ethernet interface 0/8.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/8
device(config-router-mpls-if-ethernet-0/8)# dynamic-bypass
device(config-router-mpls-if-ethernet-0/8-dynamic-bypass)# include-all 4 5
```

include-any

When a device uses CSPF to calculate the path for an LSP, it takes into account the administrative group to which an interface belongs. The user can specify which administrative groups the device can include or exclude for this calculation.

Syntax

include-any *admin_group_name* | *admin_group_name*[*admin_group_number* | *admin_group_numbe*]

no include-any *admin_group_name* | *admin_group_name*[*admin_group_number* | *admin_group_numbe*]

Command Default

No interfaces are assigned to the administrative groups in the default mode.

Parameters

admin_group_name

Specifies the group, by name, the interface must be a member of. The name can be the name of the administrative group to which an administrative group number is associated by configuration in router MPLS mode. More than one parameter can be provided.

admin_group_number

Specifies the group, by number, the interface must be a member of. Number can be from 0 to 31 representing 32 admin groups. More than one parameter can be provided.

Modes

MPLS LSP configuration mode (config-router-mpls-lsp-*lsp_name*)

MPLS router Bypass LSP configuration mode (config-router-mpls-bypass-lsp-*lsp_name*)

MPLS router MPLS interface dynamic bypass configuration mode (config-router-mpls-if-ethernet--dynamic-bypass)

Usage Guidelines

The **no** form of the command removes the assigned interface.

Use the interface level **include-any** command to configure administrative groups for dynamic bypass LSPs to be created corresponding to a protected link.

Several administrative groups may be assigned to the LSP at the same time.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures LSP *tunnel1* path calculations in either of the administrative groups "*gold* " or "*silver* ".

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp tunnel1
device(config-router-mpls-lsp-tunnel1)# include-any gold silver
```

The following example includes any group designated as group 8 and 9.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# bypass-lsp my-bypass-lsp
device(config-router-mpls-bypass-lsp-my-bypass-lsp)#  include-any  8 9
```

The following example includes any group designated as group 6 and 7 on dynamic bypass MPLS Ethernet interface *0/8*.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/8
device(config-router-mpls-if-ethernet-0/8)# dynamic-bypass
device(config-router-mpls-if-ethernet-0/8-dynamic-bypass)# include-any 6 7
```

ingress-tunnel-accounting

Excludes the Ethernet header (14 bytes) and Ethernet overhead (20 bytes) and CRC overhead (four bytes) when collecting byte statistics. In other words, it counts only the size of the MPLS packet.

Syntax

ingress-tunnel-accounting

no ingress-tunnel-accounting

Command Default

The command is disabled, by default.

Modes

MPLS policy configuration mode.

Usage Guidelines

To collect accurate statistics of the bypass LSP, it is necessary to configure ingress tunnel accounting at Label Switch Routers (LSR).

The **no** form of the command disables the configuration.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The example below is a sample configuration for the command.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy) ingress-tunnel-accounting
```

ingress-vlan-mapped-ve-counter

Enables displaying Layer 3 ingress statistics.

Syntax

ingress-vlan-mapped-ve-counter

no ingress-vlan-mapped-ve-counter

Parameters

None

Modes

Global Configuration mode

Usage Guidelines

This feature is only supported on SLX 9540 and SLX 9640 devices.

The Hardware Profile *counter-profile-6* must be enabled. When not enabled, and when this command is executed, a reminder message is displayed.

The following must be kept in mind when enabling display of Layer 3 ingress statistics:

- Ingress statistics will only be displayed where there is a one-to-one mapping between a port and a VLAN.
- If the above criteria is not met, the ingress counter will always display the value Zero (0).
- If the interface is a Port-Channel, only one Port-Channel must be associated with a VLAN.
- Ingress statistics will not be displayed for Bridge Domains.

Examples

This example shows how to enable ingress VE counters.

```
SLX # configure terminal
SLX (config) # ingress-vlan-mapped-ve-counter
SLX (config) #
```

This example disables ingress VE counters.

```
SLX # configure terminal
SLX (config) # no ingress-vlan-mapped-ve-counter
SLX (config) #
```

init-route-calc-delay

Enables BGP delayed route calculation in specific scenarios: router reload, BGP process restart, and admin reset of all the BGP peers in a VRF/SAFI using the **clear ip | ipv6 bgp neighbor all** command. BGP BEST-path selection is delayed until BGP has the route update information from all of its RIB-IN peers.

Syntax

init-route-calc-delay [**min-delay** *min_secs*| **max-delay** *max_secs* | **msg-idle-time** *idle_secs*]

no init-route-calc-delay [**min-delay** | **max-delay** | **msg-idle-time**]

Command Default

By default, BGP delayed route calculation is disabled.

Parameters

min-delay *min_secs*

Specifies the minimum delay time in seconds by which the BGP BEST-path selection is delayed. Enter an integer from 60 to 900. When the delay route calculation is enabled, the default is 180 seconds.

max-delay *max_secs*

Specifies the maximum delay time in seconds by which the BGP BEST-path selection is delayed. Enter an integer from 180 to 900. When the delay route calculation is enabled, the default is 300 seconds.

msg-idle-time *idle_secs*

Specifies the message idle time in seconds to detect the end of the learning phase for a peer. A peer is moved out of the learning phase if the time difference between subsequent update messages from the peer exceeds the message idle time. Enter an integer from 1 to 60. When the delay route calculation is enabled, the default is 2 seconds.

Modes

BGP configuration mode

Usage Guidelines

Use the **no init-route-calc-delay** command to disable the delay route calculation. When an optional keyword is include with the **no** form of this command, it resets the default setting for the keyword.

If you enter the **init-route-calc-delay** command without any options, the default settings for the minimum and maximum delay and message idle time are used.

TCP is the underlying transport mechanism used by BGP for propagating BGP update messages. Optimal usage of TCP directly helps in improving BGP performance and convergence. Configuring higher IP MTU values (4500 bytes) for the interfaces through which BGP peer IP connectivity is established helps to select optimal MSS size for BGP TCP sessions.

Examples

The following example enables the BGP delay route calculation.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# init-route-calc-delay
```

The following example configures the minimum delay time to 200 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# init-route-calc-delay min-delay 200
```

insight enable

Configures a port-channel as an insight interface.

Syntax

insight enable

no insight enable

Command Default

Insight is not enabled on the port-channel.

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **no** form of this command to disable an insight interface on the port-channel.

The connector must be enabled to support the insight interface, by means of the **insight mode** command.

Examples

This example enables an insight interface on a connector.

```
device# configure terminal
device(config)# hardware
device(config-hardware)#
device(config-hardware)# connector 0/48
device(config-connector-0/48)# insight mode
```

This example uses the **insight enable** command to enable an insight interface on a port-channel.

```
device# configure terminal
device(config)# interface port-channel 33
device(config-Port-channel-33)# insight enable
no shutdown
```

This example uses the **show interface port-channel** and **show port-channel** commands to confirm the configuration.

```
device# show interface port-channel 33
Port-channel 22 is up, line protocol is up
Hardware is AGGREGATE, address is 609c.9f5a.4558
    Current address is 609c.9f5a.4558
Interface index (ifindex) is 671088673
Minimum number of links to bring Port-channel up is 1
MTU 1548 bytes
```

```
LineSpeed Actual     : 10000 Mbit
Allowed Member Speed : 10000 Mbit
Priority Tag disable
Forward LACP PDU: Disable
Route Only: Disabled
Last clearing of show interface counters: 1d23h53m
Queueing strategy: fifo
Receive Statistics:
    0 packets, 0 bytes
    Unicasts: 0, Multicasts: 0, Broadcasts: 0
    64-byte pkts: 0, Over 64-byte pkts: 0, Over 127-byte pkts: 0
    Over 255-byte pkts: 0, Over 511-byte pkts: 0, Over 1023-byte pkts: 0
    Over 1518-byte pkts(Jumbo): 0
    Runts: 0, Jabbers: 0, CRC: 0, Overruns: 0
    Errors: 0, Discards: 0
Transmit Statistics:
    5 packets, 380 bytes
    Unicasts: 0, Multicasts: 5, Broadcasts: 0
    Underruns: 0
    Errors: 0, Discards: 0
Rate info:
    Input 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
    Output 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Route-Only Packets Dropped: 0
Time since last interface status change: 00:00:21

device# show port-channel 22
Static Aggregator: Po 22
 Aggregator type: Standard
 Number of Ports: 1
 Member ports:
   Eth 0/125   *
```

insight mode

Enables an insight interface on connector.

Syntax

insight mode

no insight mode

Command Default

By default, the connector is initialized as a regular user port. Insight mode is not enabled by default.

Modes

Hardware configuration mode for a connector

Usage Guidelines

This command enable an insight interface for a port-channel.

The insight functionality supports TPVM. To enable it, a pre-designated connector needs to be configured as insight mode before enabling the insight interface (0/125) for a port-channel. The insight mode conversion is dynamic, therefore no switch reboot is required.

When the connector is configured as insight mode, the original Ethernet user interface is deconfigured and deleted, and the insight interface 0/125 is created automatically.

Use the **no** form of this command to disable the insight interface and convert the connector to a regular port.

Examples

This example enables insight mode on connector 0/48 of SLX9540.

```
device(config)# hardware
device(config-hardware)#
device(config-hardware)# connector 0/48
device(config-connector-0/48)# insight mode
```

This example uses the **insight enable** command to enable an insight interface on a port-channel. The insight interface 0/125 is then added to this port-channel.

```
device# configure terminal
device(config)# interface port-channel 33
device(config-Port-channel-33)# insight enable
device(config-Port-channel-33)# no shutdown
```

install-igp-cost

Configures the device to use the IGP cost instead of the default BGP Multi-Exit Discriminator (MED) value as the route cost when the route is added to the Routing Table Manager (RTM).

Syntax

install-igp-cost

no install-igp-cost

Modes

BGP configuration mode

Usage Guidelines

By default, BGP uses the BGP MED value as the route cost when the route is added to the RTM. Use this command to change the default to the IGP cost.

The **no** form of the command restores the defaults.

Examples

The following example configures the device to compare MEDs.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# install-igp-cost
```

instance

Maps a VLAN to a Multiple Spanning Tree Protocol (MSTP) instance. You can group a set of VLANs to an instance.

Syntax

instance *instance_id* [**vlan** *vlan_id* | **priority** *priority_id*]

no instance

Command Default

The priority value is 32768.

Parameters

instance_id

Specifies the MSTP instance. Valid values range from 1 through 31.

vlan *vlan_id*

Specifies the VLAN to map an MSTP instance. Refer to the Usage Guidelines.

priority *priority_id*

Specifies the priority for the specified instance. Valid values range from 0 through 61440. The priority values can be set only in increments of 4096.

Modes

Spanning tree MSTP configuration mode

Usage Guidelines

The following rules apply:

- VLANs must be created before mapping to instances.
- The VLAN instance mapping is removed from the configuration if the underlying VLANs are deleted.

Enter **no instance** to remove the VLAN mapping from the MSTP instance.

Caution

This command can be used only after the VLAN is defined.

Examples

To map a VLAN to an MTSP instance:

```
device# configure terminal
device(config)# protocol spanning-tree mstp
```

```
device(conf-mstp)# instance 1 vlan 2,3
device(conf-mstp)# instance 2 vlan 4-6
device(conf-mstp)# instance 1 priority 4096
```

interface ethernet

Configures an Ethernet interface.

Syntax

interface ethernet slot/port

no interface ethernet

Command Default

No Ethernet interface is configured.

Parameters

slot/port

Specifies an interface name in slot/port format. Separate multiple ports with a comma. Use a hyphen (-) to indicate a range of ports. For example, 0/1-3,5,7-9 or 0/49:1-2,4. The maximum number of characters is 253.

Modes

Global configuration mode

Usage Guidelines

All interfaces in a range must use the same speed.

If the **breakout mode** command has been configured on the port, the breakout ports of the Ethernet interface appear after the slot and port as breakout ports 1 through 4. For example, the breakout interfaces of connector 0/25 have the following naming convention:

```
interface ethernet 0/25:1
interface ethernet 0/25:2
interface ethernet 0/25:3
interface ethernet 0/25:4
```

To configure Redundant Management, configure a physical port on the device (for example, 0/15) as a standby management port.

Examples

The following example configures breakout ports of Ethernet interface 0/1:

```
device# configure terminal
device(config)# interface ethernet 0/1:1
device(config)# interface ethernet 0/1:2
device(config)# interface ethernet 0/1:3
device(config)# interface ethernet 0/1:4
```

The following example configures port 0/15 as the redundant management port:

```
device# configure terminal
device(config)# interface ethernet 0/15
device(conf-if-eth-0/15)# redundant-management enable
```

The following example configures a range of ports:

```
device# configure terminal
device(config)# interface ethernet 0/1-2,4,6-7
device(config-if-eth-0/1-2,4,6-7)#
```

interface loopback

Configures a loopback interface.

Syntax

interface loopback *port_number*

no interface loopback *port_number*

Command Default

A loopback interface is not configured.

Parameters

port_number

Specifies the port number for the loopback interface. Range is 1 through 255.

Modes

Global configuration mode

Usage Guidelines

A loopback is a logical interface traditionally used to ensure stable routing operations.

Use the no form of this command to remove the specified loopback interface.

The following restrictions apply when the loopback interface is part of an active VXLAN overlay gateway. These restrictions are enforced to maintain consistency across the gateway.

- The loopback interface cannot be deleted.
- The IPv4 address cannot be changed.
- The VRF instance cannot be changed.

You must first use the **no activate** command in VXLAN overlay gateway configuration mode to modify the loopback interfaces. .

Use the **no** form of this command with a port parameter to remove the specified loopback interface.

Examples

The following example creates a loopback interface with a port number of 25.

```
device# configure terminal
device(config)# interface loopback 25
device(config-Loopback-25)#
```

interface management

Accesses management configuration mode.

Syntax

interface management *mgmt-id*

Parameters

mgmt-id

Specifies the management ID. The only supported value is **0**.

Modes

Global configuration mode

Usage Guidelines

The mode allows you to configure the management interface.

Examples

The following example accesses management mode.

```
device# configure terminal
device(config)# interface management 0
device(config-Management-0)#
```

interface port-channel

Creates and configures a port-channel interface.

Syntax

interface port-channel *number*

no interface port-channel *number*

Command Default

No port-channel interface is configured.

Parameters

number

Specifies a port-channel.

Modes

Global configuration mode

Usage Guidelines

Use the no form of this command to disable the interface.

Port channel scale and support for SLX 9740/Extreme 8820 devices:

Table 10: Port-channel scale for SLX 9740/Extreme 8820 devices.

Device	LAG Profile	Supported port-channel IDs	Maximum links per port-channel
SLX 9740-40/ Extreme 8820-40	default	1-256; Only 77 port-channels may be created at one time.	64
SLX 9740-80/ Extreme 8820-80	default	1-256; Only 153 port-channels may be created at one time.	64

Note

- For the 1U SLX 9740-40/Extreme 8820-40 devices, the number of LAGs will be 77, where:
  - 76 are the front end ports (all breakouts)
  - 1 (insight port)
- For the 2U SLX 9740-80/Extreme 8820-80 devices, the number of LAGs will be 153. where:
  - 152 are the front end ports (all breakouts)
  - 1 (insight port)

(SLX 9540 and SLX 9640) Maximum numbers of port-channel IDs and links per port-channel vary with device and LAG profile, as follows:

Table 11: Port-channel scale for SLX 9540 and SLX 9640 devices

Device or series	LAG profile	Supported port-channel IDs	Maximum links per port-channel
SLX 9540 and SLX 9640	default	1–256; Only 64 port-channels may be created at any one time.	64
SLX 9540 and SLX 9640	lag-profile-1	1–256; Only 64 port-channels may be created at any one time.	32

(SLX 9150, SLX 9250, Extreme 8520, and Extreme 8720) Maximum numbers of port-channel IDs and links per port-channel vary only with device, as follows:

Table 12: Port-channel support for SLX 9150, SLX 9250, Extreme 8520, and Extreme 8720 devices

Device or series	Supported port-channel IDs	Maximum links per port-channel
SLX 9150, SLX 9250, Extreme 8520, and Extreme 8720	1–256; Only 128 port-channels may be created at any one time.	64

Note
Non-default LAG profiles are not supported for the SLX 9150 and SLX 9250 devices.

Examples

To configure a port-channel interface:

```
device# configure terminal
device(config)# interface port-channel 10
device(config-Port-channel-10)#
```

interface (telemetry)

Specifies monitored interfaces for the interface telemetry profile-type.

Syntax

interface *interface*

no interface *interface*

Command Default

No interfaces are defined and the profile is inactive.

Parameters

interfaces

Specifies the profile interfaces, up to 1000 characters. The format options are:

- *slot*/*port*, for example, `0/1`
- *slot*/*port1*-*port2*, for example, `0/1-5`
- *slot*/*port1*:*breakout1*-*breakout2*, for example, `0/4:3-4`

Modes

Telemetry profile configuration mode

Usage Guidelines

If you do not specify at least one interface, the profile has no effect.

For other telemetry profiles that require you to configure interfaces, the syntax of this command is **interface-range**.

To remove interfaces from the interface profile, use the **no** form of this command.

Examples

The following example configures the interfaces to be used in the interface streaming profile.

```
device# configure terminal
device(config)# telemetry profile interface default_interface_statistics
device(config-interface-default_interface_statistics)# interface 1/2-3,2/1-3,3/6-9
```

interface management

Configures the out-of-band BMC Management Interfaces. Each out-of-band BMC interface has its own configuration mode and must be individually configured.

Syntax

interface management *interface-number*

no interface management *interface-number*

Parameters

interface-number

The unique interface ID for the out-of-band BMC management interfaces. Only interface with ID 0 (zero) can be configured. Using other values will throw an error.

Modes

Enters into the BMC Management Interface Configuration mode.

Usage Guidelines

Only interface 0 (zero) is configurable. Other interfaces are not supported yet.

The out-of-band BMC Management Interface's IP can be configured from this mode.

The out-of-band BMC Management Interface can be shutdown from this mode.

Use the **no** format of this command to make this interface inaccessible from outside of the device physical ports.

Examples

This example shows how to enter into the BMC Management Interface Configuration mode.

```
SLX # configure terminal
SLX (config)# bmc
SLX (config-bmc)# interface management 0
SLX (config-bmc-mgmt-0)# ?
Possible completions:
  describe   Display transparent command information
  do         Run an operational-mode command
  exit       Exit from current mode
  help       Provide help information
  ip         IPv4 address of this interface
  no         Negate a command or set its defaults
  pwd        Display current mode path
  shutdown   Enable or disable the interface
  top        Exit to top level and optionally run command
```

```
SLX (config-bmc-mgmt-0)#
```

This example disables this interface from being accessible from out of band locations.

```
SLX # configure terminal
SLX (config)# bmc
SLX (config-bmc)# do show running-config bmc
bmc
 user-id 1
  password $9$VaXhc9WCy+1IwRU2ZaS2vQ==
 !
 user-id 2
  password $9$VaXhc9WCy+1IwRU2ZaS2vQ==
 !
 user-id 3
 !
 interface management 0
  shutdown
 !
!
SLX (config-bmc)# no interface management 0
SLX (config-bmc)# do show running-config bmc
bmc
 user-id 1
  password $9$VaXhc9WCy+1IwRU2ZaS2vQ==
 !
 user-id 2
  password $9$VaXhc9WCy+1IwRU2ZaS2vQ==
 !
 user-id 3
 !
!
```

interface ve

Configures a virtual Ethernet (VE) interface.

Syntax

interface ve *vlan_id*

no interface ve *vlan_id*

Parameters

vlan_id

Specifies the corresponding VLAN that must already be created before the VE interface can be created. Refer to the Usage Guidelines. Separate multiple IDs with a comma. Use a hyphen (-) to indicate a range of IDs. For example, 1-3,5,7-9.

Modes

Global configuration mode

Usage Guidelines

Before you can configure a VE interface, you must create a corresponding VLAN. The VE interface must use the corresponding VLAN ID.

All interfaces in a range must use the same speed.

Use the **no** form of this command to remove a specified VE interface.

Examples

This example creates a VE interface with the VLAN ID of 56. This example assumes that VLAN 56 has already been created.

```
device# configure terminal
device(config)# interface ve 56
device(config-Ve-56)#
```

This example creates multiple VE interfaces.

```
device# configure terminal
device(config)# interface ve 1-3,5,7-9
device(config-Ve-1-3,5,7-9)#
```

This example removes a VE interface.

```
device# configure terminal
device(config)# no interface ve 5
device#
```

interval

For an implementation of an event-handler profile, specifies the number of seconds between iterations of an event-handler action, if triggered.

Syntax

interval *seconds*

no interval

Command Default

Iterations occur with no interval between them.

Parameters

seconds

Specifies the number of seconds between iterations of an event-handler action, if triggered. Valid values are 0 or a positive integer.

Modes

Event-handler activation mode

Usage Guidelines

The **interval** command is effective only if the **iterations** value is non-zero.

The **no** form of this command resets the **interval** setting to the default 0 seconds.

Examples

The following example sets the number of iterations to 3 and specifies an interval of 10 seconds between each iteration.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# iterations 3
device(config-activate-eventHandler1)# interval 10
```

The following example resets **interval** to the default value of 0 seconds.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# no interval
```

interval (telemetry)

Configures the interval delay for telemetry data streaming.

Syntax

interval *seconds*

no interval

Command Default

For the interface profile-type, the default value is 30 seconds.

For the system-utilization profile-type, the default value is 60 seconds.

For the MPLS profile-types, the default value is 240 seconds. (These profile types are supported only on SLX 9540 and SLX 9640 devices.)

For the queue profile-types, the default value is 300 seconds. (These profile types are supported only on SLX 9540 and SLX 9640 devices.)

Parameters

seconds

(SLX 9150 and SLX 9250 devices) Specifies the streaming interval. For the interface profile-type, values range from 10 through 3600 seconds, in five-second increments. For the system-utilization profile-type, values range from 60 through 14400 seconds, in five-second increments.

(SLX 9540 and SLX 9640 devices) Specifies the streaming interval. The range of values, in five-second increments:

- For the interface profile-type, from 10 through 3600 seconds.
- For the system-utilization profile-type, from 60 through 14400 seconds.
- For the MPLS profile-types, from 240 through 3600 seconds.
- For the queue profile-types, from 240 through 2400 seconds.

Modes

Telemetry profile configuration mode

Usage Guidelines

To reset the interval to the default value, use the **no interval** command.

Examples

Example of setting the interval in an interface configuration for an interface profile.

```
device# configure terminal
device(config)# telemetry profile interface default_interface_statistics
device(interface-default_interface_statistics)# interval 2000
```

Example of setting the interval for a MPLS Traffic statistics data streaming configuration using the mpls-traffic-lsp profile.

```
device# configure
device(config)# telemetry profile mpls-traffic-lsp default_mpls_traffic_lsp_statistics
device(config-telemetry-profile)# interval 340
```

ip access-group

Applies rules specified in an IPv4 access control list (ACL) to traffic entering or exiting an interface.

Syntax

ip access-group *ACLname* { **in** [**routed**]| **out** }

no ip access-group *ACLname* { **in** | **out** }

Parameters

ACLname

Specifies the name of the standard or extended IPv4 access list.

in

Applies the ACL to incoming switched and routed traffic.

out

Applies the ACL to outgoing routed and (for SLX 9150 and SLX 9250 devices) also to switched traffic.

routed

Optional Parameter. Applies only to an ingress ACL. This parameter is only supported when ACL is applied to inbound traffic on a Layer 3 sub-interface such as the VE interface.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to apply an IPv4 ACL to one of the following interface types:

- User interfaces
  - Physical Ethernet interfaces
  - Port-channels (LAGs).
  - Virtual Ethernet (VE) (attached to a VLAN or to a bridge domain)
- The management interface

You can apply a maximum of five ACLs to a user interface, as follows:

- One ingress MAC ACL—if the interface is in switchport mode
- One egress MAC ACL—if the interface is in switchport mode
- One ingress IPv4 ACL
- One egress IPv4 ACL
- One ingress IPv6 ACL

You can apply a maximum of two ACLs to the management interface, as follows:

- One ingress IPv4 ACL
- One ingress IPv6 ACL

You can apply an ACL to multiple interfaces. And you can apply an ACL twice—ingress and egress—to a given user interface.

To remove an ACL from an interface, enter the **no** form of this command.

The *routed* parameter can only be applied for *ingress* ACLs applied to a VE interface. This option is not available on other interfaces.

You cannot modify an existing ingress ACL definition to include the *routed* parameter. An error is displayed.

The `no` format of the command cannot be used to remove the *routed* parameter from the ACL. You must delete the entire ACL configuration and re-configure to change the ACL.

Examples

The following example applies an ingress IP ACL on an Ethernet interface:

```
SLX (config)# interface ethernet 0/2
SLX (conf-if-eth-0/9)# ip access-group ipacl2 in
```

The following example removes an ingress IP ACL from an Ethernet interface:

```
SLX (config)# interface ethernet 0/2
SLX (conf-if-eth-0/9)# no ip access-group ipacl2 in
```

This example shows the configuration of the *routed* parameter on an ingress ACL on a VE.

```
SLX (config)# interface ve 10
SLX (config-if-ve-10)# ip access-group ipacl2 in routed
SLX (config-if-ve-10)# do show run interface ve 10
    interface Ve 10
    ip access-group ipacl2 in routed
SLX (config-if-ve-10)#
```

ip access-list

Creates a standard or extended IPv4 access control list (ACL). In ACLs, you can define rules that permit or deny network traffic based on criteria that you specify.

Syntax

ip access-list { **standard** | **extended** } *ACLname*

no ip access-list { **standard** | **extended** } *ACLname*

Parameters

standard | **extended**

Specifies one of the following types of access lists:
standard

Contains rules that permit or deny traffic based on source addresses that you specify. The rules are applicable to all ports of the specified addresses.

extended

Contains rules that permit or deny traffic according to source and destination addresses, as well as other parameters. For example, you can also filter by port, protocol (TCP or UDP), and TCP flags.

ACLname

Specifies an ACL name unique among all ACLs (Layer 2 and Layer 3). The name can be up to 63 characters in length, and must begin with an alphanumeric character. No special characters are allowed, except for the underscore and hyphen.

Modes

Global configuration mode

Usage Guidelines

An ACL name can be up to 63 characters long, and must begin with a–z, A–Z or 0–9. You can also use underscore (_) or hyphen (-) in an ACL name, but not as the first character.

After you create an ACL, use the **seq** command to create filtering rules for that ACL.

An ACL starts functioning only after:

- Applied to an interface, using the **{ ip | ipv6 | mac } access-group** command.
- Applied at device-level, using the **{ ip | ipv6 } receive access-group** command.

To delete an ACL, use the **no access-list** command. You can delete an ACL only after you first remove it from all interfaces to which it is applied, using the **no access-group** command.

Examples

The following example creates an IPv4 standard ACL.

```
device# configure
device(config)# ip access-list standard stdACL3
```

The following example creates an IPv4 extended ACL.

```
device# configure terminal
device(config)# ip access-list extended extdACL5
```

The following example creates rules on an IPv4 standard ACL.

```
device# configure terminal
device(config)# ip access-list standard stdACL3
device(config-ipacl-std)# seq 5 permit host 10.20.33.4
device(config-ipacl-std)# seq 15 deny any
```

The following example deletes an IPv4 ACL.

```
device# configure
device(config)# no ip access-list standard stdACL3
```

The following example creates an IPv4 extended ACL and adds rules to the ACL that filter TCP packets to the management IP on port 22.

```
device# configure
device(config)# ip access-list extended management
device(config-ipacl-ext)# permit tcp x.x.x.x/24 mgt-ip eq 22
device(config-ipacl-ext)# permit tcp x.x.x.x/24 mgt-ip eq 22
device(config-ipacl-ext)# permit tcp host x.x.x.x mgt-ip eq 22
device(config-ipacl-ext)# permit tcp host x.x.x.x mgt-ip eq 22
device(config-ipacl-ext)# permit tcp host x.x.x.x mgt-ip eq 22
deny tcp any mgt-ip eq 22
```

The following example displays an ACL definition that supports flow based ingress miroring.

```
device# show access-list int eth 0/2 in
ip access-list ipl on Ethernet 0/2 at Ingress (From User)
    seq 10 permit ip host 10.10.10.1 any count mirror (Active)
    seq 20 permit tcp any host 15.15.15.1 count (Active)
```

The following example displays an ACL definition that supports flow based ingress miroring.

```
device# show access-list int eth 0/2 in
ip access-list ipl on Ethernet 0/2 at Ingress (From User)
    seq 10 permit ip host 10.10.10.1 any count mirror (150 frames)
    seq 20 permit tcp any host 15.15.15.1 count (0 frames)
```

ip address

Configures a primary or secondary IP address on an interface.

Syntax

ip address *ip-address/mask* [**secondary**][**ospf-ignore**][**ospf-passive**]

no ip address [*ip-address/mask*]

Parameters

ip-address

Specifies the IP address.

mask

Specifies the mask for the associated IP subnet. Dotted-decimal notation is not supported. For non-loopback interfaces, valid values are from 1 through 31. For loopback interfaces, the only valid value is 32.

secondary

Specifies that the address is a secondary IP address.

ospf-ignore

Disables adjacency formation with OSPF neighbors and disables advertisement of the interface to OSPF.

ospf-passive

Disables adjacency formation with OSPF neighbors but does not disable advertisement of the interface to OSPF.

Modes

Interface configuration mode

Management interface configuration mode

Port-channel configuration mode

Usage Guidelines

- Use this command to configure a primary or secondary IP address for an interface. You can also use this command to prevent OSPF from running on specified subnets. Multiple primary IP addresses are supported on an interface.
- You can use this command to configure a primary or secondary IP address for the management interface.
- For the management interface, only one primary IP address is supported.
- A primary IP address cannot overlap a configured IP subnet.
- A primary IP address must be configured before you configure a secondary IP address in the same subnet.

- To remove the configured static or DHCP address, enter **no ip address**. This resets the address to 0.0.0.0/0.
- The **no** form of the command removes a specific IP address from the interface.

Gateway IPs from multiple subnets (maximum of 32) can be configured for each FVG session. Multiple gateway IPs from the same subnet can be configured, but the number of FVG sessions for each interface remains one. One RBridge becomes the ARP responder for all the gateway IPs configured for the session.

Multiple gateway IPs are supported only for IPv4.

All restrictions for configuring an FVG gateway also apply to multiple gateway IP addresses. If IP conflicts are detected for any gateway IP configured on the session, the configuration is accepted with a RASLOG, but the session is invalidated until the conflict is resolved.

Periodic gratuitous address resolution protocol (GARP), if configured, would be sent out only for the first gateway address. When a session moves to Master, GARP is sent out for all gateway IP addresses configured on the session.

After a downgrade to an earlier version of the OS, all gateway IP configurations are removed if multiple gateway IPs are present. If only one gateway IP present, then the configuration is retained.

Examples

The following example configures a primary IP address on a specified Ethernet interface.

```
device(config)# interface ethernet 3/2
device(conf-if-eth-3/2)# ip address 10.1.1.1/24
```

```
device(config)# interface ethernet 3/2
device(conf-if-eth-3/2)# ip address 10.1.1.2/24 secondary
```

The following example configures a primary IP address on a management interface.

```
device(config)# interface Management 0
device(config-Management-0)# no ip address
device(config-Management-0)# ip address 10.1.1.2/24
```

ip address (site)

Specifies the destination IPv4 address of a tunnel for a site in a VXLAN overlay gateway configuration.

Syntax

ip address *IPv4_address*

no ip address [*IPv4_address*]

Parameters

IPv4_address

Specifies the IPv4 address of the destination tunnel.

Modes

Site configuration mode

Usage Guidelines

The tunnel mode and the source IP address are derived from the parent overlay gateway.

To change an IP addresses, you must first remove the existing address, by means of the **no ip address** *IPv4_address* or the **no ip address** commands. This also deletes all tunnels to the site.

Only one IPv4 address is allowed. The following IPv4 addresses are not allowed:

- Broadcast addresses (0.0.0.0 through 0.255.255.255)
- Localhost loopback addresses (127.0.0.0 through 127.255.255.255)
- Multicast addresses (224.0.0.0 through 239.255.255.255)
- Reserved addresses (240.0.0.0 through 255.255.,255.255)

Examples

The following example configures an IPv4 address of a destination tunnel for the site.

```
device# configure terminal
device(config)# overlay-gateway gateway1
device(config-overlay-gw-gateway1)# site mysite
device(config-site-mysite)# ip address 10.11.12.13
```

ip anycast-address

Configures an anycast-gateway IPv4 address on an interface, which uses the gateway IPv4 address for the host.

Syntax

ip anycast-address *IPv4-address/mask*

no ip anycast-address

Command Default

No address is configured.

Parameters

IPv4-address/mask

IPv4 address and mask.

Modes

Interface configuration mode on a virtual Ethernet (VE) interface.

Usage Guidelines

Use the **no** form of this command to delete the configured IPv4 anycast address from the interface.

Examples

To configure an IPv4 address and mask on a virtual Ethernet (VE) interface:

```
device# configure terminal
device(config)# interface ve 10
device(config-Ve-10)# ip anycast-address 2.2.2.2/24
```

To confirm the configuration in the running configuration:

```
device# show running-config interface ve 10
!
ip snycast-address 2.2.2.2/24
!
```

ip arp gratuitous none

Disables the gratuitous ARP (Address Resolution Protocol) control.

Syntax

ip arp gratuitous none

no ip arp gratuitous none

Command Default

By default, the gratuitous ARP control is enabled.

Modes

Global configuration mode

Usage Guidelines

Use the no form of the command to re-enable the gratuitous ARP control.

Examples

The following example disables the gratuitous ARP control.

```
device# configure terminal
device(config)# ip arp gratuitous none
```

ip arp inspection

Enables Dynamic ARP Inspection (DAI) on a VLAN.

Syntax

ip arp inspection

no ip arp inspection

Command Default

DAI is disabled.

Modes

VLAN configuration mode

Usage Guidelines

On untrusted interfaces of DAI-enabled VLANs, incoming ARP packets from permitted IP/MAC addresses are accepted only if all of the following steps were performed:

- Create the ACL, using the **arp access-list** command.
- In the ACL, create one or more rules, using the **permit ip host** command. Each rule specifies an IP/MAC address-pair.
- Apply the ACL to one or more VLANs, using the **ip arp inspection filter** command.
- Enable DAI on such VLANs, using the **ip arp inspection** command.

The **no** form of the command disables Dynamic ARP Inspection.

Examples

The following example creates an ARP access-list, applies it to VLAN 200, and enables DAI.

```
device# configure terminal
device(config)# arp access-list ARP_ACL_01
device(config-arp-acl)# permit ip host 1.1.1.1 mac host 0020.2222.2222
device(config-arp-acl)# permit ip host 1.1.1.2 mac host 0020.2222.2223
device(config-arp-acl)# exit
device(config)# vlan 200
device(conf-vlan-200)# ip arp inspection filter ARP_ACL_01
device(conf-vlan-200)# ip arp inspection
```

ip arp inspection filter

Applies an Address Resolution Protocol (ARP) ACL to a VLAN, which is one of the steps implementing Dynamic ARP Inspection (DAI) on a VLAN.

Syntax

ip arp inspection filter *ACL-name*

no ip arp inspection filter

Command Default

No ARP ACL is applied.

Parameters

ACL-name

Specifies which ACL is applied to the VLAN or interface.

Modes

VLAN configuration mode

Interface subtype configuration mode

Usage Guidelines

On untrusted interfaces of DAI-enabled VLANs, incoming ARP packets from permitted IP/MAC addresses are accepted only if all of the following steps were performed:

- Create the ACL, using the **arp access-list** command.
- In the ACL, create one or more rules, using the **permit ip host** command. Each rule specifies an IP/MAC address-pair.
- Apply the ACL to one or more VLANs, using the **ip arp inspection filter** command.
- Enable DAI on such VLANs, using the **ip arp inspection** command.

For ARP Guard, this command applies an ARP ACL to a physical or port-channel interface.

The **no** form of the command removes the current ARP ACL from the VLAN or interface.

Examples

The following example applies an ARP ACL named ARP_ACL_01 to VLAN 200.

```
device# configure terminal
device(conf)# vlan 200
device(conf-vlan-200)# ip arp inspection filter ARP_ACL_01
```

ip arp inspection trust

Configures an interface as trusted for all VLANs configured on it.

Syntax

ip arp inspection trust

no ip arp inspection trust

Command Default

The interface is untrusted.

Modes

Interface subtype configuration mode

Usage Guidelines

This command is supported only on Layer 2 physical or port-channel interfaces.

On trusted interfaces, all incoming ARP packets are accepted.

On untrusted interfaces of DAI-enabled VLANs, incoming ARP packets from permitted IP/MAC addresses are accepted only if all of the following steps were performed:

- Create the ACL, using the **arp access-list** command.
- In the ACL, create one or more rules, using the **permit ip host** command. Each rule specifies an IP/MAC address-pair.
- Apply the ACL to one or more VLANs, using the **ip arp inspection filter** command.
- Enable DAI on such VLANs, using the **ip arp inspection** command.

The no form of this command configures the interface as untrusted.

Examples

The following example configures an Ethernet interface as trusted.

```
device# configure terminal
device(conf)# interface ethernet 2/1
device(conf-if-eth-2/1)# ip arp inspection trust
```

The following example configures a port-channel interface as untrusted.

```
device# configure terminal
device(conf)# interface port-channel 171
device(config-Port-channel-171)# no ip arp inspection trust
```

ip arp learn-any

Enables address-resolution protocol (ARP) learning from any ARP request.

Syntax

ip arp learn-any

no ip arp learn-any

Command Default

Default ARP learning

Modes

VE configuration mode

Port-channel configuration mode

Usage Guidelines

This command enables learning from any ARP request (not necessarily targeted to **my ip** address).

To reset default ARP learning, use the **no** form of this command.

Examples

The following example enables learn-any on VE 100.

```
device# configure terminal
device(config)# interface ve 100
device(config-if-Ve-100)# ip arp learn-any
```

ip arp-aging-timeout

Sets how long a dynamic Address Resolution Protocol (ARP) entry stays in the ARP cache. The aging timer is reset each time an ARP reply is received.

Syntax

ip arp-aging-timeout *value*

no ip arp-aging-timeout

Command Default

ARP aging timeout is globally enabled and set to 25 minutes.

Parameters

value

Specifies how long an ARP entry stays in the ARP cache. Values range from 0 through 240 minutes.

Modes

Interface subtype configuration mode

Usage Guidelines

When the device places an entry in the ARP cache, the device also starts an aging timer for the entry. The aging timer ensures that the ARP cache does not retain learned entries that are no longer valid. An entry can become invalid when the device with the MAC address of the entry is no longer on the network.

The aging timer is reset each time an ARP reply is received.

Aging out affects dynamic (learned) entries only. Static entries do not age out.

You can modify the ARP aging timeout only at the interface level, but not at the global level.

To prevent entries from aging out, enter **ip arp-aging-timeout 0**.

The **no** form of the command restores the default aging timeout of 25 minutes.

Examples

The following command sets the ARP aging timeout to 100 minutes on an interface.

```
device(config)# interface ethernet 3/4
device(conf-if-eth-3/4)# ip arp-aging-timeout 100
```

The following command restores the ARP aging timeout to the default value on an interface.

```
device(config)# interface ethernet 3/4
device(conf-if-eth-3/4)# no ip arp-aging-timeout
```

ip dhcp relay

Syntax

ip dhcp relay [**disable-flooding** | **information option**]

no ip dhcp relay [**disable-flooding** | **information option**]

Parameters

disable-flooding

Disables flooding of DHCPv4 packets from the CPU.

information option

Enables DHCP Relay Information option.

Modes

Global Configuration Mode

Usage Guidelines

By default, flooding is not disabled and DHCPv4 packets are flooded in the Layer 2 domain.

The *no* form of this command resets to default behavior.

Examples

This example shows enabling DHCP Information Option.

```
SLX# configure terminal
SLX (config)# ip dhcp relay information option
SLX (config)#
```

This example shows the configuration to prevent flooding of DHCP packets within the Layer 2 broadcast domain.

```
SLX# configure terminal
SLX (config)# ip dhcp relay disable-flooding
SLX (config)#
```

ip dhcp relay address

Configures the IP DHCP Relay on a Layer 3 interface.

Syntax

ip dhcp relay address *ip-addr* [**use-vrf** *vrf-name*]

Parameters

ip-addr

IPv4 address of the DHCP server where the DHCP client requests are to be forwarded.

use-vrf

Use this option if the VRF where the DHCP server is located is different from the VRF of the interface where the client is connected.

vrf-name

VRF name.

Modes

Interface configuration mode

Usage Guidelines

This command uses the IPv4 address of the DHCP server where the DHCP client requests are to be forwarded.

Enter the command while in interface configuration mode for a VE or Ethernet interface where you want to configure the IP DHCP Relay. Configure up to sixteen DHCP server IP addresses per interface.

Use the **no** version of this command to remove the IP DHCP relay from the interface. If the **use-vrf** option is not used, it is assumed that the DHCP server and interface where the client is connected are on the same VRF.

Examples

To configure an IP DHCP Relay address on a Ve interface:

```
device# config
device(config)# interface ve 100
device(config-Ve-100)# ip dhcp relay address 3.1.2.255 use-vrf blue
```

ip dhcp relay gateway

Configures the IP DHCP Relay on a Layer 3 gateway interface.

Syntax

ip dhcp relay gateway *ip-addr*

no ip dhcp relay gateway *ip-addr*

Parameters

ip-addr

IPv4 gateway address of the DHCP server where the DHCP client requests are to be forwarded.

Modes

Interface configuration mode

Usage Guidelines

Use this command to configure the IP DHCP Relay on the switch Layer 3 gateway interface using the IPv4 address of the DHCP server where the DHCP client requests are to be forwarded.

Use the **no** version of this command to remove the IP DHCP Relay from the interface.

Examples

To configure an IP DHCP Relay address on an interface:

```
device(config)# interface ethernet 0/4

device(config-if-eth-0/4)# ip dhcp relay gateway 10.50.22.26
```

ip dhcp snooping

Enables DHCP snooping globally at the device level.

Syntax

ip dhcp snooping [**binding** [*mac-addr*| *ip-addr*] |**vlan** *vlan-id* | **interface** [*switchport* | *physical interface*]]

no ip dhcp snooping [**binding** [*mac-addr*| *ip-addr*] |**vlan** *vlan-id* | **interface** [*switchport* | *physical interface*]]

Command Default

By default, DHCP snooping is not enabled.

Parameters

binding [*mac-addr*| *ip-addr*]

Specifies the MAC or IP address of the host for the entry in the binding database.

vlan *vlan-id*

Specifies the VLAN ID of the host for the entry in the binding database.

interface [*switchport physical interface*]

Specifies the ID of the switchport interface.

Modes

Interface configuration mode

Usage Guidelines

DHCPv4 snooping uses trusted ports that have been identified as having legitimate DHCP servers attached. As clients communicate on the network, the device builds a *binding database*, which contains the MAC address of the host, the leased IP address, the lease time, the binding type, and the VLAN number and interface information associated with the host. The device then filters DHCP server messages from untrusted ports to protect the integrity of legitimate DHCP servers and their operation.

Use the **no** form of the command to disable DHCP snooping.

ip dhcp snooping enable

Enables DHCP snooping on one VLAN or a range of VLANs.

Syntax

ip dhcp snooping enable

no ip dhcp snooping enable

Command Default

By default, DHCP snooping is not enabled.

Modes

Interface configuration mode

ip dhcp snooping information option

Enables the insertion of Option-82 information into DHCP snooping packets.

Syntax

ip dhcp snooping information option { **allow-untrusted** }

no ip dhcp information option { **allow-untrusted** }

Command Default

By default, Option-82 information is not inserted into snooping packets.

Parameters

allow-untrusted

Globally enables the "Option-82 allow untrusted" feature on the device.

Modes

Interface configuration mode

Usage Guidelines

When you run the command with the **allow-untrusted** option, the device accepts incoming DHCP packets with Option-82 information on the untrusted port of the DHCP snooping-enabled VLAN.

Use the **no ip dhcp snooping information option** form of the command to disable the insertion of Option-82 information into snooping packets.

Use the **no ip dhcp snooping information option allow-untrusted** form of the command to disable the acceptance of Option-82 packets on the untrusted port.

ip dhcp snooping trust

Configures a Layer 2 switchport as trusted for DHCP snooping.

Syntax

ip dhcp snooping trust

no ip dhcp snooping trust

Command Default

By default, all switchports are untrusted.

Modes

Interface configuration mode

Usage Guidelines

Use the **no** form of the command to revert a switch port to the untrusted state.

ip directed-broadcast

Enables directed broadcasts on an interface. A directed broadcast is an IP broadcast to all devices within a directly attached network or subnet.

Syntax

ip directed-broadcast

no ip directed-broadcast

Command Default

Directed broadcast is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

To disable directed broadcasts on an interface, enter the **no** form of this command.

The Layer 3 interface can be physical Ethernet interface or VE interface.

Examples

The following example enables directed broadcasts on an Ethernet interface.

```
device(config)# interface ethernet 0/2
device(config-if-eth-0/2)# ip directed-broadcast
```

ip dns

Configures the Domain Name System (DNS) domain name and the primary and five additional name server IP addresses.

Syntax

ip dns { **domain-name** *domain-name* | **name-server** *ip-addr* }

ip dns name-server [**source-interface** { **ethernet** *eth-id* | **loopback** *loopback-id* | **management** *mgmt-addr* | **ve** *ve-id* }]

ip dns name-server { *ip-addr* **use-vrf vrf name** }

no ip dns { **domain-name** *domain-name* | **name-server** *ip-addr* }

no ip dns name-server [**source-interface** { **ethernet** *eth-id* | **loopback** *loopback-id* | **management** *mgmt-addr* | **ve** *ve-id* }]

Parameters

domain-name *domain-name*

Specifies the DNS domain name.

name-server *ip-addr*

Specifies the IPv4 or IPv6 address of the name server.

source-interface

Indicates the type of interface to use as the source interface or address.

ethernet *eth-id*

Specifies the Ethernet interface to use as the source interface, in slot/port format (0/1).

loopback *loopback-id*

Specifies the Loopback interface to use as the source interface.

management *mgmt-addr*

Specifies the management address (active MM or chassis IP) to use as the source address.

ve *ve-id*

Specifies the VE interface to use as the source interface.

use-vrf *vrfname*

Specifies the VRF to connect to the DNS server.

Modes

Global configuration mode

Usage Guidelines

Your first run of **ip dns name-server** specifies the default IP gateway address. Subsequent runs of the **ip dns name-server** command specifies the secondary and other IP gateway addresses.

Name servers can only be entered or removed one at a time. The newly entered name server is appended to the existing name server.

When a source interface is not specified, the default source is the IP address of the interface from which the packet egresses.

If, at run time, the source interface is not up, or the IP address for the source interface was not configured, the command behaves as though the source interface was not configured.

Use the **no** form of the command with the **domain-name** parameter to disable IP-directed broadcasts for a specific domain.

Use the **no** form of the command with the **name-server** parameter to delete a name server definition. You can delete one **name-server** at a time.

Any combination of IPv4 or IPv6 DNS name servers can be configured. You could choose to add 2 IPv6 name servers alongside 4 IPv4 name servers. However, you cannot add more than six name servers for a domain.

If you add more than six name servers for a domain, an error message displays.

```
too many 'ip dns name-server', 7 configured, at most 6 must be configured
```

Examples

The following example configures the DNS domain name and the primary name server IP address.

```
device# configure terminal
device(config)# ip dns domain-name mycompany.com
device(config)# ip dns name-server  10.70.20.1
```

This example identifies an Ethernet interface as the source interface.

```
device# configure terminal
device(config)# ip dns name-server 1.1.1.1
device(config-name-server-1.1.1.1/mgmt-vrf)# source-interface ethernet 0/1
```

This example configures six (6) DNS name servers for the domain *www.example.com*. Of these six (6) domain names, two (2) are IPv6 DNS resolvers.

```
device# configure terminal
device(config)# ip dns domain-name www.example.com
device(config)# ip dns name-server 10.24.15.150
device(config)# ip dns name-server 10.24.18.125
device(config)# ip dns name-server 172.26.71.80
device(config)# ip dns name-server 200:f8::ed:3000
device(config)# ip dns name-server 2001:eb::780:ff87
```

```
device(config)# ip dns name-server 10.37.89.80
```

ip extcommunity-list

Configures a BGP extended community filter.

Syntax

ip extcommunity-list *number* { **deny** | **permit** [**rt** *value* | **soo** *value*] *reg-expr* }

no ip extcommunity-list *number*

Command Default

No BGP extended community filter is set.

Parameters

number

Specifies an extended community list Instance number. Range is from 0 through 99 for a standard list (RT- or SOO-based), and from 100 through 500 for an expanded list (regular-expression-based).

deny

Denies access for a matching condition.

permit

Permits access for a matching condition.

rt

Specifies the route target (RT) extended community.
value

This value can be one of the following formats:

- autonomous-system-number : network-number
- ip-address : network-number

soo

Specifies the site of origin (SOO) extended community.
value

This value can be one of the following formats:

- autonomous-system-number : network-number
- ip-address : network-number

reg-expr

Specifies a regular expression. For more information, see the "BGP4 Regular Expression Pattern-matching" topic in the *Extreme SLX-OS Layer 3 Routing Configuration Guide*.

Modes

Global configuration mode

Usage Guidelines

Use the no form of this command to delete a BGP extended community list.

Examples

The following example specifies a standard extended community list, permits a route target, and denies a site of origin.

```
device# configure terminal
device(config)# ip extcommunity-list 99 permit rt 123:2
device(config)# ip extcommunity-list 99 deny soo 124:1
```

The following example specifies an expanded extended community list and permits a regular expression.

```
device# configure terminal
device(config)# ip extcommunity-list 101 permit 100:*
```

The following example deletes an extended community list.

```
device# configure terminal
device(config)# no ip extcommunity-list 101
```

ip flowspec rules statistics

Enables statistics for Border Gateway Protocol flow specification (BGP flowspec) rules.

Syntax

ip flowspec rules statistics [**vrf** *vrf-name*]

no ip flowspec rules statistics [**vrf** *vrf-name*]

Command Default

Flowspec statistics are disabled.

Parameters

vrf *vrf-name*

Name of a VRF instance.

Modes

Global configuration mode

Usage Guidelines

When statistics are enabled, they appear in the output of the **show ip flowspec rules** command.

Statistic	Description
Matched	Number of packets or bytes that match the flowspec rule
Transmitted	Number of packets matching the flowspec rule that are transmitted
Dropped	Number of packets matching the flowspec rule that are dropped

The **no** form of the command disables statistics for BGP flowspec rules.

Examples

The following example shows how to enable statistics for BGP flowspec rules.

```
device# configure terminal
device(config)# ip flowspec rules statistics
```

The following example shows how to disable statistics for BGP flowspec rules in a VRF named red.

```
device# configure terminal
device(config)# no ip flowspec rules statistics vrf red
```

ip forward

Enables IPv4 forwarding on a physical or virtual Ethernet interface that is configured for IPv6 only.

Syntax

ip forward

no ip forward

Command Default

By default, IPv4 forwarding is disabled on physical and virtual Ethernet interfaces.

Modes

Interface subtype configuration mode

Usage Guidelines

When IPv4 forwarding is enabled on an IPv6 interface, IPv4 packets are accepted and forwarded over the interface.

IPv4 forwarding configuration is only allowed on Layer-3 interfaces that have an IPv6 address or IPv6 address link-local configuration. IPv4 forwarding configuration is not allowed on interfaces with an unnumbered or IPv4-address configuration. Similarly, when IPv4 forwarding is configured on an interface, you cannot configure the interface as an unnumbered interface or with an IPv4 address.

When IPv4 forwarding is configured on an interface, you cannot delete the last IPv6 address configuration on that interface.

The **no** form of the command disables IPv4 forwarding on a physical or virtual Ethernet interface.

Examples

The following example shows how to enable IPv4 forwarding on physical Ethernet interface 0/5.

```
device# configure terminal
device(config)# interface ethernet 0/5
device(conf-if-eth-0/5)# ip forward
```

The following example shows how to enable IPv4 forwarding on virtual Ethernet interface 10.

```
device# configure terminal
device(config)# interface ve 10
device(conf-if-ve-10)# ip forward
```

ip global-subnet-broadcast-acl

Applies an IP broadcast ACL (bACL) at device level.

Syntax

ip global-subnet-broadcast-acl *acl-name*

no ip global-subnet-broadcast-acl *acl-name*

Command Default

No bACL is applied at device level.

Parameters

acl-name

Specifies the standard or extended bACL.

Modes

Global configuration mode

Usage Guidelines

IP broadcast ACLs (bACLs) provide hardware-based filtering of IP subnet-based directed broadcast and network-address traffic.

Broadcast ACLs are not supported on SLX 9150 or SLX 9250 devices.

The **no** form of this command removes a bACL from the device.

Examples

The following example applies a bACL at device level.

```
device# configure terminal
device(config)# ip global-subnet-broadcast-acl bacl_10
```

The following example removes a bACL from the device.

```
device# configure terminal
device(config)# ip global-subnet-broadcast-acl bacl_10
```

ip icmp-fragment enable

Configures a device to drops all fragmented ICMP packets that are destined to that device.

Syntax

ip icmp-fragment enable

no ip icmp-fragment enable

Command Default

By default, a device does not drop fragmented ICMP packets that are destined to itself.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of the command to disable the feature.

Examples

The following example enables a device to drop fragmented ICMP packets.

```
device# configure terminal
device(config)# ip icmp-fragment enable
```

ip icmp rate-limiting

Limits the rate at which IPv4 Internet Control Message Protocol (ICMP) messages are sent on a network.

Syntax

ip icmp rate-limiting *milliseconds*

no ip icmp rate-limiting

Command Default

By default, rate limiting is enabled on the management port, but is disabled on the other ports.

Parameters

milliseconds

Time interval per ICMP packet in milliseconds. The range is from 0-4294967295. The default is 1000.

Modes

Interface configuration mode

Port-channel configuration mode

Usage Guidelines

This is an interface-specific configuration.

The **no** form of the command will revert to the default setting. Set the interval to 0 to disable IPv4 ICMP rate-limiting.

Examples

The following example enables IPv4 ICMP rate-limiting on an Ethernet interface.

```
device(config)# interface ethernet 3/5
device(conf-int-eth-3/5)# ip icmp rate-limiting 10000
```

ip icmp redirect

Enables IPv4 Internet Control Message Protocol (ICMP) Redirect messages, which request that packets be sent on an alternative route.

Syntax

ip icmp redirect

no ip icmp redirect

Command Default

ICMP redirect messages are disabled by default.

Modes

Interface configuration mode

Usage Guidelines

Note
This command is only available on SLX 9640 and SLX 9540.

Note
This command is not supported on port-channel (PO)/virtual ethernet (VE) interfaces.

The **no** form of the command disables IPv4 ICMP Redirect messages.

User can disable ICMP redirect messages when traffic needs to be routed into and out of the same Layer 3 interface.

Examples

The following example enables IPv4 ICMP Redirect messages on an Ethernet interface.

```
device(config)# interface ethernet 2/5
device(conf-int-eth-2/5)# ip icmp redirect
```

ip icmp unreachable

Enables a Layer 3 device to respond to IPv4 ICMP unreachable messages.

Syntax

ip icmp unreachable

no icmp unreachable

Command Default

By default, the device does not respond to ICMP unreachable notifications.

Modes

Interface configuration mode

Usage Guidelines

Use the **no** form of the command to disable the feature.

Examples

The following example enables a device to respond to ICMP unreachable notifications to the indicated source.

```
device# configure terminal
device(config)# interface ve 2
device(config-int-ve-2)# ip address 2.1.1.1/24
device(config-int-ve-2)# ip icmp unreachable
```

ip igmp immediate-leave

Removes a group from the IGMP table immediately following receipt of a Leave Group request.

Syntax

ip igmp immediate-leave

no ip igmp immediate-leave

Command Default

This command is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

This command treats an interface as if it had one multicast client, so that the receipt of a Leave Group request on the interface causes the group to be removed immediately from the multicast database.

Enter the **no** form of this command to restore the default behavior.

Examples

To configure an Ethernet interface to remove a group from the IGMP table immediately following receipt of a Leave Group request:

```
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip igmp immediate-leave
```

ip igmp last-member-query-interval

Sets the IGMP last-member query interval for an interface.

Syntax

ip igmp last-member-query-interval *milliseconds*

no ip igmp last-member-query-interval

Command Default

By default, the query interval is 1000 milliseconds.

Parameters

milliseconds

Response time in milliseconds. Range is from 100-25500 milliseconds. The default is 1000.

Modes

Interface subtype configuration mode

Usage Guidelines

The last-member query interval is the time in milliseconds that the IGMP router waits to receive a response to a group-specific query message, including messages sent in response to a host-leave message.

Enter the **no** form of this command to restore the default.

Examples

To set the last-member query interval to 1500 milliseconds on an interface:

```
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip igmp last-member-query-interval 1500
```

ip igmp query-interval

Sets the IGMP query interval for an interface.

Syntax

ip igmp query-interval *seconds*

no ip igmp query-interval *seconds*

Command Default

See Parameters.

Parameters

seconds

Response time in seconds. Range is from 1 through 18000 seconds. The default is 125.

Modes

Interface subtype configuration mode

Usage Guidelines

The query interval is the amount of time between IGMP query messages sent by the device.

Enter the **no** form of this command to restore the default.

Examples

To set the query interval to 500 seconds on an interface:

```
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip igmp query-interval 500
```

ip igmp query-max-response-time

Sets the maximum response time for IGMP queries for an interface.

Syntax

ip igmp query-max-response-time *seconds*

no ip igmp query-max-response-time

Command Default

The default is 10 seconds.

Parameters

seconds

Response time in seconds. Range is from 1 through 25 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

When a host receives the query packet, it starts counting to a random value, less than the maximum response time. When this timer expires, the switch (host) replies with a report, provided that no other host from the same group has responded yet.

Enter the **no** form of this command to restore the default.

Examples

To set the maximum response time to 20 seconds:

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip igmp query-max-response-time 20
```

ip igmp router-alert-check-disable

Disables the snooping check for the presence of the router alert option.

Syntax

ip igmp router-alert-check-disable

no ip igmp router-alert-check-disable

Command Default

By default, the snooping check is enabled.

Modes

Global configuration mode

Usage Guidelines

IGMP snooping checks for the presence of the router alert option in the IP packet header of the IGMP message. Packets that do not include this option are dropped.

Examples

The following example disables the snooping router alert check globally.

```
device(config)# ip igmp router-alert-check-disable
```

ip igmp snooping enable

Enables Internet Group Management Protocol (IGMP) snooping on a VLAN.

Syntax

ip igmp snooping enable

no ip igmp snooping enable

Command Default

By default, snooping is enabled.

Modes

VLAN configuration mode

Usage Guidelines

IGMP snooping allows a network device to listen in on the IGMP conversation between hosts and routers. By listening to these conversations, the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them.

Enter **no ip igmp snooping enable** to disable snooping for a specific VLAN.

Examples

To enable IGMP on a VLAN:

```
device(config)# vlan 1
device(config-Vlan-1)# ip igmp snooping enable
```

ip igmp snooping fast-leave

Enables Internet Group Management Protocol (IGMP) snooping fast-leave processing for a VLAN. This allows the removal of an interface from the forwarding table without sending out group-specific queries to the interface.

Syntax

ip igmp snooping fast-leave

no ip igmp snooping fast-leave

Command Default

By default, fast-leave processing is enabled.

Modes

VLAN configuration mode.

Usage Guidelines

Use the **no ip igmp snooping fast-leave** form of the command to disable this function.

Examples

To enable snooping fast-leave for a specific VLAN:

```
device(config)# vlan 1
device(config-Vlan-1)# ip igmp snooping fast-leave
```

ip igmp snooping last-member-query-interval

Sets the IGMP snooping last member query interval value in milliseconds.

Syntax

ip igmp snooping last-member-query-interval *value*

no ip igmp snooping last-member-query-interval *value*

Command Default

The default is 1000 ms.

Parameters

value

Sets the value in milliseconds. The range is 100 to 25500 milliseconds.

Modes

VLAN configuration mode

Usage Guidelines

When a leave is received, a group-specific query is sent. Last member query interval configuration controls the time interval between last member queries sent.

Examples

The following example sets the IGMP snooping last member query interval.

```
device(config)# vlan 1
device(config-Vlan-1)# ip igmp snooping last-member-query-interval 2000
```

ip igmp snooping mrouter interface

Configures a VLAN port member to be a multicast router interface.

Syntax

ip igmp snooping mrouter interface { **ethernet** *slot/port* | **port-channel** *interface number* }

no ip igmp snooping mrouter interface { **ethernet** *slot/port* | **port-channel** *interface number* }

Command Default

By default, a VLAN port member is not a multicast router interface.

Parameters

ethernet *slot/port*

Specifies a valid port number.

port-channel *interface number*

Specifies the interface is a port-channel.

Modes

VLAN configuration mode

Usage Guidelines

A multicast router interface faces toward a multicast router or other Internet Group Management Protocol (IGMP) querier.

The **no** form of this command removes the configured mrouter.

Examples

The following example configures a VLAN port member to be a multicast router interface.

```
device(config)# vlan 1
device(config-Vlan-1)# ip igmp snooping mrouter interface ethernet 1/1
```

ip igmp snooping querier enable

Activates the Internet Group Management Protocol (IGMP) snooping querier on a VLAN.

Syntax

ip igmp snooping querier enable

no ip igmp snooping querier enable

Command Default

By default, the IGMP snooping querier is enabled.

Modes

VLAN configuration mode

Usage Guidelines

Multicast routers use IGMP snooping to learn which groups have members on their attached physical networks. The snooping querier sends IGMP queries to trigger IGMP responses from devices that are to receive IP multicast traffic. The IGMP snooping querier receives these responses and maps the appropriate forwarding addresses.

The **no ip igmp snooping querier enable** form of the command disables the IGMP snooping querier.

Examples

The following example enables the IGMP snooping querier on a VLAN.

```
device(config)# vlan 1
device(config-vlan-1)# ip igmp snooping querier enable
```

ip igmp snooping query-interval

Sets the IGMP snooping query interval in seconds.

Syntax

ip igmp snooping query-interval *seconds*

no ip igmp snooping query-interval *seconds*

Command Default

The query interval is enabled by default with a value of 125 seconds.

Parameters

seconds

Sets the IGMP snooping query interval in seconds. The range is 1-18000 seconds.

Modes

VLAN configuration mode

Usage Guidelines

The snooping query interval is the frequency with which the device sends group membership queries.

Examples

The following example sets the IGMP snooping query interval.

```
device(config)# vlan 1
device(config-vlan-1)# ip igmp snooping query-interval 200
```

ip igmp snooping query-max-response-time

Sets the IGMP snooping query maximum response time.

Syntax

ip igmp snooping query-max-response-time *seconds*

no ip igmp snooping query-max-response-time *seconds*

Command Default

The maximum response time is enabled by default with a value of 10 seconds.

Parameters

seconds

Specifies the IGMP snooping query maximum response time in seconds. The range is 1-25 seconds.

Modes

VLAN configuration mode

Usage Guidelines

The IGMP snooping query maximum response time is the number of seconds that a device wait sfor an IGMP (V1 or V2) response from an interface before concluding that the group member on that interface is down and removing it from the group.

Examples

The following example sets the IGMP snooping query max response time.

```
device(config)# vlan 1
device(config-Vlan-1)# ip igmp snooping query-max-response-time 15
```

ip igmp snooping static-group

Configures an interface in a VLAN as a static member of a multicast group.

Syntax

ip igmp snooping static-group { *ip-address* } {**interface** *ethernet/port-channel* }

no ip igmp snooping static-group { *ip-address* } {**interface** *ethernet/port-channel* }

Command Default

By default, an interface in a VLAN is not a static member of a multicast group.

Parameters

ip-address

Specifies the multicast address to be joined in A.B.C.D format.

interface

Specifies the interface.
ethernet/port-channel

Specifies the interface type.

Modes

VLAN configuration mode

Usage Guidelines

A snooping-enabled VLAN cannot forward multicast traffic to ports that do not receive IGMP membership reports. If clients cannot send reports, you can configure a static group which applies to specific ports. The static group allows packets to be forwarded to the static group ports even though they have no client membership reports.

Examples

The following example configures a static group for an Ethernet interface.

```
device# configure terminal
device(config)# vlan 10
device(config-vlan-10)# ip igmp snooping static-group 225.0.0.1 interface ethernet 6/15
```

ip igmp snooping version

Sets the IGMP version used for snooping for a VLAN.

Syntax

ip igmp snooping version [**1**|**2**|**3**]

no ip igmp snooping version

Command Default

By default, snooping uses IGMP version 2.

Parameters

1|**2** |**3**

Specifies the version of IGMP that you want to use.

Modes

VLAN configuration mode

Usage Guidelines

The **no ip igmp snooping version** form of the command resets IGMP to version 2.

Examples

The following example sets the version to 3 for a VLAN.

```
device# configure terminal
device(config)# vlan 10
device(config-vlan-10)# ip igmp snooping version 3
```

ip igmp ssm-map

Enables the IGMPv2 Source Specific Multicast mapping.

Syntax

ip igmp ssm-map [*ASCII string*| **enable** *source-address*]

no ip igmp ssm-map [*ASCII string* | **enable** *source-address*]

Parameters

ASCII string

Specifies the prefix list name.

enable *source-address*

Specifies the source address.

Modes

Global configuration mode

Router PIM configuration mode

Usage Guidelines

A prefix list is used for SSM mapping with permit clauses.

Use the **no** form of this command to disable SSM mapping.

Examples

The following example enables the SSM mapping for IGMPv2 and configures an SSM map at the global level.

```
device(config)# ip igmp ssm-map enable
device(config)# ip igmp ssm-map ssm-map-230-to-232 203.0.0.10
device(config)# ip igmp ssm-map ssm-map-233-to-234 204.0.0.10
```

The following example enables the SSM range configuration at the router PIM level.

```
device(config)# router pim
    device(config-pim-router)# ssm-enable range PL_ssm_range -230-to-234
```

The following example shows a prefix list configuration for the SSM range.

```
device(config)# ip prefix-list PL_ssm_range  seq 5 permit 230.0.0.0/8
device(config)# ip prefix-list PL_ssm_range seq 10 permit 231.0.0.0/8
device(config)# ip prefix-list PL_ssm_range seq 10 permit 232.0.0.0/8
device(config)# ip prefix-list PL_ssm_range seq 10 permit 233.0.0.0/8
device(config)# ip prefix-list PL_ssm_range seq 10 permit 234.0.0.0/8
```

The following example shows a prefix list configuration for an SSM map.

```
device(config)# ip prefix-list ssm-map-230-to-232 seq 5 permit 230.0.0.0/8
device(config)# ip prefix-list ssm-map-230-to-232 seq 10 permit 231.0.0.0/8
device(config)# ip prefix-list ssm-map-230-to-232 seq 15 permit 232.0.0.0/8

device(config)# ip prefix-list ssm-map-233-to-234 seq 5 permit 233.0.0.0/8
device(config)# ip prefix-list ssm-map-233-to-234 seq 10 permit 234.0.0.0/8
device(config)# ip prefix-list ssm-map-230-to-232 seq 15 permit 232.0.0.0/8
```

ip igmp static-group

Configures the IGMP static group membership entries for a specific interface.

Syntax

ip igmp static-group *A.B.C.D*

no ip igmp static-group *A.B.C.D*

Parameters

A.B.C.D

Specifies the group address, as a subnet number in dotted decimal format (for example, 10.0.0.1), as the allowable range of addresses to be included in the multicast group.

Modes

Interface subtype configuration mode

Usage Guidelines

Use IGMP static group membership to test multicast forwarding without a receiver host. Traffic is forwarded to an interface without the need to receive membership reports from host members. Packets to the group are fast-switched out of a specific interface. Static group membership entries are automatically added to the IGMP cache and the PIM mcache table.

Examples

The following example creates a static multicast group for an interface.

```
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip igmp static-group 225.0.0.10
```

ip igmp version

Specifies the IGMP version on a device.

Syntax

ip igmp version *version-number*

no ip igmp version *version-number*

Command Default

IGMP Version 2 is enabled.

Parameters

version-number

Specifies the version number: 1, 2, or 3. Version 2 is the default.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of this command restores the default; IGMP Version 2 is enabled.

Examples

The following example, in interface configuration mode, enables IGMP Version 3 for a physical port.

```
device# configure terminal
device(config)# interface ethernet 1/1/5
device(config-if-1/1/5)# ip igmp version 3
```

ip interface loopback (overlay gateway)

Sets the loopback port number for the VXLAN overlay gateway.

Syntax

ip interface loopback *loopback_id*

no ip interface loopback *loopback_id*

Parameters

loopback_id

Specifies a loopback interface. Range is from 1 through 255.

Modes

Overlay gateway configuration mode

Usage Guidelines

Use the **no** form of this command to delete the interface from the gateway.

Examples

The following example configures a loopback interface to the overlay gateway instance.

```
device# configure terminal
device(config)# overlay-gateway gateway1
device(config-overlay-gw-gateway1)# ip interface loopback 10
```

ip irdp

Enables IPv4 ICMP Router Discovery Protocol.

Syntax

ip irdp

no ip irdp

Command Default

By default, the ICMP Router Discovery Protocol is not enabled.

Modes

Interface configuration mode

Usage Guidelines

Routers use the IPv4 ICMP Router Discovery Protocol to announce their presence to other systems in the subnet. Hosts use the protocol to dynamically discover IPv4 routers in the same subnet.

The protocol is disabled by default on Layer 3 interfaces. Use the **ip irdp** command to enable the protocol at the interface level.

Examples

This example enables the IPv4 ICMP Router Discovery Protocol on Ethernet interface 0/2.

```
device# configure terminal
device(config)# interface ethernet 0/2
device(config-if-eth-0/2)# ip irdp
```

ip large-community-list extended

Configures a BGP Large Community access control list (ACL), specifies the large-community name, and specifies whether to permit or deny traffic, including through the use of a regular expression.

Syntax

ip large-community-list extended *large-community-list-name* [**seq** *seq*] { **deny** | **permit** } *string*

no ip large-community-list extended *large-community-list-name* [[**seq** *seq*] { **deny** | **permit** } *string*]

Command Default

No extended large-community list is configured.

Parameters

large-community-list-name

Specifies an ACL, from 1 through 32 ASCII characters in length.

seq *seq-value*

Specifies a sequence value. Valid values range from 1 through 65535.

deny

Denies a matching pattern based on a regular expression string.

permit

Permits a matching pattern based on a regular expression string.

string

A regular expression. Range is from 1 through 32 ASCII characters.

Modes

Global configuration mode

Usage Guidelines

Unlike a standard large-community list, this command does accept a regular expression.

The **no** form of the command removes a configured ACL.

Examples

The following example creates an extended community list.

```
device# configure terminal
device(config)# ip large-community-list extended lc-acl-ext-1 seq 10 permit _4567*
```

ip large-community-list standard

Configures a BGP Large-Community access control list (ACL), specifies the large-community number or type, and whether to permit or deny traffic.

Syntax

ip large-community-list standard *large-community-list-name* [**seq** *seq-value*] { **deny** | **permit** } *ADMIN:OPER1:OPER2*

no ip large-community-list standard *large-community-list-name* [[**seq** *seq-value*]{**deny** | **permit** } *ADMIN:OPER1:OPER2*]

Command Default

No large-community ACL is configured.

Parameters

large-community-list-name

Range is from 1 through 32 ASCII characters.

deny

Denies a matching pattern based on a large community pattern specified in the list.

permit

Permits a matching pattern based on a large community pattern specified in the list.

seq *seq-value*

Specifies a sequence value. Valid values range from 1 through 65535.

ADMIN

A four-octet namespace identifier for a BGP Large-Communities Global Administrator.

OPER1

A four-octet operator-defined value for BGP Large-Communities Local Data Part 1.

OPER2

A four-octet operator-defined value for BGP Large-Communities Local Data Part 2.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to remove the BGP Large-Community ACL.

A standard large-community list does not accept a regular expression.

There are two ways to delete a filter from the list. The first is by using the sequence number parameter **no ip large-community-list standard** *large-community-list-name* **seq** *seq-value*. The second is by executing the syntax **no ip large-community-list standard** *large-community-list-name* , resulting in all filters within the large-community list container, being removed from the configuration database.

Examples

The following example creates a standard large-community list.

```
device# configure terminal
device(config)# ip large-community-list standard lc-acl-1 seq 10 permit 64497:1:528
```

ip mtu

Sets the IP maximum transmission unit (MTU) globally or on an interface.

Syntax

ip mtu *size*

no ip mtu

Command Default

The default IP MTU size is 1500 bytes.

Parameters

size

Specifies the size of the IP MTU globally or the interface. Enter an integer from 1300 through 9194 bytes.

Modes

Global configuration mode

Interface configuration mode

Port-channel configuration mode

Usage Guidelines

The **no** form of the command reverts the MTU size to the default value.

Using the **no** form of this command in global configuration mode resets the default value on all interfaces except the interfaces that you manually configured with MTU values.

When you change the IP MTU size globally, the change is applied to all Ethernet and VE interfaces on the device. However, it does not change a configured interface MTU value. The configured interface value takes precedence over the configured global MTU value.

The **show running-config** command displays the the MTU size when it is not the default value. If you change the global MTU size and do not change the interface MTU size, the **show running-config** command does not display the global MTU value at the interface level.

If the interface is part of a VE, change the IPv4 MTU only at the VE interface and not at the physical port. All member ports of a VE inherit the VE-interface IPv4 MTU value.

Examples

The following example sets the IP MTU to 2000 bytes on the specified Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 2/9
device(conf-if-eth-2/9)# ip mtu 2000
```

The following example changes the IP MTU for a VE.

```
device# configure terminal
device(config)# interface ve 103
device(config-vif-103)# ip mtu 2000
```

The following example changes the IP MTU globally.

```
device(config)# ip mtu 2000
```

ip option

Blocks packets that have IP options. Also blocks packets that are marked for processing directly by the device's control plane processing unit.

Syntax

ip option [**disable** | **disable-cpu**]

no ip option [**disable** | **disable-cpu**]

show running-configuration ip

Command Default

By default, packets with IP options are not blocked. Similarly, packets that are marked directly for the *Control Plane Processing Unit* (CPU) are not blocked by default.

Modes

Global configuration mode

Usage Guidelines

The *disable* and *disable-cpu* options are mutually exclusive. You cannot use one if the other is already configured. For example, if you have configured the *disable* option, you cannot configure the *disable-cpu* option without removing the previous configuration.

Use the **no** form of the command to unblock packets that have IP options.

The `show running-configuration ip` checks if ip option disable is already configured or not.

Examples

The following example blocks packets that have IP options set.

```
SLX#configure terminal
SLX (config) # ip option disable
```

The following example blocks packets that are destined for the CPU.

```
SLX# configure terminal
SLX (config) # ip option disable-cpu
```

The following example displays the error that will be displayed when you try to configure over an existing `ip option` configuration.

```
SLX# configure terminal
SLX (config) # ip option ?
Possible completions:
  disable      IP option disable
  disable-cpu  IP option disable for CPU
```

```
SLX (config)# ip option disable-cpu
SLX (config)# do show running-config ip option
```

The following example displays an error when the other command is executed.

```
ip option disable-cpu

SLX (config)# ip option disable
    %% Error: IP option disable-cpu is configured.
    It needs to be unconfigured before executing this command.
```

ip ospf active

Sets a specific OSPF interface to active.

Syntax

ip ospf active

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **ip ospf active** command on each interface participating in adjacency formation. This command overrides the global passive setting on that interface, and enables transmission of OSPF control packets.

Examples

The following example sets a specific OSPFv2 Ethernet interface to active.

```
device# configure termnial
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf active
```

ip ospf area

Enables OSPFv2 on an interface.

Syntax

ip ospf area *area-id | ip-addr*

no ip ospf area

Command Default

Disabled.

Parameters

area-id

Area ID in decimal format. Valid values range from 1 through 2147483647.

ip-addr

Area ID in IP address format.

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command disables OSPFv2 on the interface.

When configuring OSPF on a VE interface that will be applied to a GRE tunnel, the MTU configured in that VE is applied to the GRE tunnel and is used as the MTU for the tunnel. When configuring the MTU for the tunnel interface, the assigned MTU value takes into account the 24 bytes reserved for the GRE Tunnel Header. This 24 bytes is automatically reduced from the target MTU.

Note
The 24 bytes consists of a 20 Byte GRE Outer Header and a 4 Byte Outer IP Header.

For example, when the VE MTU is set to the default MTU 1500, the GRE tunnel MTU will automatically be adjusted to 1476 Bytes and the remaining 24 bytes are used to carry the GRE Tunnel Header information . If the VE MTU is set to any value other than the default MTU value, the reserved 24 bytes will be automatically reduced from your target configuration before it is set as the VE's MTU.

In the case where you want to assign the maximum permissible MTU of 9194 Bytes, you must manually reduce the reserved 24 Bytes. In this case, you should set the MTU value at 9170 Bytes.

Examples

The following example enables a configured OSPFv2 area named 1 on a specific OSPFv2 virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ip ospf area 1
```

ip ospf auth-change-wait-time

Configures authentication-change hold time.

Syntax

ip ospf auth-change-wait-time *wait-time*

no ip ospf auth-change-wait-time

Command Default

Wait time is 300 seconds

Parameters

wait-time

Time before an authentication change takes place. Valid values range from 0 to 14400 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to set or reset the authentication change hold time for the interface to which you are connected.

OSPFv2 provides graceful authentication change for the following types of authentication changes:

Changing authentication methods from one of the following to another of the following:

- Simple text password
- MD5 authentication
- No authentication

Configuring a new simple text password or MD5 authentication key.

Changing an existing simple text password or MD5 authentication key

The **no** form of the command resets the wait time to the default of 300 seconds.

Examples

The following example sets the wait time to 400 seconds on a specific OSPF virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ip ospf auth-change-wait-time 400
```

ip ospf authentication-key

Configures simple password-based authentication for OSPF.

Syntax

ip ospf authentication-key *password*

no ip ospf authentication-key

Command Default

Authentication is disabled.

Parameters

password

OSPF processes *password* as a plain text password.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to set or reset simple password-based authentication on the OSPFv2 interface to which you are connected. The **no** form of the command disables OSPFv2 authentication.

Examples

The following example configures an authentication key for an OSPF virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ip ospf authentication-key morningadmin
```

ip ospf bfd

Enables Bidirectional Forwarding Detection (BFD) on a specific OSPFv2 interface.

Syntax

ip ospf bfd

no ip ospf bfd

Modes

Interface subtype configuration mode

Usage Guidelines

BFD sessions are initiated only if BFD is also enabled globally using the **bfd** command in OSPF router configuration mode. If BFD is disabled using the **no bfd** command in OSPF router configuration mode, BFD sessions on specific OSPFv2 interfaces are deregistered.

The **no** form of the command removes all BFD sessions from a specified interface.

Examples

The following example enables BFD on an OSPF Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/4
device(conf-if-eth-1/4)# ip ospf bfd
```

The following example disables BFD on an OSPF virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 24
device(config-if-ve-24)# no ip ospf bfd
```

ip ospf cost

Configures cost for a specific interface.

Syntax

ip ospf cost *value*

no ip ospf cost

Command Default

Cost value is 1.

Parameters

value

Cost value. Valid values range from 1 through 65535. The default is 1.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to set or reset the OSPFv2 cost on the interface. If the cost is not configured with this command, OSPFv2 calculates the value from the reference and interface bandwidths.

The **no** form of the command disables the configured cost.

Examples

The following example sets the cost to 520 on a specific Loopback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# ip ospf cost 520
```

ip ospf database-filter

Configures filters for different types of outgoing Link State Advertisements (LSAs).

Syntax

ip ospf database-filter { **all-external** | **all-summary-external** { **allow-default-and-type-4** | **allow-default-out** | **out** } }

ip ospf database-filter all-out

no ip ospf database-filter all-external

no ip ospf database-filter all-out

no ip ospf database-filter all-summary-external

Command Default

All filters are disabled.

Parameters

all-external

Blocks all external LSAs.

all-summary-external

Blocks all summary (Type 3) and external (type 5) LSAs.

allow-default-and-type-4

Allows default-route LSAs and Type 4 LSAs, but block all other LSAs.

allow-default-out

Allows default-route LSAs, but block all other LSAs.

out

Filters outgoing LSAs.

all-out

Blocks all LSAs.

Modes

Interface subtype configuration mode

Usage Guidelines

By default, the device floods all outbound LSAs on all the OSPF interfaces within an area. You can configure a filter to block outbound LSAs on an OSPF interface. This feature is particularly useful when you want to block LSAs from some, but not all, of

the interfaces attached to the area. When enabled, this command blocks the specified outgoing LSAs on the interface. Some cases where you might want to enable filters are:

- To control the information being advertised to the network.
- To use a passive router for debugging only.

The **no** form of the command disables configurations.

Note
You cannot block LSAs on virtual links.

Examples

The following example applies a filter to block flooding of all LSAs on a specific OSPF Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf database-filter all-out
```

ip ospf dead-interval

Configures the neighbor dead interval, which is the number of seconds that a neighbor router waits for a hello packet from the device before declaring the router down.

Syntax

ip ospf dead-interval *interval*

no ip ospf dead-interval

Command Default

The specified time period is 40 seconds.

Parameters

interval

Dead interval in seconds. Valid values range from 3 through 65535 seconds. The default is 40.

Modes

Interface subtype configuration mode

Usage Guidelines

If you change the dead interval, the hello interval is automatically changed to a value that is one fourth that of the new dead interval, unless the hello interval is also explicitly configured using the **ip ospf hello-interval** command.

The recommended setting is that:

- The dead interval is four times that of the hello interval.
- The hello interval is ¼ times that of the dead interval.

The **running-config** command displays only explicitly configured values of the hello interval, which means that a value that was automatically changed as the result of a dead-interval change is not displayed.

The **no** form of the command restores the default value.

Examples

The following example sets the dead interval to 200 on a specific OSPFv2 virtual Ethernet (VE) interface.

```
device# configure terminal
```

```
device(config)# interface ve 1
device(config-if-Ve-1)# ip ospf dead-interval 200
```

ip ospf hello-interval

Configures the hello interval, which is the length of time between the transmission of hello packets that this interface sends to neighbor routers.

Syntax

ip ospf hello-interval *interval*

no ip ospf hello-interval

Command Default

The default value is 10 seconds.

Parameters

interval

Hello interval in seconds. Valid values range from 1 through 65535.

Modes

Interface subtype configuration mode

Usage Guidelines

If you change the hello interval, the dead interval is automatically changed to a value that is four times that of the new hello interval, unless the dead interval is also explicitly configured using the **ip ospf dead-interval** command.

The recommended setting is that:

- The dead interval is four times that of the hello interval.
- The hello interval is ¼ times that of the dead interval.

The **running-config** command displays only explicitly configured values of the dead interval, which means that a value that was automatically changed as the result of a hello-interval change is not displayed.

The **no** form of the command restores the default value.

Examples

The following example sets the hello interval to 50 on a specific OSPFv2 virtual Ethernet (VE) interface:

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ip ospf hello-interval 50
```

ip ospf ldp-sync

Enables Label Distribution Protocol (LDP) synchronization with OSPF and configures the hold down time interval for an interface.

Syntax

ip ospf ldp-sync { **disable** | **enable** }

no ip ospf ldp-sync enable

Command Default

Disabled.

Parameters

`disable`

Disables LDP synchronization.

`enable`

Enables LDP synchronization.

Modes

Interface subtype configuration mode

Examples

The following example enables LDP synchronization with OSPF for an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf ldp-sync enable
```

The following example disables LDP synchronization with OSPF for a loopback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Looback-1)# ip ospf ldp-sync disable
```

ip ospf md5-authentication

Configures MD5 password and authentication change hold time.

Syntax

ip ospf md5-authentication { **key-activation-wait-time** *wait-time* | **key-id** *id* **key** *password* }

no ip ospf md5-authentication key-id

Command Default

No authentication.

Parameters

key-activation-wait-time *wait-time*

Sets the time that OSPFv2 waits before activating a new MD5 key. This parameter provides a graceful transition from one MD5 key to another without disturbing the network. All new packets transmitted after the wait time ends use the newly configured MD5 Key. OSPFv2 packets that contain the old MD5 key are accepted for up to five minutes after the new MD5 key is in operation. Valid values range from 0 to 14400 seconds.

key-id

Sets MD5 key.
id

Identifies the MD5 key ID. Valid values range from 1 and 255.

key *password*

Specifies the MD5 authentication ID and sets a password.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to set or reset the MD5 password and/or authentication change hold time on the interface to which you are connected.

By default, the authentication key is encrypted. If you want the authentication key to be in clear text, insert a 0 between authentication-key and string. The software adds a prefix to the authentication key string in the configuration. For example, the following portion of the code has the encrypted code "2".

Enter **no ip ospf md5-authentication key-id** to disable this configuration.

Note
MD5 passwords cannot have ASCII character 32 ('SPACE') as a part of the password string.

Examples

The following example sets the time that OSPFv2 waits before activating a new MD5 key to 240 seconds on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf md5-authentication key-activation-wait-time 240
```

The following example sets the MD5 key ID to 22 and a password “myospfpassword” on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf md5-authentication key-id 22 key myospfpassword
```

ip ospf mtu-ignore

Enables or disables maximum transmission unit (MTU) match checking.

Syntax

ip ospf mtu-ignore

no ip ospf mtu-ignore

Command Default

Enabled

Modes

Interface subtype configuration mode

Usage Guidelines

In default operation, the IP MTU on both sides of an OSPFv2 link must be the same, and a check of the MTU is performed when Hello packets are first exchanged.

The **no** form of the command disables MTU-match checking on a specific interface.

Examples

The following example disables MTU-match checking on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# no ip ospf mtu-ignore
```

The following example enables MTU-match checking on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf mtu-ignore
```

ip ospf network

Configures the network type for the interface. Point-to-point can support unnumbered links, which requires less processing by OSPF.

Syntax

ip ospf network { **broadcast** | **non-broadcast** | **point-to-point** }

no ip ospf network

Command Default

Network type is broadcast.

Parameters

broadcast

Network type is broadcast.

non-broadcast

Network type is non-broadcast. An interface can be configured to send OSPF traffic to its neighbor as unicast packets rather than multicast packets.

point-to-point

Network type is point-to-point.

Modes

Interface subtype configuration mode

Usage Guidelines

On a non-broadcast interface, the devices at either end of the interface must configure non-broadcast interface type and the neighbor IP address. There is no restriction on the number of devices sharing a non-broadcast interface.

To configure an OSPF interface as a non-broadcast interface, the feature must be enabled on a physical interface or a VE, following the **ip ospf area** statement, and then specify the IP address of the neighbor in the OSPF configuration. The non-broadcast interface configuration must be done on the OSPF devices at either end of the link.

The **no** form of the command removes the network-type configuration.

Examples

The following example configures an OSPFv2 point-to-point link on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf network point-to-point
```

The following example configures an OSPFv2 broadcast link on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf network broadcast
```

ip ospf passive

Sets a specific OSPFv2interface to passive.

Syntax

ip ospf passive

no ip ospf passive

Command Default

All OSPF interfaces are active.

Modes

Interface subtype configuration mode

Usage Guidelines

Passive interfaces accept and process all OSPF protocol traffic, but they do not send any traffic.

You might want to set an interface to passive mode if:

- You are planning to use the router mostly for debugging purposes.
- The router is a stub and does not route traffic.

The **no** form of the command sets an interface back to active.

Examples

The following example sets a specific OSPFv2 Ethernet interface to passive.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf passive
```

ip ospf priority

Configures priority for designated router (DR) election.

Syntax

ip ospf priority *value*

no ip ospf priority

Command Default

The default value is 1.

Parameters

value

Priority value. Valid values range from 0 through 255.

Modes

Interface subtype configuration mode

Usage Guidelines

The OSPFv2 router assigned the highest priority becomes the designated router, and the OSPFv2 router with the second-highest priority becomes the backup router.

The **no** form of the command restores the default value.

Examples

The following example sets a priority of 10 for the OSPFv2 router that is connected to an OSPFv2 Virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ipv6 ospf priority 10
```

ip ospf retransmit-interval

Configures the retransmit interval. The retransmit interval is the time between Link-State Advertisement (LSA) retransmissions to adjacent routers for a given interface.

Syntax

ip ospf retransmit-interval *interval*

no ip ospf retransmit-interval

Command Default

The interval is 5 seconds.

Parameters

interval

Retransmit interval in seconds. Valid values range from 0 through 3600 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command resets the retransmit interval to its default.

Examples

The following example sets the retransmit interval to 8 for all OSPFv2 devices on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf retransmit-interval 8
```

ip ospf transmit-delay

Configures transmit delay for link-update packets. The transmit delay is the estimated time required for OSPFv2 to send link-state update packets on the interface to which you are connected.

Syntax

ip ospf transmit-delay *value*

no ip ospf transmit-delay

Command Default

The transmit delay is set to 1 second.

Parameters

value

Transmit delay in seconds. Valid values range from 0 through 3600 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command restores the default value.

Examples

The following example sets a transmit delay of 25 seconds for devices on a specific OSPFv2 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip ospf transmit-delay 25
```

ip pim dr-priority

Configures the designated router (DR) priority on IPv4 interfaces.

Syntax

ip pim dr-priority *priority-value*

no ip pim dr-priority *priority-value*

Command Default

The default DR priority value is 1.

Parameters

priority-value

Specifies the DR priority value as an integer. The range is 0 through 65535.

Modes

Interface configuration mode

Usage Guidelines

The **no** form of this command restores the default DR priority value, 1.

You must enable PIM globally before you enable it on an interface.

You can configure the **ip pim dr-priority** command in either Dense mode (DM) or Sparse mode (SM).

If more than one device has the same DR priority on a subnet (as in the case of default DR priority on all), the device with the numerically highest IP address on that subnet is elected as the DR.

The DR priority information is used in the DR election only if all the PIM devices connected to the subnet support the DR priority option. If at least one PIM device on the subnet does not support this option, the DR election falls back to the backwards compatibility mode in which the device with the numerically highest IP address on the subnet is declared the DR regardless of the DR priority values.

Examples

This example configures a DR priority value of 50.

```
device(config)# interface ethernet 1/1
device(config-if-e10000-1/1)# ip pim dr-priority 50
```

ip pim snooping enable

Enables IP PIM snooping on a VLAN.

Syntax

ip pim snooping enable

no ip pim snooping enable

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of the command disables PIM snooping on the VLAN.

Use this command to enable Layer 2 PIM snooping on a VLAN. You must enable IGMP snooping on the interface before enabling PIM snooping.

Examples

The following example enables PIM snooping on a VLAN.

```
device(config)# vlan 1
device(config-vlan-1)# ip pim snooping enable
```

ip pim-sparse

Enables or disables Protocol Independent Multicast Sparse Mode on port channels, physical or VE interfaces.

Syntax

ip pim-sparse

no ip pim-sparse

Command Default

Protocol Independent Multicast (PIM) is not enabled on an interface.

Modes

Interface subtype configuration mode

Usage Guidelines

PIM must be enabled on the device before enabling PIM-sparse. PIM-sparse can be enabled on interfaces

Enter **no ip pim-sparse** to disable this feature.

Examples

To enable PIM Sparse Mode on a virtual Ethernet (VE) interface:

```
device(config)# int ve 1
device(config-if-Ve-1)# ip pim-sparse
```

To enable PIM Sparse Mode on a router port:

```
device(config)# int eth 1/1
device(config-if-eth-1/1)# ip pim-sparse
```

ip pim ttl-threshold

Sets the IP PIM time to live (TTL) threshold.

Syntax

ip pim ttl-threshold *value*

no ip pim ttl-threshold

Command Default

The default value is 1.

Parameters

priority value

Specifies the TTL threshold value. The range is 1 to 64.

Modes

Interface configuration mode

Usage Guidelines

The TTL threshold defines the minimum value required in a packet for it to be forwarded out of the interface after the TTL has been decremented.

For example, if the TTL for an interface is set at 10, only those packets that enter with a TTL value of 11 or more are forwarded through the TTL-10 interface. With a default TTL threshold of 1, only packets ingressing with a TTL of 2 or greater are forwarded. The TTL threshold only applies to routed interfaces and is ignored by switched interfaces. Possible TTL values are 1 to 64. The default TTL value is 1.

The **no** form of the command restores the default TTL threshold 1.

Examples

The following example sets the TTL value.

```
device(config)# interface ethernet 1/1
device(config-if-eth-1/1)# ip pim ttl-threshold 50
```

ip port (telemetry)

Specifies the IPv4 address and port of a telemetry collector.

Syntax

ip *ipv4-address* **port** *port-number*

no ip

Command Default

The IPv4 port is not designated.

Parameters

ipv4-address

Specifies the IPv4 address of a telemetry collector.

port *port-number*

Specifies the port.

Modes

Telemetry-collector configuration mode

Usage Guidelines

To remove the IP/port configuration from the telemetry collector, use the **no** form of this command.

Examples

The following example specifies the telemetry destination IP address and port.

```
device# configure terminal
device(config)# telemetry collector collector_1
device(config-collector-collector_1)# ip 10.168.112.10 port 1
```

ip policy route-map

Enables policy-based routing (PBR).

Syntax

ip policy route-map *map-name*

no ip policy route-map *map-name*

Command Default

PBR is not enabled.

Parameters

map-name

Specifies the name of the route map.

Modes

Interface configuration mode

Port-channel configuration mode

Virtual interface configuration mode

Usage Guidelines

The **no** form of the command disables PBR.

Examples

The following example enables PBR on a specific interface.

```
device# configure terminal
device(config)# route-map test-route permit 99
device(config-route-map-test-route/permit/99)# match ip address acl 99
device(config-route-map-test-route/permit/99)# set ip next-hop 192.168.3.1
device(config-route-map-test-route/permit/99)# exit
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip policy route-map test-route
```

ip prefix-list

Configures an IP prefix list instance.

Syntax

ip prefix-list *name* **seq** *sequence-number* { **deny** *ip-prefix/prefix-length* | **permit** *ip-prefix/prefix-length* } [**ge** *ge-value*] [**le** *le-value*]

no ip prefix-list *name*

Parameters

name

Permitted values are between 1 and 32 characters. Although the first character must be alphabetic, the others can be alphanumeric, underscores (_) or minus signs (-).

deny *ip-prefix/prefix-length*

Denies a route specified in the prefix list. The prefix list matches only on the specified prefix and prefix length, unless you use the **ge** *ge-value* or **le** *le-value* parameters.

permit *ip-prefix/prefix-length*

Permits a route specified in the prefix list. The prefix list matches only on the specified prefix and prefix length, unless you use the **ge** *ge-value* or **le** *le-value* parameters.

ge *ge-value*

Specifies the minimum prefix length to be match. The range is from *ge-value* to 32.

le *le-value*

Specifies the maximum prefix length to be matched. The range is from the *le-value* to the *prefix-length* parameter.

seq *sequence-number*

Specifies an IPv4 prefix list sequence number. If you do not specify a sequence number, the software numbers them in increments of 5, beginning with prefix list entry 5. The device interprets the prefix list entries in numerical order, beginning with the lowest sequence number.

Modes

Global configuration mode

Usage Guidelines

Enter **no ip prefix-list** *name* to disable this feature.

The *ge-value* or *le-value* you specify must meet the following condition for *prefix-length* : ge-value <= le-value <= 32

If you do not specify *le-value* **ge** *ge-value* or **le** *le-value* , the prefix list matches only on the exact prefix you specify with the *ip-prefix/prefix-length* parameter.

Examples

This example denies routes on 1.2.0.0/8, where the subnet mask length must be greater than or equal to 20 and less than or equal to 28, and permits routes on 10.1.0.0/16. A name is also assigned to this configuration.

```
device# config
device(config)#
device(config)# ip prefix-list test deny 10.2.0.0/8 ge 20 le 28 description deny-internal-
ip-range
device(config)# ip prefix-list test permit 10.1.0.0/16 description allow-internal-ip-range
```

ip proxy-arp

Enables Proxy Address Resolution Protocol (APR) on an interface.

Syntax

ip proxy-arp

no ip proxy-arp

Command Default

Proxy ARP is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Proxy ARP enables a device to answer ARP requests from devices in one network on behalf of devices in another network. Because ARP requests are MAC-layer broadcasts, they reach only the devices that are directly connected to the sender of the ARP request. Therefore, ARP requests do not cross routers.

The **no** form of the command disables Proxy ARP on an interface.

Examples

The following example enables Proxy ARP on a specified interface.

```
device(config)# interface ethernet 3/4
device(conf-if-eth-3/4)# ip proxy-arp
```

The following example disables Proxy ARP on a specified interface.

```
device(config)# interface ethernet 3/4
device(conf-if-eth-3/4)# no ip proxy-arp
```

ip receive access-group

Applies an IPv4 access control list (ACL) at global configuration level. Such *receive-path ACLs* filter incoming route-processor traffic according to rules that you create, but do not filter data-path traffic.

Syntax

ip receive access-group *acl-name*

ip receive access-group *acl-name* **sequence** *seq-number*

no ip receive access-group *acl-name*

Command Default

No receive-path ACLs are applied.

Parameters

acl-name

Specifies the name of the standard or extended IP access list.

sequence *seq-number*

Specifies the sequence of the rACL you are applying. Values range from 1 through 2047.

Modes

Global configuration mode

Usage Guidelines

For both interface ACLs and receive-path ACLs, you use identical commands to create the ACLs. You also use identical commands to define permit/deny/hard-drop rules in the ACLs. The only variance is the command you use to apply the ACL:

- To apply an interface ACL—from an interface-subtype configuration mode—you use the { **ip** | **ipv6** | **mac** } **access-group** command.
- To apply a receive-path ACL—from global configuration mode—you use the { **ip** | **ipv6** } **receive access-group** command.

You can apply a maximum of 400 receive-path ACLs to a device, as follows:

- 200 IPv4 receive-path ACLs
- 200 IPv6 receive-path ACLs

To remove a receive-path ACL, enter the **no** form of this command.

Examples

The following example creates an IPv4 extended ACL, defines rules in the ACL, and applies it as a receive-path ACL.

```
device(config)# ip access-list extended ipv4-receive-acl-example
device(conf-ipacl-ext)# hard-drop tcp host 10.0.0.1 any count
device(conf-ipacl-ext)# hard-drop udp any host 20.0.0.1 count
device(conf-ipacl-ext)# permit tcp host 10.0.0.2 any eq telnet count
device(conf-ipacl-ext)# permit tcp host 10.0.0.2 any eq bgp count

device(conf-ipacl-ext)# exit
device(config)# ip receive access-group ipv4-receive-acl-example
```

The following example creates two IPv4 extended ACLs, defines rules in the ACLs, and applies them as receive-path ACLs—specifying the priority of each ACL.

```
device#configure terminal
device(config)# ip access-list extended test-racl-1
device(conf-ipacl-ext)# deny ip 2.2.2.2/32 1.1.1.1/32
device(config)# ip access-list extended test-racl-2
device(conf-ipacl-ext)# permit ip 2.2.2.2/32 any
device(conf-ipacl-ext)# exit

device(config)#ip receive access-group test-racl-1 seq 10
device(config)#ip receive access-group test-racl-2 seq 20
```

ip route

Adds a static route to the IP routing table.

Syntax

ip route *dest-ip-addr* [**next-hop-vrf** *next-vrf-name*] *next-hop-address* [*metric*] [**distance** *distance*] [**tag** *tag-number*] [**name** *name-value*]

ip route *dest-ip-addr* { **ethernet** *slot/port* | **port-channel** *number* | **ve** *ve-number* } [*metric*] [**distance** *distance*] [**tag** *tag-number*] [**name** *name-value*]

ip route *dest-ip-addr* **null 0** [*metric*] [**distance** *distance*] [**tag** *tag-number*] [**name** *name-value*]

ip route next-hop-recursion

no ip route *dest-ip-addr* [**next-hop-vrf** *next-vrf-name*] *next-hop-address*

no ip route *dest-ip-addr* { **ethernet** *slot/port* | **ve** *ve-number* }

no ip route *dest-ip-addr* **null 0**

no ip route next-hop-recursion

Parameters

next-hop-vrf *vrf-name*

Specifies the name of the non-default VRF to be used for as the next-hop gateway.

dest-ip-addr

Specifies the destination IPv4 address and mask in the format A.B.C.D/L (where "L" is the prefix length of the mask).

next-hop-addr

Specifies the IPv4 address of the next hop.

ethernet *slot* **/** *port*

Specifies the destination Ethernet port.

next-hop-vrf *next-vrf-name*

VRF name of the next hop.

port-channel *number*

Specifies a port-channel interface.

ve *vlan-id*

Specifies the outgoing interface type as VE.

null 0

Configures the Layer 3 switch to drop IP packets to a specific network or host address by configuring a "null" (sometimes called "null0") static route for the address.

metric

Specifies the cost metric of the route. Valid values range from 1 through 16. The default is 1.

distance *distance*

Specifies the administrative distance of the route. When comparing otherwise equal routes to a destination, an SLX-OS device prefers lower administrative distances over higher ones. Valid values range from 1 through 254. The default is 1.

tag *tag-number*

Specifies the tag value of the route to use for route filtering with a route map. Valid values range from 0 through 4294967295. The default is 0.

next-hop-recursion

Specifies that if the next hop for a static route is reachable, then that route is added to the routing table.

name *name-value*

Specifies the name to be assigned to this IP route. This field can be used to assign a meaningful, human readable description to this route configuration. Maximum length 127 characters.

Modes

Global configuration mode

VRF configuration mode

Usage Guidelines

The **no** form of the command followed by the route identifier removes a static route.

If you do not want to specify a next-hop IP address, you can instead specify a physical or virtual interface on the SLX-OS device. If you specify an Ethernet port, the device forwards packets destined for the static route's destination network to the specified interface. Conceptually, this feature makes the destination network like a directly connected network, associated with an SLX-OS device interface.

The port or virtual interface you use for the static route's next hop must have at least one IP address configured on it. The address does not need to be in the same subnet as the destination network.

For a default route, use the following as the destination IP address 0.0.0.0/0.

You can create a null route for traffic for traffic that should not be forwarded. To create a null route, use the key phrase **null 0** as the next hop.

Examples

The following example configures a static route to 10.95.7.0 addresses, using 10.95.6.157 as the next-hop gateway.

```
device(config)# ip route 10.95.7.0/24 10.95.6.157
```

The following example configures a default route to next-hop IP address 10.24.4.1.

```
device(config)# ip route 0.0.0.0/0 10.24.4.1
```

The following example configures a static route with an Ethernet interface as the destination, and assigns a name to it.

```
device(config)# ip route 192.128.2.69/24 ethernet 4/1 name route-sj-01
```

The following example configures a null static route to drop packets destined for network 10.157.22.x.

```
device(config)# ip route 10.157.22.0/24 null 0
```

The following example configures non-recursive lookup in the default VRF.

```
device(config)# ip route next-hop-recursion
```

The following example configures non-recursive lookup in a non-default VRF named red.

```
device(config)# vrf red
device(config-vrf-red)# address-family ipv4 unicast
device(config-vrf-red-ipv4-unicast)# ip route next-hop-recursion
```

ip route next-hop-recursion

Enables recursive lookup for IPv4 next-hop routes.

Syntax

ip route next-hop-recursion

no ip route next-hop-recursion

Command Default

By default, next-hop recursive lookups are enabled.

Modes

Global configuration mode

VRF configuration mode

Usage Guidelines

The **no** form of the command disables recursive lookups.

Examples

The following example disables recursive lookups in the default VRF.

```
device# configure terminal
device(config)# no ip route next-hop-recursion
```

The following example disables recursive lookups in a non-default VRF.

```
device(config) vrf red
device(config-vrf-red)# address-family ipv4 unicast
device(config-vrf-red-ipv4-unicast)no ip route next-hop-recursion
```

The following example re-enables recursive lookups in the default VRF.

```
device# configure terminal
device(config)# ip route next-hop-recursion
```

The following example re-enables recursive lookups in a non-default VRF.

```
device(config) vrf red
device(config-vrf-red)# address-family ipv4 unicast
device(config-vrf-red-ipv4-unicast)ip route next-hop-recursion
```

ip route static bfd

Configures a Bidirectional Forwarding Detection (BFD) session for a static IPv4 route.

Syntax

ip route static bfd *dest-ip-address source-ip-address* [**interval** *transmit-time* **min-rx** *receive-time* **multiplier** *number*]

Command Default

By default, BFD is not configured for an IPv4 static route.

Parameters

dest-ip-address

Specifies the IPv4 address of the BFD neighbor.

source-ip-address

Specifies the source IPv4 address.

interval *transmit-time*

Specifies the interval, in milliseconds, a device waits to send a control packet to BFD peers. Valid values range from 50 through 30000. The default is 300 milliseconds.

min-rx *receive-time*

Specifies the interval, in milliseconds, a device waits to receive a control packet from BFD peers. Valid values range from 50 through 30000. The default is 300 milliseconds.

multiplier *number*

Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD determines that the connection to that peer is not operational. Valid values range from 3 through 50. The default is 3.

Modes

Global configuration mode

Address-family IPv4 unicast VRF configuration mode

Usage Guidelines

The local device needs the **interval** *transmit-time* and **min-rx** *receive-time* variables. The actual values in use will be the negotiated values.

For single-hop static BFD sessions, the interval value is taken from the outgoing interface. For multi-hop BFD sessions, if the configured **interval** and **min-rx** parameters conflict with those of an existing session, the lower values are used.

Examples

This example configures a BFD session on an IPv4 static route.

```
 device# configure terminal
device(config)#)# ip route static bfd 10.0.2.1 10.1.1.1 interval 500 min-rx 500
multiplier 5
```

This example configures a BFD session on an IPv4 static route in a non-default VRF instance.

```
device# configure terminal
device(config)# vrf orange
device(config-vrf-orange)# address-family ipv4 unicast
device(vrf-ipv4-unicast)# ip route static bfd 10.2.2.2 10.3.3.3 interval 600 min-rx 700
multiplier 10
```

ip route static bfd holdover-interval

Sets the time interval for which BFD session DOWN notifications are delayed before an IP static route is notified that a BFD session is down.

Syntax

ip route static bfd holdover-interval *time*

no ip route static bfd holdover-interval

Command Default

By default, the BFD holdover interval is 0 seconds.

Parameters

time

Specifies the BFD holdover-time interval in seconds. Valid values range from 1 through 30. The default is 0.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of the command to revert to the default value of 0.

If the BFD session is restored within the specified time interval, no DOWN notification is sent.

Holdover interval values are configured globally and apply to all VRFs.

Examples

This example sets the BFD holdover interval globally for IP static routes to 15.

```
device# configure terminal
device(config)# ip route static bfd holdover-interval 15
```

This example removes the configured BFD holdover interval for IP static routes.

```
device# configure terminal
device(config)# no ip route static bfd holdover-interval
```

ip router-id

Changes the router ID that is already in configured.

Syntax

ip router-id *A.B.C.D*

no ip router-id *A.B.C.D*

Parameters

A.B.C.D

Specifies the IPv4 address that you want as the router ID.

Modes

Global configuration mode

VRF configuration mode

Usage Guidelines

Though a device has IP addresses assigned to various interfaces, some routing protocols identify the device by the router ID rather than the IP addresses assigned to the interfaces connected by the protocol.

The **no** form of the command removes the configured router ID and restores the default router ID.

Examples

The following example specifies the router ID as 192.158.1.2.

```
device# configure terminal
device(config)# ip router-id 192.158.1.2
```

ip router isis

Enables Intermediate System-to-Intermediate System (IS-IS) routing at the interface level.

Syntax

ip router isis

Command Default

Disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Use the **no** form of this command to disable IS-IS routing for the interface.

Examples

The following example enables IS-IS routing for an interface Ethernet.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ip router isis
```

ip source-guard enable

Enables IP Source Guard, which provides filtering on an untrusted Layer 2 access port.

Syntax

ip source-guard enable

no ip source-guard enable

Command Default

By default, IP Source Guard is not enabled.

Modes

Global configuration mode

Usage Guidelines

IP Source Guard provides source IP address filtering on a Layer 2 port to prevent a malicious host from impersonating a legitimate host by assuming the IP address of the legitimate host.

Use the **no** form of the command to disable IP Source Guard.

ip subnet-broadcast-acl

Applies an IP broadcast ACL (bACL) to an interface.

Syntax

ip subnet-broadcast-acl *acl-name*

no ip subnet-broadcast-acl *acl-name*

Command Default

No bACL is applied.

Parameters

acl-name

Specifies the standard or extended bACL.

Modes

Interface subtype configuration mode

Usage Guidelines

Broadcast ACLs are not supported on SLX 9150 or SLX 9250 devices.

The **no** form of this command removes a bACL from the interface.

Examples

The following example applies a bACL to a physical interface.

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# ip subnet-broadcast-acl bacl_10
```

The following example applies a bACL to a VE.

```
device# configure terminal
device(config)# interface ve 50
device(config-ve-50)# ip subnet-broadcast-acl bacl_20
```

ip subnet-rate-limit

Configures the Committed Information Rate (CIR) and Committed Burst Size (CBS) for IPv4 and IPv6 subnet trap frames.

Syntax

ip subnet-rate-limit cir *cir-rate* [**cbs** *cbs-size*]

no ip subnet-rate-limit

Command Default

By default, CIR and CBS are not configured.

Parameters

cir *cir-rate*

(Required) Defines the value of the CIR. Acceptable values range from 0 to 10,000 Kbps.

cbs *cbs-size*

Defines the value of the CBS. Acceptable values range from 0 to 32 KB.

Modes

Control plane configuration mode

Usage Guidelines

The CIR is the maximum number of bits that a port can receive or send during a one-second interval. The rate of the traffic that matches the traffic policing policy cannot exceed the CIR. The CIR represents a portion of interface bandwidth, expressed in bits per second (bps), and it cannot exceed port bandwidth. CIR-defined traffic that does not use the available CIR accumulates credit up to the amount defined by the CBS. This credit is the number of bytes that can be used to accommodate temporary bursts in traffic that exceed the CIR.

(SLX 9150 and SLX 9250) By default, IPv4 and IPv6 subnet trap frames are diverted to a separate queue (queue number 9). You can use the **ip subnet-rate-limit** command to further limit the rate of IPv6 subnet trap frames .

(SLX 9540 and SLX 9640) By default, IPv4 and IPv6 subnet trap frames are rate-limited to 10,000 Kbps. You can use the **ip subnet-rate-limit** command to further limit IPv4 and IPv6 subnet trap frames.

Examples

The following example configures the CIR to 134 Kbps and the CBS to 34 KB.

```
device# configure terminal
device(config)# control-plane
device(config-control-plane)# ip subnet-rate-limit cir 134 cbr 34
```

ip vrrp-extended auth-type

Configures the type of authentication used on a Virtual Router Redundancy Protocol Extended (VRRP-E) interface.

Syntax

ip vrrp-extended auth-type md5-auth *auth-text*

no ip vrrp-extended auth-type md5-auth

Command Default

No authentication is configured for a VRRP-E interface.

Parameters

auth-type

Authentication type used to verify the *password*.

md5-auth *auth-text*

Configures MD5 authentication on the interface. The maximum length of the text string is 64 characters.

Modes

Virtual Ethernet (VE) interface configuration mode

Usage Guidelines

This configuration is for VE interfaces only.

If the **md5-auth** option is configured, syslog and SNMP traps are generated if a packet is being dropped due to MD5 authentication failure. Using MD5 authentication implies that the software does not need to run checksum verification on the receiving device and can rely on the authentication code (message digest 5 algorithm) to verify the integrity of the VRRP-E message header.

The **no** form of this command removes the VRRP-E authentication from the interface.

Note
MD5 passwords cannot have ASCII character 32 ('SPACE') as a part of the password string.

Examples

The following example configures MD5 authentication on VE interface 20.

```
device(config)# protocol vrrp-extended
```

```
device(config)# interface ve 20
device(config-if-Ve-20)# ip vrrp-extended auth-type md5-auth lyk28d3j
```

ip

Syntax

ip [**dhcp** | **address**]

ip dhcp

ip address *ip-address/mask* **gw** *gw-ip-address*

no ip dhcp

no ip address *ip-address/mask* **gw** *gw-ip-address*

Parameters

dhcp

The IP address of the BMC Management Interface is assigned by an external DHCP server.

address *ip-address* **/** *mask*

The IP address of the BMC Management Interface is assigned manually by assigning an IPv4 address and a netmask.

gw *gw-ip-address*

The gateway IP address for the BMC Management Interface is assigned manually. This is an IPv4 address.

Modes

BMC Interface Configuration mode

Usage Guidelines

The **no** format of this command resets the interface to the following IPv4 address and gateway configuration. IPv4 address **192.168.11.1/24** is assigned with the default gateway IPv4 address of **0.0.0.0**.

This preconfigured *ip-address/mask* and *gateway-ip-address* is assigned for both the **no ip dhcp** and **no ip address <ip-address>/<mask> gw <gw-ip-address>** commands.

Examples

This example shows the manual configuration of an IPv4 address to the BMC Management Interface with ID 0.

```
SLX # configure terminal
SLX (config)# bmc
SLX (config-bmc)# interface management 0
SLX (config-bmc-mgmt-0)# ip address 10.9.9.10/24 gw 10.9.9.2
```

```
SLX (config-bmc-mgmt-0)# do show running-config bmc interface 0
bmc
 interface management 0
  no shutdown
  ip address 10.9.9.23/24 gw 10.9.9.2
 !
!
SLX (config-bmc-mgmt-0)#
```

This example shows how to disable a manually configured IPv4 address for the BMC Management Interface.

```
SLX # configure terminal
SLX (config)# bmc
SLX (config-bmc)# interface management 0
SLX (config-bmc-mgmt-0)# no ip address 10.9.9.10/24 gw 10.9.9.2
SLX (config-bmc-mgmt-0)# do show running-config bmc interface 0
bmc
 interface management 0
  shutdown
 !
!
SLX (config-bmc-mgmt-0)#
```

This example shows how to configure the BMC Management Interface to receive its IPv4 address from an external DHCP server.

```
SLX # configure terminal
SLX (config)# bmc
SLX (config-bmc)# interface management 0
SLX (config-bmc-mgmt-0)# ip dhcp
```

ipv6 access-group

Applies rules specified in an IPv6 access control list (ACL) to traffic entering an interface.

Syntax

ipv6 access-group *ACLname* **in** [**routed**]

no ipv6 access-group *ACLname* **in** [**routed**]

Parameters

ACLname

Specifies the name of the standard or extended IPv6 access list.

in

Applies the ACL to incoming switched and routed traffic.

routed

Applies this ACL only on Routed traffic.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to apply an IPv6 ACL to one of the following interface types:

- User interfaces
  - Physical interfaces
  - Port-channels (LAGs)
  - Virtual Ethernet (VE) (attached to a VLAN or to a bridge domain)
- The management interface

You can apply a maximum of five ACLs to a user interface, as follows:

- One ingress MAC ACL—if the interface is in switchport mode
- One egress MAC ACL—if the interface is in switchport mode
- One ingress IPv4 ACL
- One egress IPv4 ACL
- One ingress IPv6 ACL

You can apply a maximum of two ACLs to the management interface, as follows:

- One ingress IPv4 ACL
- One ingress IPv6 ACL

You can apply an ACL to multiple interfaces.

To remove an ACL from an interface, enter the **no** form of this command.

The following guidelines apply to the `routed` keyword:

- The `routed` keyword is applicable for the following devices:
  - SLX 9150
  - SLX 9250
  - SLX 9740
  - Extreme 8520
  - Extreme 8720
  - Extreme 8820
- The `routed` keyword is not applicable for the following devices:
  - SLX 9540
  - SLX 9640
- The `routed` keyword is applicable only in the ingress direction.
- Applies only to the Virtual Ethernet (VE) interfaces.

Examples

The following example applies an IPv6 ACL on an Ethernet interface to incoming traffic.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# ipv6 access-group ipv6_acl_7 in
```

The following example removes an IPv6 ACL from an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# no ipv6 access-group ipv6_acl_7 in
```

The following example applies an IPv6 ACL on an Virtual Ethernet interface to incoming routed traffic.

```
device# configure terminal
device(config)# interface Ve 10
device(conf-if-Ve-10)# ipv6 access-group ipv6_acl_7 in routed
```

ipv6 access-list

Creates a standard or extended IPv6 access control list (ACL). In ACLs, you can define rules that permit or deny network traffic based on criteria that you specify.

Syntax

ipv6 access-list { **standard** | **extended** } *ACLname*

no ipv6 access-list { **standard** | **extended** } *ACLname*

Parameters

standard | **extended**

Specifies one of the following types of access lists:
standard

Contains rules that permit or deny traffic based on source addresses that you specify. The rules are applicable to all ports of the specified addresses.

extended

Contains rules that permit or deny traffic according to source and destination addresses, as well as other parameters. For example, you can also filter by port, protocol (TCP or UDP), and TCP flags.

ACLname

Specifies an ACL name unique among all ACLs (Layer 2 and Layer 3). The name can be up to 63 characters in length, and must begin with an alphanumeric character. No special characters are allowed, except for the underscore and hyphen.

Modes

Global configuration mode

Usage Guidelines

An ACL name can be up to 63 characters long, and must begin with a–z, A–Z or 0–9. You can also use underscore (_) or hyphen (-) in an ACL name, but not as the first character.

After you create an ACL, use the **seq** command to create filtering rules for that ACL.

An ACL starts functioning only after:

- Applied to an interface, using the **{ ip | ipv6 | mac } access-group** command.
- Applied at device-level, using the **{ ip | ipv6 } receive access-group** command.

To delete an ACL, use the **no access-list** command. You can delete an ACL only after you first remove it from all interfaces to which it is applied, using the **no access-group** command.

Examples

The following example creates an IPv6 standard ACL:

```
device# configure
device(config)# ipv6 access-list standard stdV6ACL1
```

The following example creates an IPv6 extended ACL:

```
device# configure
device(config)# ipv6 access-list extended ipv6_acl_1
```

The following example creates rules on an IPv6 standard ACL:

```
device# configure
device(config)# ipv6 access-list standard stdV6ACL1
device(conf-ipv6-std)# seq 10 permit 2001:db8:85a3:0:0:8a2e:370:7334
device(conf-ipv6-std)# seq 11 deny any
```

The following example deletes an IPv6 ACL:

```
device# configure
device(config)# no ipv6 access-list standard stdV6ACL1
```

ipv6 address

Configure an IPv6 address for an interface.

Syntax

ipv6 address *pv6-prefix//prefix-length* [**secondary**] [**anycast** | **eui-64**]

no ipv6 address *pv6-prefix//prefix-length* [**secondary**] [**anycast** | **eui-64**]

ipv6 address *ipv6-address* **link-local**

no ipv6 address *ipv6-address* **link-local**

Parameters

ipv6-address

Specifies the IPv6 address.

ipv6-prefix

Specifies the IPv6 prefix address in this format: X:X::X:X/M.

prefix-length

A decimal value specifying the length of the IPv6 prefix.

secondary

Specifies that the address is a secondary address. A maximum of 256 secondary addresses can be configured.

anycast

Configures an address as an anycast address.

eui-64

Configures the global address with an EUI-64 interface ID in the low-order 64 bits. The interface ID is automatically constructed in IEEE EUI-64 format using the interface's MAC address.

Modes

Interface configuration mode

Port-channel configuration mode

Usage Guidelines

A secondary address cannot be configured on an interface unless the primary address is configured first.

The primary address cannot be deleted on an interface unless the secondary addresses are deleted first.

This command is not supported on loopback or management interfaces.

Examples

This example shows how to configure a primary, secondary global, or unique local IPv6 unicast address, including a manually configured interface ID:

```
device(config)# configure terminal
device(config)# interface ethernet 3/1
device(conf-if-eth-2/3)# ipv6 address 2001:db8:12d:1300:240z:d0ff:fe48:4672/64
```

This example shows how to remove the IPv6 unicast address, including a manually configured interface ID from an interface:

```
device(conf-if-eth-2/3)# no ipv6 address 2001:db8:12d:1300:240z:d0ff:fe48:4672/64
```

ipv6 anycast-address

Configures an anycast-gateway IPv6 address on an interface, which uses the gateway IPv6 address for the host.

Syntax

ipv6 anycast-address { *IPv6-address/ mask* }

no ipv6 anycast-address

Command Default

No address is configured.

Parameters

IPv6-address / mask

IPv6 address and mask.

Modes

interface configuration mode on a virtual Ethernet (VE) interface.

Usage Guidelines

An IPv4 and IPv6 anycast MAC address cannot be configured as the same MAC address.

Use the **no** form of this command to delete the configured IPv6 anycast address from the interface.

Examples

To configure an IPv6 address and mask on a virtual Ethernet (VE) interface:

```
device# configure terminal
device(config)# interface ve 10
device(config-Ve-10)# ipv6 anycast-address fe80::1234/64
```

To confirm the configuration in the running configuration:

```
device# show running-config interface ve 10
!
ipv6 snycast-address fe80::1234/64
!
```

show ipv6 dhcp relay

Displays the DHCPv6 delegated prefixes information for the complete system.

Syntax

show ipv6 dhcp relay

Parameters

None

Modes

Privileged EXEC mode

Usage Guidelines

None.

Examples

The following example shows how to display the DHCPv6 delegated prefixes for the complete system.

```
SLX-Router#show ipv6 dhcp relay
Current DHCPv6 Relay Agent State: Enabled
DHCPv6 enabled interface(s): ve 100 ve 101 ve 102 ve 103 ve 104 ve 105
DHCPv6 Relay Prefix Delegation Notification:
    Maximum Delegated Prefixes Allowed:20000
    Current Delegated Prefixes:4
```

ipv6 dhcp relay distance

Assigns the administrative distance to DHCPv6 Routes installed in RIB-IPv6 Route Table for the learned delegated prefixes on the interface.

Syntax

ipv6 dhcp relay distance *distance-value*

no ipv6 dhcp relay distance *distance-value*

Parameters

distance *distance-value*

The value of administrative distance configured. The default value is 10. Values can be in the range 1 - 255.

Modes

Interface Configuration Mode

Usage Guidelines

The **no** form of the command set the parameter to default value of 10.

Examples

The following example shows how to set the administrative distance value.

```
SLX(config)# interface Ve 5
SLX(config-Port-channel-1)# ipv6 dhcp relay distance 2
```

ipv6 dhcp relay address

Configures the IPv6 DHCP Relay address on a Layer 3 interface.

Syntax

ipv6 dhcp relay address *ipv6-addr* [**interface** *interface-type interface-name*] [**use-vrf** *vrf-name*]

no ipv6 dhcp relay address *ipv6-addr* [**interface** *interface-type interface-name*] [**use-vrf** *vrf-name*]

Parameters

ipv6-addr

IPv6 address of the DHCP server where the DHCP client requests are to be forwarded.

interface

This parameter specifies the outgoing interface, used when the relay address is a link-local or multicast address

interface-type

The type of interface - Ethernet or VE.

interface-name

The interface name or VE ID.

use-vrf

Use this option if the VRF where the DHCP server is located is different from the VRF of the interface where the client is connected.

vrf-name

VRF name.

Modes

Interface subtype configuration mode

Usage Guidelines

This command uses the IPv6 address of the DHCP server where the DHCP client requests are to be forwarded. You can configure the address on a virtual Ethernet (VE) or an Ethernet interface. You can configure up to 16 relay destination addresses on an interface.

Enter the command while in interface subtype configuration mode for a VE or Ethernet interface where you want to configure the IPv6 DHCP Relay. Use the **no** version of this command to remove the IPv6 DHCP Relay from the interface. If the **use-vrf** option is not used, it is assumed that the DHCP server and interface where the client is connected are on the same VRF.

If the relay address is a link local address or a multicast address, an outgoing interface must be configured for IPv6 relay to function. In instances where the server address is relayed to a different VRF compared to a client connected interface VRF, in addition to the relay address, you must also specify the user-vrf, otherwise IPv6 relay may not function correctly. IPv6 route leaking is also required for IPv6 reachability.

The **no** form of the command deletes the IPv6 DHCP Relay address from the interface.

Examples

To configure an IPv6 DHCP Relay address on a Ve interface:

```
device# config
device(config)# interface ve 100
device(config-Ve-100)# ipv6 dhcp relay address 2001::1122:AABB:CCDD:3344 use-vrf blue
```

To configure an IPv6 DHCP Relay address on an interface:

```
(config)# interface ethernet 2/3
device(conf-if-eth-2/3)# ipv6 dhcp relay address fe80::224:38ff:febb:e3c0  interface
ethernet 2/5
```

ipv6 dhcp relay distance

Assigns the administrative distance to DHCPv6 Routes installed in RIB-IPv6 Route Table for the learned delegated prefixes on the interface.

Syntax

ipv6 dhcp relay distance *distance-value*

no ipv6 dhcp relay distance *distance-value*

Parameters

distance *distance-value*

The value of administrative distance configured. The default value is 10. Values can be in the range 1 - 255.

Modes

Interface Configuration Mode

Usage Guidelines

The **no** form of the command set the parameter to default value of 10.

Examples

The following example shows how to set the administrative distance value.

```
SLX(config)# interface Ve 5
SLX(config-Port-channel-1)# ipv6 dhcp relay distance 2
```

ipv6 dhcp relay maximum-delegated-prefixes

Configures the maximum number of delegated prefixes that can be learned by the system.

Syntax

ipv6 dhcp relay maximum-delegated-prefixes *maximum-delegated-prefix-value*

no ipv6 dhcp relay maximum-delegated-prefixes

Parameters

maximum-delegated-prefixes *maximum-delegated-prefix-value*

The number of delegated prefixes configured at the global and interface levels. The default value is 8000 at global level and 1000 at the interface level. Values can be in the range 0 - 20,000.

Modes

Global Configuration mode

Interface Configuration Mode

Usage Guidelines

The **no** form of the command disables the ipv6 dhcp relay maximum-delegated-prefixes and sets to default values.

Examples

The following example shows how to configure DHCPv6 Prefix Delegation at the global level.

```
SLX(config)# ipv6 dhcp relay maximum-delegated-prefixes 20000
```

The following example shows how to configure DHCPv6 Prefix Delegation at an interface's level.

```
SLX(config)# interface Ethernet 0/1
SLX(conf-if-eth-0/1)#ipv6 dhcp relay maximum-delegated-prefixes 10000
```

ipv6 dns

Configures the DNS domain name and the primary and secondary name-server IPv6 addresses.

Syntax

ipv6 dns { **domain-name** *domain_name* | **name-server** *name_server* }

no ipv6 dns { **domain-name** *domain_name* | **name-server** *name_server* }

Parameters

domain-name *domain_name*

Specifies the DNS domain name.

name-server *name_server*

Specifies the IPv6 address of the primary and secondary name servers. Both the IPv6 and IPv4 addresses are supported.

Modes

Global configuration mode

Usage Guidelines

Your first run of **ipv6 dns name-server** specifies the default IP gateway address. Your second run of **ipv6 dns name-server** specifies the secondary IP gateway address.

Name servers can only be entered or removed one at a time. The newly entered name server will append to the existing name server.

To disable IP directed broadcasts for a specific domain, enter **no ipv6 dns domain-name** *domain_name*.

To delete a name-server definition, enter **no ipv6 dns name-server** *ipv6_address_of_name_server*.

Examples

The following example configures DNS.

```
device(config)# ipv6 dns domain-name mycompany.com
device(config)# ipv6 dns name-server 2001:db8:12d:1300:240z:d0ff:fe48:4672
```

ipv6 icmpv6 redirect

Enables IPv6 Internet Control Message Protocol (ICMP) Redirect messages, which request that packets be sent on an alternative route.

Syntax

ipv6 icmpv6 redirect

no ipv6 icmpv6 redirect

Command Default

ICMPv6 redirect messages are disabled by default.

Modes

Interface configuration mode

Usage Guidelines

Note
This command is only available on SLX 9640 and SLX 9540.

Note
This command is not supported on port-channel (PO)/virtual ethernet (VE) interfaces.

The **no** form of the command disables IPv6 ICMP Redirect messages.

User can disable ICMP redirect messages when traffic needs to be routed into and out of the same Layer 3 interface.

Examples

The following example enables IPv6 ICMP Redirect messages on an Ethernet interface.

```
device(config)# interface ethernet 2/5
device(conf-int-eth-2/5)# ipv6 icmpv6 redirect
```

ipv6 icmpv6 rate-limiting

Limits the rate at which IPv6 Internet Control Message Protocol version 6 (ICMPv6) messages are sent on a network.

Syntax

ipv6 icmpv6 rate-limiting *milliseconds*

no ipv6 icmpv6 rate-limiting

Command Default

This command is enabled on the management port and on the front-end ports.

Parameters

milliseconds

Time interval per ICMP packet. The range is from 1 through 4294967295 milliseconds. The default is 1000 milliseconds.

Modes

Interface configuration mode

Usage Guidelines

This is an interface-specific configuration.

The no form of this command reverts the rate limiting to the default settings.

Set the rate limiting to 0 to disable icmpv6 rate limiting.

Examples

The following example enables IPv6 ICMP rate-limiting on an Ethernet interface.

```
device(config)# interface ethernet 3/5
device(conf-int-eth-3/5)# ipv6 icmpv6 rate-limiting
```

ipv6 icmpv6 unreachable

Enables a Layer 3 device to respond to IPv6 ICMP unreachable messages.

Syntax

ipv6 icmpv6 unreachable

no ipv6 icmpv6 unreachable

Command Default

By default, the device does not respond to ICMP unreachable messages.

Modes

Interface configuration mode.

Usage Guidelines

Use the **no** form of the command to disable the feature.

Examples

The following example enables a device to respond to ICMP unreachable notifications to the indicated source.

```
device# configure terminal
device(config)# interface ve 2
device(config-int-ve-2)# ip address 200::1/64
device(config-int-ve-2)# ip icmp unreachable
```

ipv6 mld snooping enable

Enables IPv6 MLD (Multicast Listener Discovery) snooping for a VLAN or a bridge domain.

Syntax

ipv6 mld snooping enable

no ipv6 mld snooping enable

Command Default

By default, IPv6 MLD snooping is not enabled.

Modes

VLAN or bridge domain configuration mode

Usage Guidelines

The **no ipv6 mld snooping** form of the command disables MLD snooping.

Examples

The following example enables IPv6 MLD snooping for a VLAN.

```
device# configure terminal
device(config)# vlan 10
device(config-vlan-10)# ipv6 mld snooping enable
```

The following example enables IPv6 MLD snooping for a bridge domain.

```
device# configure terminal
device(config)# bridge-domain 10
device(config-bridge-domain-10)# ipv6 mld snooping enable
```

ipv6 mld snooping fast-leave

Enables MLD snooping fast-leave processing for a VLAN or a bridge domain.

Syntax

ipv6 mld snooping fast-leave

no ipv6 mld snooping fast-leave

Command Default

By default, fast-leave processing is disabled.

Modes

VLAN or bridge domain configuration mode

Usage Guidelines

The **no ipv6 mld snooping fast-leave** form of the command disables fast-leave processing.

Fast-leave processing allows the removal of an interface from the forwarding table without sending out group-specific queries to the interface.

Examples

The following example enables fast-leave processing on a VLAN.

```
device# configure terminal
device(config)# vlan 10
device(config-vlan-10)# ipv6 mld snooping ?
Possible completions:
    fast-leave   Fast Leave Processing
device(config-vlan-10)# ipv6 mld snooping fast-leave
```

The following example enables fast-leave processing on a bridge domain.

```
device# configure terminal
device(config)# bridge-domain 10
device(config-bridge-domain-10)# ipv6 mld snooping ?
Possible completions:
    fast-leave   Fast Leave Processing
device(config-bridge-domain-10)# ipv6 mld snooping fast-leave
```

ipv6 mld snooping last-member-query-interval

Sets the time limit for sending last member queries for a VLAN or bridge domain.

Syntax

ipv6 mld snooping last-member-query-interval *interval*

no ipv6 mld snooping last-member-query-interval

Command Default

By default, the query interval is 1000 milliseconds.

Parameters

interval

Specifies the time limit for sending last member queries. Valid values range from 100 milliseconds to 25500 milliseconds.

Modes

VLAN or bridge domain configuration mode

Usage Guidelines

Last member queries are sent when a multicast host is the last to leave a group. Queries are sent until a response is received or the last member query interval has expired.

The **no ipv6 mld snooping last-member-query-interval** form of the command restores the default interval of 1000 milliseconds.

Examples

The following example configures the last member query interval for a VLAN.

```
device# configure terminal
device(config)# vlan 10
device(config-vlan-10)# ipv6 mld snooping last-member-query-interval ?
Possible completions:
    <100-25500>   Last Member Query Interval value (Default: 1000ms)
device(config-vlan-10)# ipv6 mld snooping last-member-query-interval 3000
```

The following example configures the last member query interval for a bridge domain.

```
device# configure terminal
device(config)# bridge-domain 10
device(config-bridge-domain-10)# ipv6 mld snooping last-member-query-interval ?
Possible completions:
    <100-25500>   Last Member Query Interval value (Default: 1000ms)
device(config-bridge-domain-10)# ipv6 mld snooping last-member-query-interval 10000
```

ipv6 mld snooping mrouter interface

Configures a VLAN port member to be a multicast router (mrouter) port.

Syntax

ipv6 mld snooping mrouter interface [**ethernet** | **port-channel**]*interface_name*

no ipv6 mld snooping mrouter interface [**ethernet** | **port-channel**] *interface_name*

Command Default

By default, a VLAN port member is not an mrouter port.

Parameters

ethernet

Specifies the type of interface to configure.
interface_name

Specifies the Ethernet name in the following format: x/y, where x is the slot number and y is the interface (port) number. For example, 0/2.

port-channel

Specifies the type of interface to configure.
interface_name

Specifies the port channel name. For example, 10.200, where 10 is the port channel.

Modes

VLAN configuration mode

Usage Guidelines

The **no ipv6 mld snooping mrouter interface** form of the command removes the mrouter configuration.

Examples

The following example configures an Ethernet port as an mrouter port.

```
device# configure terminal
device(config)# vlan 10
device(config-vlan-10)# ipv6 mld snooping mrouter interface ?
Possible completions:
    Ethernet The list of Ethernet LIFs.
    Port-channel The list of port-channel LIFs.
device(config-vlan-10)# ipv6 mld snooping mrouter interface Ethernet 0/2
```

The following example removes the mrouter configuration.

```
device# configure terminal
device(config)# vlan 10
device(config-vlan-10)# no ipv6 mld snooping mrouter interface Ethernet 0/2
```

ipv6 mld snooping mrouter logical-interface

Configures a logical member port of a bridge domain to be a multicast router (mrouter) port.

Syntax

ipv6 mld snooping mrouter logical-interface [**ethernet** | **port-channel**] *logical_interface_name*

no ipv6 mld snooping mrouter logical-interface [**ethernet** | **port-channel**] *logical_interface_name*

Command Default

By default, a logical member port is not an mrouter port.

Parameters

ethernet

Specifies the type of interface to configure.
logical_interface_name

Specifies the Ethernet name in the following format: x/y, where x is the slot number and y is the interface (port) number. For example, 0/2.200.

port-channel

Specifies the type of interface to configure.
logical_interface_name

Specifies the port channel name. For example, 10.200, where 10 is the port channel.

Modes

Bridge-domain configuration mode

Usage Guidelines

The **no ipv6 mld snooping mrouter logical-interface** form of the command removes the mrouter configuration.

Examples

The following example configures an Ethernet port as an mrouter port.

```
device# configure terminal
device(config)# bridge-domain 10
device(config-bridge-domain-10)# ipv6 mld snooping mrouter logical-interface ?
Possible completions:
    Ethernet The list of Ethernet LIFs.
    Port-channel The list of port-channel LIFs.
```

```
device(config-bridge-domain-10)# ipv6 mld snooping mrouter logical-interface Ethernet
0/2.200
```

The following example removes the mrouter configuration.

```
device# configure terminal
device(config)# bridge-domain 10
device(config-bridge-domain-10)# no ipv6 mld snooping mrouter logical-interface Ethernet
0/2.200
```

ipv6 mld snooping querier enable

Activates the MLD snooping querier function for a VLAN or bridge domain.

Syntax

ipv6 mld snooping querier enable

no ipv6 mld snooping querier enable

Command Default

By default, the snooping querier is disabled.

Modes

VLAN or bridge domain configuration mode

Usage Guidelines

The **no ipv6 mld snooping querier enable** form of the command disables the querier function.

In a subnet, one multicast router is elected as an MLD querier. The MLD querier sends out the following types of queries to hosts.

- Multicast Listener General query: (MLD v1, v2) Asks whether any host is listening to any group.
- Multicast Listener Group-specific query: (MLD v1, v2) Asks whether any host is listening to a specific multicast group. This query is sent in response to a host leaving the multicast group. The router can quickly determine whether any remaining hosts are interested in the group.
- Multicast Listener Group-and-source-specific query: (MLD v2) Asks whether any host is listening to group multicast traffic from a specific multicast source. This query is sent in response to a host indicating that it is not interested in receiving group-specific multicast traffic from the multicast source. The router can quickly determine whether any remaining hosts are interested in receiving group multicast traffic from that source.

Examples

The following example enables the querier function for a VLAN.

```
device# configure terminal
device(config)# vlan 10
device(config-vlan-10)# ipv6 mld snooping querier ?
Possible completions:
    enable Enable snooping querier
device(config-vlan-10)# ipv6 mld snooping querier enable
```

The following example enables the querier function for a bridge domain.

```
device# configure terminal
device(config)# bridge-domain 10
device(config-bridge-domain-10)# ipv6 mld snooping querier ?
Possible completions:
    enable Enable snooping querier
device(config-bridge-domain-10)# ipv6 mld snooping querier enable
```

ipv6 mld snooping query-interval

Sets the interval between MLD snooping queries for a VLAN or a bridge domain.

Syntax

ipv6 mld snooping query-interval *interval*

no ipv6 mld snooping query-interval

Command Default

By default, the interval is 125 seconds.

Parameters

interval

Valid intervals range from 1 second to 1800 seconds.

Modes

VLAN or bridge domain configuration mode

Usage Guidelines

The **no ipv6 mld snooping query-interval** form of the command restores the default interval of 125 seconds.

In any given subnet, one multicast router is elected to act as an MLD querier. The MLD querier sends out the following types of queries to hosts, at the interval you set.

- Multicast Listener General query: (MLD v1, v2) Asks whether any host is listening to any group.
- Multicast Listener Group-specific query: (MLD v1, v2) Asks whether any host is listening to a specific multicast group. This query is sent in response to a host leaving the multicast group. The router can quickly determine whether any remaining hosts are interested in the group.
- Multicast Listener Group-and-source-specific query: (MLD v2) Asks whether any host is listening to group multicast traffic from a specific multicast source. This query is sent in response to a host indicating that it is not interested in receiving group-specific multicast traffic from the multicast source. The router can quickly determine whether any remaining hosts are interested in receiving group multicast traffic from that source.

Examples

The following example configures the interval for a VLAN.

```
device# configure terminal
device(config)# vlan 10
```

```
device(config-vlan-10)#ipv6 mld snooping query-interval ?
Possible completions:
    <1-18000>    Query Interval value (Default: 125 s)
device(config-vlan-10)# ipv6 mld snooping query-interval 500
```

The following example configures the interval for a bridge domain.

```
device# configure terminal
device(config)# bridge-domain 10
device(config-bridge-domain-10)#ipv6 mld snooping query-interval ?
Possible completions:
    <1-18000>    Query Interval value (Default: 125 s)
device(config-bridge-domain-10)# ipv6 mld snooping query-interval 600
```

ipv6 mld snooping query-max-response-time

Sets the maximum amount of time to wait for a response from a snooping query for a VLAN or a bridge domain.

Syntax

ipv6 mld snooping query-max-response-time *response-time*

no ipv6 mld snooping query-max-response-time

Command Default

By default, the maximum response time is 10 seconds.

Parameters

response-time

Valid values range from 1 second to 25 seconds.

Modes

VLAN or bridge domain configuration mode.

Usage Guidelines

The **no ipv6 mld snooping query-max-response-time** form of the command restores the default interval of 10 seconds.

Examples

The following example configures the maximum response time for a VLAN.

```
device# configure terminal
device(config)# vlan 10
device(config-vlan-10)# ipv6 mld snooping query-max-response-time ?
Possible completions:
    <1-25>           Query Response Time (Default: 10 s)
device(config-vlan-10)# ipv6 mld snooping query-max-response-time 20
```

The following example configures the maximum response time for a bridge domain.

```
device# configure terminal
device(config)# bridge-domain 10
device(config-bridge-domain-10)# ipv6 mld snooping query-max-response-time ?
Possible completions:
    <1-25>           Query Response Time (Default: 10 s)
device(config-bridge-domain-10)# ipv6 mld snooping query-max-response-time 15
```

ipv6 mld snooping static-group

Configures a static group on an Ethernet or a port channel for a VLAN or a bridge domain.

Syntax

ipv6 mld snooping static-group *ipv6 address* **interface** [**ethernet** | **port-channel**] *interface name*

ipv6 mld snooping static-group *ipv6 address* **logical-interface** [**ethernet** | **port-channel**] *logical interface name*

no ipv6 mld snooping static-group *ipv6 address* **interface** [**ethernet** | **port-channel**]*interface name*

no ipv6 mld snooping static-group *ipv6 address* **logical-interface** [**ethernet** | **port-channel**] *logical interface name*

Command Default

By default, a static group is not configured.

Parameters

ipv6 address

Specifies the IPv6 address for which to configure a static group.

interface

Specifies the VLAN interface for which to configure a static group.
ethernet *interface name*

Specifies the Ethernet name in the following format: x/y, where x is the slot number and y is the interface (port) number. For example, 0/3.

port-channel *interface name*

Specifies the port channel name. For example, 10.200, where 10 is the port channel.

logical-interface

Specifies the bridge domain interface for which to configure a static group.
ethernet *logical interface name*

Specifies the Ethernet name in the following format: x/y, where x is the slot number and y is the interface (port) number. For example, 0/2.200.

port-channel *logical interface name*

Specifies the port channel name. For example, 10.200, where 10 is the port channel.

Modes

VLAN or bridge domain configuration mode

Usage Guidelines

The **no ipv6 mld snooping static-group** form of the command removes the static group.

A snooping-enabled VLAN or bridge domain cannot forward multicast traffic to ports that do not receive MLD membership reports. If clients cannot send reports, you can configure a static group that applies to specific ports. The static group allows packets to be forwarded to the static group ports even though they have no client membership reports.

Examples

The following example configures a static group on a VLAN Ethernet.

```
device# configure terminal
device(config)# interface vlan 10
device(config-vlan-10)# ipv6 mld snooping static-group ff28::1 interface Ethernet 0/3
```

The following example removes the static group from a VLAN Ethernet.

```
device# configure terminal
device(config)# interface vlan 10
device(config-vlan-10)# no ipv6 mld snooping static-group ff28::1 interface Ethernet 0/3
```

The following example configures a static group on a bridge domain Ethernet.

```
device# configure terminal
device(config)# bridge domain 10
device(config-bridge-domain-10)# ipv6 mld snooping static-group ff28::2 logical interface
Ethernet 0/2.200
```

The following example removes the static group from a bridge domain Ethernet.

```
device# configure terminal
device(config)# bridge domain 10
device(config-bridge-domain-10)# no ipv6 mld snooping static-group ff28::2 logical
interface Ethernet 0/2.200
```

ipv6 mld snooping version

Sets the MLD version that the querier uses for snooping for a VLAN or a bridge domain.

Syntax

ipv6 mld snooping version [**1** | **2**]

no ipv6 mld snooping version

Command Default

By default, the querier uses MLD version 1.

Parameters

1 | **2**

Specifies the version of MLD that you want to use.

Modes

VLAN or bridge domain configuration mode

Usage Guidelines

The **no ipv6 mld snooping version** form of the command resets MLD to version 1.

Examples

The following example sets the version to 2 for a VLAN.

```
device# configure terminal
device(config)# vlan 10
device(config-vlan-10)# ipv6 mld snooping version ?
Possible completions:
    <MLD version 1 or 2 (Default: 1)>
device(config-vlan-10)# ipv6 mld snooping version 2
```

The following example sets the version to 2 for a bridge domain.

```
device# configure terminal
device(config)# bridge-domain 10
device(config-bridge-domain-10)# ipv6 mld snooping version ?
Possible completions:
    <MLD version 1 or 2 (Default: 1)>
device(config-bridge-domain-10)# ipv6 mld snooping version 2
```

ipv6 mld ssm-map enable

Associates a prefix list with a source address, known as Source Specific Multicast (SSM) mapping.

Syntax

ipv6 mld ssm-map enable *prefix_name map source IPv6 address*

no ipv6 mld ssm-map enable *prefix_name map source IPv6 address*

Command Default

By default, SSM mapping is not enabled.

Parameters

prefix_name

Specifies the name of the prefix list to associate with an IPv6 address.

map source IPv6 address

Specifies the IPv6 address to associate with a prefix list.

Modes

VLAN or bridge domain configuration mode

Usage Guidelines

Use the **no ipv6 mld ssm-map enable** form of the command to disable SSM mapping on the indicated prefix and IPv6 address.

Examples

The following example maps IPv6 address 2::100 to a prefix list named prefix1.

```
device# configure terminal
devicee(config)# vlan 10
device(config-vlan-10)# ipv6 mld ssm-map prefix1 2::100
```

ipv6 nd cache expire

Configures the time interval after which the Neighbor Discovery cache is deleted or refreshed.

Syntax

ipv6 nd cache expire *seconds*

no ipv6 nd cache expire *seconds*

Command Default

Default expiration time is 1500 seconds.

Parameters

seconds

Specifies how long an entry stays in the Neighbor Discovery cache. The range is from 30 through 14400 seconds. The default is 1500.

Modes

Interface subtype configuration mode

Usage Guidelines

Cache entries expire and are deleted if they remain in a "stale" state as defined by *seconds*.

You can modify the ND expiration time only at the interface level, but not at the global level.

The **no** form of this command restores the default aging timeout of 1500 seconds.

Examples

The following example sets the Neighbor Discovery expiration time to 2500 seconds on an Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 1/2
conf-if-eth-1/2)# ipv6 nd cache expire 2500
```

ipv6 nd cache interface-limit

Configure the number of entries in the Neighbor Discovery cache table. This command can be used to configure the global limit as well as the limit on individual layer 3 interfaces.

Syntax

ipv6 nd cache interface-limit *1-97280*

no ipv6 nd cache interface-limit

Modes

Global Configuration and Interface Configuration Modes

Usage Guidelines

The minimum neighbor discovery cache limit that can be configured per interface is one (1). The maximum neighbor discovery limit per interface is the same as the system's maximum neighbor discovery cache limit. This maximum limit varies between the various systems. The maximum value that can be configured is 97280 entries.

The command when executed in the Global Configuration mode configures the maximum number of entries for all IPv6 neighbor discovery tables.

The command when executed within an interface's configuration mode, configures the limit on that interface's IPv6 neighbor discovery table.

The **no** format of the global form of this command removes the configured neighbor discovery cache limit from all the interfaces. However, it does not remove neighbor discovery limitations configured on individual interfaces which were configured using the **ipv6 nd cache interface-limit** command.

Examples

The following example sets the IPv6 neighbor discovery table limit to 100 globally.

```
SLX(config)#  ipv6 nd cache interface-limit 100
```

The following example sets the IPv6 neighbor discovery table limit to 250 entries for the ethernet interface 3/5.

```
SLX (config)# interface ethernet 3/5
SLX (config-if-eth-3/5)# ipv6 nd cache interface-limit 250
```

This example displays the neighbor discovery cache limit configuration on a VE interface.

```
SLX # show ipv6 neighbor ve 4227
```

```
Configured ND Cache limit : 100

Total Entries in Interface : 4
Address                         Mac-address     L3 Interface  L2 Interface
Age         Type
-------------------------------------------------------------------------------------------
----------------------
200:30:70:7::2                  887e.25d3.e20b  Ve 4277       Tu 32769 (10.20.20.10)
Never       Mct-Sticky
200:30:70:7::33                 0034.000c.5501  Ve 4277       Tu 32772 (172.31.254.63)
00:06:27    Dynamic
fe80::30:7:70:33                0034.000c.5501  Ve 4277       Tu 32772 (172.31.254.63)
00:06:22    Dynamic
fe80::8a7e:25ff:fed3:e20b       887e.25d3.e20b  Ve 4277       Tu 32769 (10.20.20.10)
Never       Mct-Sticky

SLX #
```

ipv6 option disable

Blocks packets that have IPv6 RH options.

Syntax

ipv6 option disable

no ipv6 option disable

Command Default

By default, IPv6 packets with RH options are not blocked.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of the command to unblock packets that have IP options.

Examples

The following example blocks IPv6 packets that have RH options.

```
device# configure terminal
device(config)# ipv6 option disable
```

ipv6 ospf active

Sets a specific OSPFv3 interface to active.

Syntax

ipv6 ospf active

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **ipv6 ospf active** command on each interface participating in adjacency formation. This command overrides the global passive setting on that interface, and enables transmission of OSPFv3 control packets.

Examples

The following example sets a specific OSPFv3 Ethernet interface to active.

```
device# configure termnial
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf active
```

ipv6 ospf area

Enables OSPFv3 on an interface.

Syntax

ipv6 ospf area *area-id | ip-addr*

no ipv6 ospf area

Command Default

OSPFv3 is disabled.

Parameters

area-id

Area ID in dotted decimal or decimal format.

ip-addr

Area ID in IP address format.

Modes

Interface subtype configuration mode

Usage Guidelines

This command enables an OSPFv3 area on the interface to which you are connected.

The **no** form of the command disables OSPFv3 on this interface.

When configuring OSPF on a VE interface that will be applied to a GRE tunnel, the MTU configured in that VE is applied to the GRE tunnel and is used as the MTU for the tunnel. When configuring the MTU for the tunnel interface, the assigned MTU value takes into account the 24 bytes reserved for the GRE Tunnel Header. This 24 bytes is automatically reduced from the target MTU.

Note
The 24 bytes consists of a 20 Byte GRE Outer Header and a 4 Byte Outer IP Header.

For example, when the VE MTU is set to the default MTU 1500, the GRE tunnel MTU will automatically be adjusted to 1476 Bytes and the remaining 24 bytes are used to carry the GRE Tunnel Header information . If the VE MTU is set to any value other than the default MTU value, the reserved 24 bytes will be automatically reduced from your target configuration before it is set as the VE's MTU.

In the case where you want to assign the maximum permissible MTU of 9194 Bytes, you must manually reduce the reserved 24 Bytes. In this case, you should set the MTU value at 9170 Bytes.

Examples

The following example enables a configured OSPFv3 area named 0 on a specific OSPFv3 Loopback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# ipv6 ospf area 0
```

ipv6 ospf authentication ipsec

Specifies IP security (IPsec) as the authentication type for an OSPFv3 interface.

Syntax

ipv6 ospf authentication ipsec key-add-remove-interval *interval*

no ipv6 ospf authentication ipsec key-add-remove-interval *interval*

Command Default

Disabled.

Parameters

key-add-remove-interval *interval*

Specifies the OSPFv3 authentication key add-remove interval. Valid values range from decimal numbers 0 through 14400. The default is 300.

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command removes IPsec authentication from the interface.

Examples

The following example enables IPsec on a specified OSPFv3 Looback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# ipv6 ospf area 0
device(config-Loopback-1)# ipv6 ospf authentication ipsec
```

The following example sets the OSPFv3 authentication key add-remove interval to 480.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# ipv6 ospf area 0
device(config-Loopback-1)# ipv6 ospf authentication ipsec key-add-remove-interval 480
```

ipv6 ospf authentication ipsec disable

Disables IP security (IPsec) services on an OSPFv3 interface.

Syntax

ipv6 ospf authentication ipsec disable

no ipv6 ospf authentication ipsec disable

Command Default

Authentication is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to disable IPsec if it is enabled on the interface. Packets that are sent out will not be IPSec encapsulated and the received packets which are IPSec encapsulated will be dropped.

The **no** form of the command re-enables IPSec on the interface if IPsec is already configured on the interface.

Examples

The following example disables IPsec on a specific OSPFv3 interface where IPsec is already enabled.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# ipv6 ospf authentication ipsec disable
```

ipv6 ospf authentication spi

Specifies the security policy index (SPI) value for an OSPFv3 interface.

Syntax

ipv6 ospf authentication spi *spi* { **ah** | **esp null** } { **hmac-md5** | **hmac-sha1** } **key** *key* }

no ipv6 ospf authentication spi

Command Default

Disabled.

Parameters

spi

SPI value. Valid values range from decimal numbers 512 through 4294967295.

ah

Specifies Authentication Header (ah) as the protocol to provide packet-level security.

esp

Specifies Encapsulating Security Payload (ESP) as the protocol to provide packet-level security.

null

Specifies that the ESP payload is not encrypted.

hmac-md5

Enables Hashed Message Authentication Code (HMAC) Message Digest 5 (MD5) authentication on the OSPFv3 interface.

hmac-sha1

Enables HMAC Secure Hash Algorithm 1 (SHA-1) authentication on the OSPFv3 interface.

key

Number used in the calculation of the message digest.

key

The 40 hexadecimal character key.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ipv6 ospf authentication spi** *spi* to remove the SPI value from the interface.

Examples

The following example enables ESP and HMAC-SHA-1 on an OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf area 0
device(conf-if-eth-1/1)# ipv6 ospf authentication spi 512 esp null hmac-sha1 key
abcef12345678901234fedcba098765432109876
```

The following example enables AH and HMAC-MD5 on an OSPFv3 virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ipv6 ospf area 0
device(config-if-Ve-1# ipv6 ospf authentication spi 750 ah hmac-md5 key
abcef12345678901234fedcba098765432109876
```

ipv6 ospf bfd

Enables Bidirectional Forwarding Detection (BFD) on a specific OSPFv3 interface.

Syntax

ipv6 ospf bfd

no ipv6 ospf bfd

Modes

Interface subtype configuration mode

Usage Guidelines

BFD sessions are initiated only if BFD is also enabled globally using the **bfd** command in OSPFv3 router configuration mode. If BFD is disabled using the **no bfd** command in OSPFv3 router configuration mode, BFD sessions on specific interfaces are deregistered.

The **no** form of the command removes all BFD sessions from a specified interface.

Examples

The following example enables BFD on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/4
device(conf-if-eth-1/4)# ipv6 ospf bfd
```

The following example disables BFD on an OSPFv3 virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 24
device(config-if-Ve-24)# no ipv6 ospf bfd
```

ipv6 ospf cost

Configures cost for a specific OSPFv3 interface.

Syntax

ipv6 ospf cost *value*

no ipv6 ospf cost

Command Default

Cost value is 1.

Parameters

value

Cost value. Valid values range from 1 through 65535. The default is 1.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to set or reset the OSPFv3 cost on the interface. If the cost is not configured with this command, OSPFv3 calculates the value from the reference and interface bandwidths.

For more information, refer to the **auto-cost reference-bandwidth** command.

The **no** form of the command disables the configured cost.

Examples

The following example sets the cost to 620 on a specific OSPFv3 Virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ipv6 ospf cost 620
```

ipv6 ospf dead-interval

Specifies the time period for which a neighbor router waits for a hello packet from the device before declaring the router down.

Syntax

ipv6 ospf dead-interval *interval*

no ipv6 ospf dead-interval

Command Default

The specified time period is 40 seconds.

Parameters

interval

Dead interval in seconds. Valid values range from 3 through 65535 seconds. The default is 40.

Modes

Interface subtype configuration mode

Usage Guidelines

If you change the dead interval, the hello interval is automatically changed to a value that is one fourth that of the new dead interval, unless the hello interval is also explicitly configured using the **ipv6 ospf hello-interval** command.

The recommended setting is that:

- The dead interval is four times that of the hello interval.
- The hello interval is ¼ times that of the dead interval.

The **running-config** command displays only explicitly configured values of the hello interval, which means that a value that was automatically changed as the result of a dead-interval change is not displayed.

The **no** form of the command restores the default value.

Examples

The following example sets the dead interval to 80 on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
```

```
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf dead-interval 80
```

ipv6 ospf hello-interval

Sets the length of time between the transmission of hello packets that an interface sends to neighbor routers.

Syntax

ipv6 ospf hello-interval *interval*

no ipv6 ospf hello-interval

Command Default

The length of time between the transmission of hello packets is set to 10 seconds.

Parameters

interval

Hello interval in seconds. Valid values range from 1 through 65535 seconds. The default is 10.

Modes

Interface subtype configuration mode

Usage Guidelines

If you change the hello interval, the dead interval is automatically changed to a value that is four times that of the new hello interval, unless the dead interval is also explicitly configured using the **ipv6 ospf dead-interval** command.

The recommended setting is that:

- The dead interval is four times that of the hello interval.
- The hello interval is ¼ times that of the dead interval.

The **running-config** command displays only explicitly configured values of the dead interval, which means that a value that was automatically changed as the result of a hello interval change is not displayed.

The **no** form of the command restores the default value.

Examples

The following example sets the hello interval to 20 on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
```

```
device(conf-if-eth-1/1)# ipv6 ospf hello-interval 20
```

ipv6 ospf hello-jitter

Sets the allowed jitter between HELLO packets.

Syntax

ipv6 ospf hello-jitter *interval*

no ipv6 ospf hello-jitter

Command Default

10%

Parameters

jitter

Allowed interval between hello packets.Valid values range from 1 through 50 percent (%).

Modes

Interface subtype configuration mode

Usage Guidelines

The hello interval can vary from the configured hello-interval to a maximum of percentage value of configured jitter.

Examples

The following example sets the hello jitter to 20 on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf hello-jitter 20
```

ipv6 ospf instance

Specifies the number of OSPFv3 instances running on an interface.

Syntax

ipv6 ospf instance *instanceID*

no ipv6 ospf instance

Parameters

instanceID

Instance identification number. Valid values range from 0 through 255.

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command restores the default value.

Examples

The following example sets the number of IPv6 OSPF instances to 35 on a specific Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf instance 35
```

ipv6 ospf mtu-ignore

Enables or disables maximum transmission unit (MTU) match checking.

Syntax

ipv6 ospf mtu-ignore

no ipv6 ospf mtu-ignore

Command Default

Enabled.

Modes

Interface subtype configuration mode

Usage Guidelines

In default operation, the IP MTU on both sides of an OSPFv3 link must be the same, and a check of the MTU is performed when Hello packets are first exchanged.

The **no** no form of the command disables MTU-match checking on a specific interface.

Examples

The following example disables MTU-match checking on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# no ipv6 ospf mtu-ignore
```

The following example disables MTU-match checking on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf mtu-ignore
```

ipv6 ospf network

Configures network type.

Syntax

ipv6 ospf network { **broadcast** | **point-to-point** }

no ipv6 ospf network

Command Default

Network type is broadcast.

Parameters

broadcast

Network type is broadcast, such as Ethernet.

point-to-point

Network type is point-to-point.

Modes

Interface subtype configuration mode

Usage Guidelines

Point-to-point can support unnumbered links, which requires less processing by OSPFv3.

The **no** form of the command removes the network-type configuration.

Note
The network type non-broadcast is not supported at this time.

Examples

The following example configures an OSPFv3 point-to-point link on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf network point-to-point
```

The following example configures an OSPFv3 broadcast link on a specific OSPFv3 Loopback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# ipv6 ospf network broadcast
```

ipv6 ospf passive

Sets a specific OSPFv3 interface to passive.

Syntax

ipv6 ospf passive

no ipv6 ospf passive

Modes

Interface subtype configuration mode

Usage Guidelines

The **ipv6 ospf passive** command disables transmission of OSPFv3 control packets on that interface. OSPFv3 control packets received on a passive interface are discarded.

The **no** form of the command sets an interface back to active.

Examples

The following example sets a specific OSPFv3 virtual Ethernet (VE) interface to passive.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ipv6 ospf passive
```

ipv6 ospf priority

Configures priority for designated router (DR) election and backup designated routers (BDRs) on the interface you are connected to.

Syntax

ipv6 ospf priority *value*

no ipv6 ospf priority

Command Default

The value is set to 1.

Parameters

value

Priority value. Valid values range from 0 through 255. The default is 1.

Modes

Interface subtype configuration mode

Usage Guidelines

The OSPFv3 router assigned the highest priority becomes the designated router, and the OSPFv3 router with the second-highest priority becomes the backup router.

The **no** form of the command restores the default value.

Examples

The following example sets a priority of 4 for the OSPFv3 router that is connected to an OSPFv3 Virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 1
device(config-if-Ve-1)# ipv6 ospf priority 4
```

ipv6 ospf retransmit-interval

Configures the retransmit interval. The retransmit interval is the time between Link-State Advertisement (LSA) retransmissions to adjacent routers for a given interface.

Syntax

ipv6 ospf retransmit-interval *interval*

no ipv6 ospf retransmit-interval

Command Default

The interval is 5 seconds.

Parameters

interval

Retransmit interval in seconds. Valid values range from 0 through 3600 seconds. The default is 5.

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command resets the retransmit interval to its default.

Examples

The following example sets the retransmit interval to 8 for all OSPFv3 devices on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf retransmit-interval 8
```

ipv6 ospf suppress-linklsa

Suppresses link LSA advertisements.

Syntax

ipv6 ospf suppress-linklsa

no ipv6 ospf suppress-linklsa

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command restores the defaults where link LSA advertisements are not suppressed.

Examples

The following example suppresses link LSAs from being advertised on devices on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf suppress-linklsa
```

ipv6 ospf transmit-delay

Configures transmit delay for link-update packets. The transmit delay is the estimated time required for OSPFv3 to send link-state update packets on the interface to which you are connected.

Syntax

ipv6 ospf transmit-delay *value*

no ipv6 ospf transmit-delay

Command Default

The transmit delay is set to 1 second.

Parameters

value

Transmit delay in seconds. Valid values range from 0 through 3600 seconds.

Modes

Interface subtype configuration mode

Usage Guidelines

The **no** form of the command restores the default value.

Examples

The following example sets a transmit delay of 25 seconds for devices on a specific OSPFv3 Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 ospf transmit-delay 25
```

ipv6 pim dr-priority

Specifies the DR (designated router) priority of an IPv6 PIM-enabled interface.

Syntax

ipv6 pim dr-priority *priority-value*

no ipv6 pim dr-priority

Command Default

The default priority value is 1.

Parameters

priority-value

Valid values range from 0 through 65535.

Modes

Interface configuration mode

Usage Guidelines

Important

Use the **ipv6 router pim** command to globally enable IPv6 PIM routing before setting the DR priority.

The DR receives all Join messages from the hosts below it. The DR then sends only one Join message to the rendezvous point (RP) on behalf of the hosts. Similarly, the DR attached to the source registers with the RP.

The router with the highest DR priority is the elected DR for an interface. If multiple routers have the same DR priority, the router with the highest IP address is the elected DR.

The **no ipv6 pim dr-priority** form of the command restores the default priority of 1.

Examples

The following example specifies the DR priority on a virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 30
device(config-if-ve-30)# ipv6 pim dr-priority 100
```

ipv6 pim snooping enable

Enable IPv6 PIM snooping on a VLAN or bridge domain.

Syntax

ipv6 pim snooping enable

no ipv6 pim snooping enable

Command Default

By default, IPv6 PIM snooping is enabled when IPv6 PIM is enabled on a Layer 3 VLAN interface.

By default, IPv6 PIM snooping is disabled on a Layer 2 interface.

Modes

VLAN or bridge-domain configuration mode

Usage Guidelines

The **no ipv6 pim snooping enable** form of the command disable disables snooping.

Examples

This example enables IPv6 PIM snooping on a VLAN.

```
device# configure terminal
device(config)# vlan 30
device(config-vlan-30)# ipv6 pim snooping enable
```

ipv6 pim ttl-threshold

Configures the Time to Live (TTL) threshold on an IPv6 PIM-enabled interface.

Syntax

ipv6 pim ttl-threshold *threshold-value*

no ipv6 pim ttl-threshold

Command Default

The default threshold value is 1.

Parameters

threshold-value

Valid values range from 1 through 64.

Modes

Interface configuration mode

Usage Guidelines

Important

Use the **ipv6 router pim** command to globally enable IPv6 PIM routing before configuring the TTL threshold.

As a packet is forwarded out of an interface, its TTL value is reduced. The TTL threshold is the smallest TTL value that a packet can have for an interface to forward it.

Important

An interface can have only one TTL threshold. You cannot configure different thresholds for IPv4 PIM and IPv6 PIM. The most recent configured value, whether for IPv4 PIM or IPv6 PIM, overwrites the previous value.

The **no ipv6 pim ttl-threshold** form of the command restores the default TTL of 1.

Examples

The following example configures the TTL threshold ton a virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 30
device(config-if-ve-30)# ipv6 pim ttl-threshold 64
```

ipv6 pim-sparse

Enables IPv6 PIM routing on an interface.

Syntax

ipv6 pim-sparse

no ipv6 pim-sparse

Command Default

By default, IPv6 PIM routing is disabled on an interface.

Modes

Interface configuration mode

Usage Guidelines

Important
Use the **ipv6 router pim** command to globally enable IPv6 PIM routing before enabling it on an interface.

Perform Layer 3 configuration for VLANs, Bridge Domains, or LAGs under their interfaces at the Layer 3 level.

The **no ipv6 pim-sparse** form of the command disables IPv6 PIM routing.

Examples

This example enables IPv6 PIM on a virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 30
device(config-if-ve-30)# ipv6 pim-sparse
```

ipv6 policy route-map

Enables IPv6 policy-based routing (PBR).

Syntax

ipv6 policy route-map *map-name*

no ipv6 policy route-map *map-name*

Command Default

IPv6 PBR is not enabled.

Parameters

map-name

Specifies the name of the route map.

Modes

Interface configuration mode

Port-channel configuration mode

Virtual interface configuration mode

Usage Guidelines

The **no** form of the command disables IPv6 PBR.

Examples

The following example enables PBR on a specific interface.

```
device(config)# route-map test-route permit 99
device(config-route-map-test-route/permit/99)# match ipv6 address acl 99
device(config-route-map-test-route/permit/99)# set ipv6 next-hop
2001:db8:0:0:0:ff00:42:8329
device(config-route-map-test-route/permit/99)# exit
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 policy route-map test-route
```

ipv6 prefix-list

Configures an IPv6 prefix list for basic traffic filtering

Syntax

ipv6 prefix-list *name* **deny** *ipv6-prefix/prefix-length* [**ge** *ge-value*] [**le** *le-value*]

ipv6 prefix-list *name* **permit** *ipv6-prefix/prefix-length* [**ge** *ge-value*] [**le** *le-value*]

ipv6 prefix-list *name* **seq** *instance-number* { **deny ge** *ge-value* **le** *le-value* | **permit ge** *ge-value* **le** *le-value* }

no ipv6 prefix-list *name*

Parameters

name

Specifies the prefix list name.

deny *ip-prefix/prefix-length*

Denies a route specified in the prefix list. The prefix list matches only on the specified prefix/prefix length, unless you use the **ge** *ge-value* or **le** *le-value* parameters.

ge *ge-value*

Specifies minimum prefix length to be matched. The range is from *ge-value* to 128.

le *le-value*

Specifies maximum prefix length to be matched. The range is from the *le-value* to the *prefix-length* parameter.

permit *ip-prefix/prefix-length*

Permits a route specified in the prefix list. The prefix list matches only on the specified prefix/prefix length, unless you use the **ge** *ge-value* or **le** *le-value* parameters.

seq

Specifies an IPv6 prefix list sequence number of entry.

instance

Specifies an IPv6 prefix list instance number.

Modes

Global configuration mode

Usage Guidelines

An IPv6 prefix list is composed of one or more conditional statements that execute a permit or deny action if a route matches a specified prefix. In prefix lists with multiple statements, you can specify a sequence number for each statement. The specified sequence number determines the order in which the statement appears in the prefix.

You can configure an IPv6 prefix list on a global basis, then use it as input to other commands or processes, such as route aggregation, route redistribution, route distribution, route maps, and so on. When an SLX-OS device interface sends or receives an IPv6 packet, it applies the statements within the IPv6 prefix list in their order of appearance to the packet. As soon as a match occurs, the device takes the specified action (permit or deny the packet) and stops further comparison for that packet.

You can use permit statements in the prefix list to specify the traffic that you want to send to the other feature. If you use deny statements, the traffic specified by the deny statements is not supplied to the other feature. You can configure up to one hundred IPv6 prefix lists.

You must specify the ipv6-prefix parameter in hexadecimal using 16-bit values between colons as documented in RFC 4291. You must specify the prefix-length parameter as a decimal value. A slash mark (/) must follow the ipv6-prefix parameter and precede the prefix-length parameter.

The *ge-value* or *le-value* you specify must meet the following condition for *prefix-length* :

```
ge-value <= le-value <= 128
```

Examples

The following example creates a prefix-list that allows routes with the prefix 2001:db8::/32 .

```
device# configure terminal
device(config)# ipv6 prefix-list route1 permit 2001:db8::/32
device(config)# interface ethernet 2/1
device(conf-if-eth-2/1)# ipv6 prefix-list route1
```

ipv6 protocol vrrp

Globally enables IPv6 VRRPv3.

Syntax

ipv6 protocol vrrp

no ipv6 protocol vrrp

Command Default

IPv6 VRRPv3 is not enabled.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command globally disables VRRPv3.

Examples

To enable IPv6 VRRPv3 globally:

```
device# configure terminal
device(config)# ipv6 protocol vrrp
```

ipv6 protocol vrrp-extended

Globally enables IPv6 VRRP-Ev3.

Syntax

ipv6 protocol vrrp-extended

no ipv6 protocol vrrp-extended

Command Default

IPv6 VRRP-Ev3 is disabled.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command globally disables IPv6 VRRP-Ev3.

Examples

To enable IPv6 VRRP-Ev3 globally:

```
device# configure terminal
device(config)# ipv6 protocol vrrp-extended
```

ipv6 receive access-group

Applies an IPv6 access control list (ACL) at global configuration level. Such *receive-path ACLs* filter incoming route-processor traffic according to rules that you create, but do not filter data-path traffic.

Syntax

ipv6 receive access-group *acl-name* [**sequence** *seq-number*]

no ipv6 receive access-group *acl-name*

Command Default

No receive-path ACLs are applied.

Parameters

acl-name

Specifies the name of the standard or extended IP access list.

sequence *seq-number*

Specifies the sequence of the rACL you are applying. Values range from 1 through 2047.

Modes

Global configuration mode

Usage Guidelines

For both interface ACLs and receive-path ACLs, you use identical commands to create the ACLs. You also use identical commands to define permit/deny rules in the ACLs. The only variance is the command you use to apply the ACL:

- To apply an interface ACL, from an interface-subtype configuration mode you use the { **ip** | **ipv6** | **mac** } **access-group** command.
- To apply a receive-path ACL, from global configuration mode you use the { **ip** | **ipv6** } **receive access-group** command.

You can apply a maximum of 400 receive-path ACLs to a device, as follows:

- 200 IPv4 receive-path ACLs
- 200 IPv6 receive-path ACLs

To remove a receive-path ACL, enter the **no** form of this command.

Examples

The following example creates an IPv6 extended ACL, defines rules in the ACL, and applies it as a receive-path ACL.

```
device(config)# ipv6 access-list extended ipv6-receive-acl-example
device(conf-ipacl-ext)# hard-drop tcp host 10::1 any count
device(conf-ipacl-ext)# hard-drop udp any host 20::1 count
device(conf-ipacl-ext)# permit tcp host 10::2 any eq telnet count
device(conf-ipacl-ext)# permit tcp host 10::2 any eq bgp count

device(conf-ipacl-ext)# exit
device(config)# ipv6 receive access-group ipv6-receive-acl-example
```

The following example creates two IPv6 extended ACLs, defines rules in the ACLs, and applies them as receive-path ACLs—specifying the priority of each ACL.

```
device# configure terminal
device(config)# ipv6 access-list extended test-racl-v6-1
device(conf-ip6acl-ext)# deny ipv6 host 2::2 any count
device(conf-ip6acl-ext)# exit
device(config)# ipv6 access-list extended test-racl-v6-2
device(conf-ip6acl-ext)# permit ipv6 host 3::3 any
device(conf-ip6acl-ext)# exit


device(config)# ipv6 receive access-group test-racl-v6-1 seq 10
device(config)# ipv6 receive access-group test-racl-v6-2 seq 20
```

ipv6 route

Configures an IPv6 static route.

Syntax

ipv6 route *dest-ipv6-prefix* **/** *prefix-length next-hop-ipv6-address* [*metric*] [**distance** *number*] [**tag** *tag-number*] [**name** *name-value*]

ipv6 route *dest-ipv6-prefix* **/** *prefix-length link-local-next-hop-ipv6-address* [**ethernet** *slot/port*] [*metric*] [**distance** *number*] [**tag** *tag-number*] [**name** *name-value*]

ipv6 route *dest-ipv6-prefix* **/** *prefix-length link-local-next-hop-ipv6-address* [**port-channel** *number*] [*metric*] [**distance** *number*] [**tag** *tag-number*] [**name** *name-value*]

ipv6 route *dest-ipv6-prefix* **/** *prefix-length link-local-next-hop-ipv6-address* [**ve** *ve-id*] [*metric*] [**distance** *number*] [**tag** *tag-number*] [**name** *name-value*]

ipv6 route next-hop-recursion

no ipv6 route *dest-ipv6-prefix* **/** *prefix-length next-hop-ipv6-address*

no ipv6 route *dest-ipv6-prefix* **/** *prefix-length link-local-next-hop-ipv6-address* [**ethernet** *slot/port*]

no ipv6 route *dest-ipv6-prefix* **/** *prefix-length link-local-next-hop-ipv6-address* [**port-channel** *number*]

no ipv6 route *dest-ipv6-prefix* **/** *prefix-length link-local-next-hop-ipv6-address* [**ve** *ve-id*]

no ipv6 route next-hop-recursion

Command Default

No IPv6 static route is configured by default.

Parameters

dest-ipv6-prefix

Destination IPv6 prefix in hexadecimal with 16-bit values between colons, as specified in RFC 2373.

prefix-length

A decimal value specifying the length of the IPv6 address prefix.

next-hop-ipv6-address

IPv6 address of the next-hop gateway.

link-local-next-hop-ipv6-address

IPv6 address of the link-local next-hop gateway.

ethernet *slot/port*

Specifies the Ethernet slot and port.

port-channel *number*

Specifies a port-channel interface.

ve *ve-id*

Specifies the virtual Ethernet (VE) interface.

metric

Specifies a value that the Layer 3 switch uses to compare this route to other static routes in the IPv6 static route table that have the same destination. The metric applies only to routes that the Layer 3 switch has already placed in the IPv6 static route table. Two or more routes to the same destination with the same metric will load share (as in ECMP load sharing). The range is from 1 through 16. The default is 1.

distance *number*

Specifies an administrative distance. The range is from 1 through 254. The default is 1. This is a value that the Layer 3 switch uses to compare this route with routes from other route sources that have the same destination. By default, static routes take precedence over routes learned by routing protocols. To choose a dynamic route over a static route, configure the static route with a higher administrative distance than the dynamic route. A distance of 255 is considered unreachable.

tag

Specifies a tag value for the route. The route tag can be used for route redistribution to routing protocols by means of route maps (as in IPv4 static route redistribution).
tag-number

A number from 0 through 4294967295. The default is 0.

next-hop-recursion

Specifies that if the next hop for a static route is reachable, then that route is added to the routing table.

name *name-value*

Specifies the name to be assigned to this IPv6 route. This field can be used to assign a meaningful, human readable description to this route configuration. Maximum length 127 characters.

Modes

Global configuration mode

VRF configuration mode

Usage Guidelines

Use the **no** form of the command with the same parameters to remove the IPv6 static route.

Examples

The following example creates an IPv6 static route for a destination network with the prefix 2001:DB8::0/32 and a next-hop gateway with the global address 2001:DB8:0:ee44::1. It also assigns a name to it.

```
device# configure terminal
device(config)# ipv6 route 2001:DB8::0/32 2001:DB8:0:ee44::1 name route-sj-01
```

The following example configures non-recursive lookup in the default VRF.

```
device(config)# ipv6 route next-hop-recursion
```

The following example configures non-recursive lookup in a non-default VRF named red.

```
device(config)# vrf red
device(config-vrf-red)# address-family ipv6 unicast
device(config-vrf-red-ipv6-unicast)# ipv6 route next-hop-recursion
```

ipv6 route next-hop-recursion

Enables recursive lookup for IPv6 next-hop routes.

Syntax

ipv6 route next-hop-recursion

no ipv6 route next-hop-recursion

Command Default

By default, next-hop recursive lookups are enabled.

Modes

Global configuration mode

VRF configuration mode

Usage Guidelines

The **no** form of the command disables recursive lookups.

Examples

The following example disables recursive lookups in the default VRF.

```
device# configure terminal
device(config)# no ipv6 route next-hop-recursion
```

The following example disables recursive lookups in a non-default VRF.

```
device(config) vrf red
device(config-vrf-red)# address-family ipv6 unicast
device(config-vrf-red-ipv6-unicast)no ipv6 route next-hop-recursion
```

The following example re-enables recursive lookups in the default VRF.

```
device# configure terminal
device(config)# ipv6 route next-hop-recursion
```

The following example re-enables recursive lookups in a non-default VRF.

```
device(config) vrf red
device(config-vrf-red)# address-family ipv6 unicast
device(config-vrf-red-ipv6-unicast)ipv6 route next-hop-recursion
```

ipv6 route null

Configures an IPv6 null route for discarding traffic.

Syntax

ipv6 route *dest-ipv6-prefix*/*prefix-length* **null 0** [*metric*] [**distance** *number*] [**tag** *tag-number*]

no ipv6 route *dest-ipv6-prefix*/*prefix-length* **null 0**

Command Default

No IPv6 static route is configured by default.

Parameters

dest-ipv6-prefix

Destination IPv6 prefix in hexadecimal with 16-bit values between colons, as specified in RFC 2373.

prefix-length

A decimal value specifying the length of the IPv6 address prefix.

next-hop-ipv6-address

IPv6 address of the next-hop gateway.

null 0

Causes packets to the selected destination to be dropped by shunting them to the "null 0" interface. (This is the only available option.)

ethernet *slot/port*

Specifies the Ethernet slot and port.

metric

Specifies a value that the Layer 3 switch uses to compare this route to other static routes in the IPv6 static route table that have the same destination. The metric applies only to routes that the Layer 3 switch has already placed in the IPv6 static route table. Two or more routes to the same destination with the same metric will load share (as in ECMP load sharing). The range is from 1 through 16. The default is 1.

distance *number*

Specifies an administrative distance. The range is from 1 through 254. The default is 1. This is a value that the Layer 3 switch uses to compare this route with routes from other route sources that have the same destination. By default, static routes take precedence over routes learned by routing protocols. To choose a dynamic route over a static route, configure the static route with a higher administrative distance than the dynamic route. A distance of 255 is considered unreachable.

tag

Specifies a tag value for the route. The route tag can be used for route redistribution to routing protocols by means of route maps (as in IPv4 static route redistribution).
tag-number

A number from 0 through 4294967295. The default is 0.

Modes

Global configuration mode

VRF configuration mode

Usage Guidelines

Use the **no** form of the command with the same parameters to remove the null route.

Related commands:

- **ipv6 route**
- **ipv6 route** next-hop-vrf

Examples

The following example creates a primary route to all 2001 : DB8 : : 0/32 destinations through virtual interface (ve) 3. The primary route has the default cost metric of 1. The example aslo creates an alternative null route (with a cost metric of 2) to drop packets when the primary route is not available.

```
device# configure terminal
device(config)# ipv6 route 2001 : DB8 : : 0/32 fe80::1 ve 3
device(config)# ipv6 route 2001 : DB8 : : 0/32 null 0 2
```

ipv6 route next-hop-vrf

Configures an IPv6 static route through a named VRF.

Syntax

ipv6 route *ipv6-prefix/prefix-length* **next-hop-vrf** *vrf_name next-hop-ipv6-address* [*metric*] [**distance** *number*] [**tag** *tag-number*]

no ipv6 route *ipv6-prefix/prefix-length* **next-hop-vrf** *vrf_name next-hop-ipv6-address*

Command Default

No IPv6 static route is configured by default.

Parameters

dest-ipv6-prefix

Destination IPv6 prefix in hexadecimal with 16-bit values between colons, as specified in RFC 2373.

prefix-length

A decimal value specifying the length of the IPv6 address prefix.

next-hop-ipv6-address

IPv6 address of the next-hop gateway.

next-hop-vrf *vrf_name next-hop-ipv6-address*

Specifies a VRF instance and a next-hop IPv6 address.

metric

Specifies a value that the Layer 3 switch uses to compare this route to other static routes in the IPv6 static route table that have the same destination. The metric applies only to routes that the Layer 3 switch has already placed in the IPv6 static route table. Two or more routes to the same destination with the same metric will load share (as in ECMP load sharing). The range is from 1 through 16. The default is 1.

distance *number*

Specifies an administrative distance. The range is from 1 through 254. The default is 1. This is a value that the Layer 3 switch uses to compare this route with routes from other route sources that have the same destination. By default, static routes take precedence over routes learned by routing protocols. To choose a dynamic route over a static route, configure the static route with a higher administrative distance than the dynamic route. A distance of 255 is considered unreachable.

tag

Specifies a tag value for the route. The route tag can be used for route redistribution to routing protocols by means of route maps (as in IPv4 static route redistribution).

tag-number

A number from 0 through 4294967295. The default is 0.

Modes

Global configuration mode

VRF configuration mode

Usage Guidelines

Use the **no** form of the command with the same parameters to remove the IPv6 static route.

Related commands:

- **ipv6 route**
- **ipv6 route** null

Examples

The following example creates an IPv6 static route to IPv6 2001:DB8::0/32 destinations through the VRF named "partners" and the next-hop router with the IPv6 address 2001:DB8:0:ee44::1.

```
device# configure terminal
device(config)# ipv6 route 2001:DB8::0/32 next-hop-vrf partners 2001:DB8:0:ee44::1
```

ipv6 route static bfd

Configures Bidirectional Forwarding Detection (BFD) session parameters for IPv6 static routes.

Syntax

ipv6 route static bfd *dest-ipv6-address source-ipv6-address* [*interface-type interface-name*] [**interval** *transmit-time* **min-rx** *receive-time* **multiplier** *number*]

no ipv6 route static bfd *dest-ipv6-address source-ipv6-address* [**interfacetype** *interface-name*]

no IPv6 route static bfd *dest-ipv6-address source-ipv6-address* [**interfacetype** *interface-name*] [**interval** *transmit-time* **min-rx** *receive-time* **multiplier** *number*]

Command Default

By default, BFD is not configured for an IPv6 static route.

Parameters

dest-ipv6-address

Specifies the IPv6 address of BFD neighbor.

source-ipv6-address

Specifies the source IPv6 address.

interface-type

The type of interface, such as Ethernet or Ve.

interface-name

The interface number or VLAN ID.

interval*transmit-time*

Specifies the interval, in milliseconds, a device waits to send a control packet to BFD peers. Valid values range from 50 through 30000. The default is 300 milliseconds.

min-rx *receive-time*

Specifies the interval, in milliseconds, a device waits to receive a control packet from BFD peers. Valid values range from 50 through 30000. The default is 300 milliseconds.

multiplier *number*

Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD determines that the connection to that peer is not operational. Valid values range from 3 through 50. The default is 3.

Modes

Global configuration mode

Address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the no form of this command without the *interval* parameter to remove the configured BFD IPv6 static route.

Use the no form of this command with the *interval* parameter to revert the configured interval value to the default value.

The *transmit-time* and *receive-time* variables are the intervals needed by the local device. The actual values in use will be the negotiated values.

For single-hop static BFD sessions, the interval value is taken from the outgoing interface. For multi-hop BFD sessions, if the configured **interval** and **min-rx** parameters conflict with those of an existing session, the lower values are used.

For IPv6 static BFD sessions, if the BFD neighbor is link-local, the source IPv6 address must also be link-local.

If an IPv6 BFD session is running for a link-local BFD neighbor, the *interface-type interface-name* parameters are mandatory because the link-local address can be the same on multiple interfaces.

Examples

This example configures a BFD session on an IPv6 static route, specifying a VE interface.

```
device# configure terminal
device(config)# ipv6 route static bfd fe80::a fe80::b ve 20 interval 100 min-rx 100
multiplier 10
```

This example configures a BFD session on an IPv6 static route in a non-default VRF instance.

```
device# configure terminal
device(config)# vrf orange
device(config-vrf-orange)# address-family ipv6 unicast
device(vrf-ipv6-unicast)# ipv6 route static bfd fe70::a fe60::b ve 10 interval 1000 min-
rx 2000 multiplier 20
```

ipv6 route static bfd holdover-interval

Sets the time interval for which BFD session DOWN notifications are delayed before an IPv6 static route is notified that a BFD session is down.

Syntax

ipv6 route static bfd holdover-interval *time*

no ipv6 route static bfd holdover-interval

Command Default

By default, the BFD holdover interval is 0 seconds.

Parameters

time

Specifies the BFD holdover-time interval in seconds. Valid values range from 1 through 30. The default is 0.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of the command to revert to the default value of 0.

If the BFD session is restored within the specified time interval, no DOWN notification is sent.

Holdover interval values are configured globally and apply to all VRFs.

Examples

This example sets the BFD holdover interval globally for IPv6 static routes to 25.

```
device# configure terminal
device(config)# ipv6 route static bfd holdover-interval 25
```

This example removes the configured BFD holdover interval for IPv6 static routes.

```
device# configure terminal
device(config)# no ipv6 route static bfd holdover-interval
```

ipv6 router isis

Enables Intermediate System-to-Intermediate System (IS-IS) routing at the interface level.

Syntax

ipv6 router isis

Command Default

Disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only..

The **no** form of the command disables IS-IS routing for the interface.

Examples

The following example enables IS-IS routing for an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# ipv6 router isis
```

ipv6 router ospf

Enables and configures the Open Shortest Path First version 3 (OSPFv3) routing protocol.

Syntax

ipv6 router ospf [**vrf** *name*]

no ipv6 router ospf

Command Default

Disabled.

Parameters

vrf *name*

Specifies a nondefault VRF.

Modes

Global configuration mode

Usage Guidelines

If you save the configuration to the startup-config file after disabling OSPFv3, all OSPFv3 configuration information is removed from the startup-config file.

Use this command to enable the OSPFv3 routing protocol and enter OSPFv3 router or OSPFv3 router VRFconfiguration mode. OSPFv3 maintains multiple instances of the routing protocol to exchange route information among various VRF instances.

The **no** form of the command deletes all current OSPFv3 configurations and blocks any further OSPFv3 configuration.

Examples

The following example enables OSPFv3 on a default VRF and enters OSPFv3 router configuration mode.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)#
```

ipv6 router pim

Globally enables PIM routing for IPv6 and enters IPv6 PIM router configuration mode for the default virtual routing and forwarding (VRF) or the specified VRF.

Syntax

ipv6 router pim vrf [*VRF-name*]

no ipv6 router pim vrf [*VRF-name*]

Command Default

By default, IPv6 PIM routing is disabled.

Parameters

vrf*VRF-name*

Specifies the VRF for which you want to enable or disable IPv6 PIM. If no VRF is specified, the default VRF is used.

Modes

Global configuration mode

Usage Guidelines

The **no ipv6 router pim** form of the command disables IPv6 PIM routing.

Protocol-Independent Multicast (PIM) is one of several protocols designed for IP multicast. PIM does not rely on a specific routing protocol to create its network topology state, but uses routing information from other protocols. PIM messages are sent encapsulated in an IP packet where the IP protocol is 103 and the version is 6 for IPv6. Depending on the type of message, packets are sent to the PIM All-Router-Multicast address (FF02::D) or sent as unicast to a specific host.

Examples

The following example enables IPv6 PIM and enters IPv6 PIM router configuration mode for the default VRF.

```
device# configure terminal
device(config)# ipv6 router pim
device(config-ipv6-router-pim-vrf-default-vrf)#
```

ipv6 prefix-list

Configures an IPv6 prefix list for basic traffic filtering

Syntax

ipv6 prefix-list *name* **deny** *ipv6-prefix/prefix-length* [**ge** *ge-value*] [**le** *le-value*]

ipv6 prefix-list *name* **permit** *ipv6-prefix/prefix-length* [**ge** *ge-value*] [**le** *le-value*]

ipv6 prefix-list *name* **seq** *instance-number* { **deny ge** *ge-value* **le** *le-value* | **permit ge** *ge-value* **le** *le-value* }

no ipv6 prefix-list *name*

Parameters

name

Specifies the prefix list name.

deny *ip-prefix/prefix-length*

Denies a route specified in the prefix list. The prefix list matches only on the specified prefix/prefix length, unless you use the **ge** *ge-value* or **le** *le-value* parameters.

ge *ge-value*

Specifies minimum prefix length to be matched. The range is from *ge-value* to 128.

le *le-value*

Specifies maximum prefix length to be matched. The range is from the *le-value* to the *prefix-length* parameter.

permit *ip-prefix/prefix-length*

Permits a route specified in the prefix list. The prefix list matches only on the specified prefix/prefix length, unless you use the **ge** *ge-value* or **le** *le-value* parameters.

seq

Specifies an IPv6 prefix list sequence number of entry.

instance

Specifies an IPv6 prefix list instance number.

Modes

Global configuration mode

Usage Guidelines

An IPv6 prefix list is composed of one or more conditional statements that execute a permit or deny action if a route matches a specified prefix. In prefix lists with multiple statements, you can specify a sequence number for each statement. The specified sequence number determines the order in which the statement appears in the prefix.

You can configure an IPv6 prefix list on a global basis, then use it as input to other commands or processes, such as route aggregation, route redistribution, route distribution, route maps, and so on. When an SLX-OS device interface sends or receives an IPv6 packet, it applies the statements within the IPv6 prefix list in their order of appearance to the packet. As soon as a match occurs, the device takes the specified action (permit or deny the packet) and stops further comparison for that packet.

You can use permit statements in the prefix list to specify the traffic that you want to send to the other feature. If you use deny statements, the traffic specified by the deny statements is not supplied to the other feature. You can configure up to one hundred IPv6 prefix lists.

You must specify the ipv6-prefix parameter in hexadecimal using 16-bit values between colons as documented in RFC 4291. You must specify the prefix-length parameter as a decimal value. A slash mark (/) must follow the ipv6-prefix parameter and precede the prefix-length parameter.

The *ge-value* or *le-value* you specify must meet the following condition for *prefix-length* :

```
 ge-value <= le-value <= 128
```

Examples

The following example creates a prefix-list that allows routes with the prefix 2001:db8::/32 .

```
device# configure terminal
device(config)# ipv6 prefix-list route1 permit 2001:db8::/32
device(config)# interface ethernet 2/1
device(conf-if-eth-2/1)# ipv6 prefix-list route1
```

ipv6 subnet-zero drop

Drops packets destined for IPv6 subnet-router anycast addresses.

Syntax

ipv6 subnet-zero drop

no ipv6 subnet-zero drop

Command Default

By default, packets destined for IPv6 subnet-router anycast addresses are allowed.

Modes

Global configuration mode

Usage Guidelines

When you have previously used the **ipv6 subnet-zero drop** command to drop packets destined for IPv6 subnet-router anycast addresses, use the **no** form of the command to restore the default configuration and allow IPv6 subnet anycast address traffic.

Examples

The following example configures dropping packets destined for IPv6 subnet anycast addresses.

```
device# configure terminal
device(config)# ipv6 subnet-zero drop
```

ipv6 vrrp-extended auth-type

Configures the type of authentication used on a Virtual Router Redundancy Protocol Extended (VRRP-E) interface.

Syntax

ipv6 vrrp-extended auth-type md5-auth *auth-text*

no ipv6 vrrp-extended auth-type md5-auth

Command Default

No authentication is configured for a VRRP-E interface.

Parameters

md5-auth *auth-text*

Configures MD5 authentication on the interface. The maximum length of the text string is 64 characters.

Modes

Virtual Ethernet (VE) interface configuration mode

Usage Guidelines

This configuration is for VE interfaces only.

If the **md5-auth** option is configured, syslog and SNMP traps are generated if a packet is being dropped due to MD5 authentication failure. Using MD5 authentication implies that the software does not need to run checksum verification on the receiving device and can rely on the authentication code (message digest 5 algorithm) to verify the integrity of the VRRP-E message header.

The **no** form of this command removes the VRRP-E authentication from the interface.

Examples

The following example configures MD5 authentication on VE interface 20.

```
device(config)# ipv6 protocol vrrp-extended
device(config)# interface ve 20
device(config-if-Ve-20)# ipv6 vrrp-extended auth-type md5-auth lyk28d3j
```

ipv6 vrrp-extended-group

Configures an IPv6 VRRP-Ev3 group and enters into the VRRP-E configuration mode.

Syntax

ipv6 vrrp-extended-group *group-ID*

no ipv6 vrrp-extended-group *group-ID*

Parameters

group-ID

A number from 1 through 255 that you assign to the VRRP-Ev3 group.

Modes

Virtual Ethernet (VE) interface configuration mode

Usage Guidelines

Enter **no ipv6 vrrp-extended-group** *group-ID* to remove the specific IPv6 VRRP-Ev3 group. If you remove a group, you cannot retrieve it. You would have to redo the configuration procedure.

This configuration is for virtual Ethernet (VE) interfaces only. IPv6 VRRP-Ev3 must be enabled on the device before the IPv6 VRRP-E group is configured.

Examples

The following example shows how to assign the VE interface with a VLAN number of 2019 to the VRRP-Ev3 group with the ID of 19.

```
device# configure terminal
device(config)# ipv6 protocol vrrp-extended
device(config)# interface ve 2019
device(config-Ve-2019)# ipv6 address 2001:2019:8192::122/64
device(config-Ve-2019)# ipv6 vrrp-extended-group 19
device(config-vrrp-extended-group-19)#
```

ipv6 vrrp-group

Configures an IPv6 VRRPv3 group and enters into the virtual router configuration mode.

Syntax

ipv6 vrrp-group *group-ID*

no ipv6 vrrp-group *group-ID*

Parameters

group-ID

A value from 1 through 255 that you assign to the VRRPv3 group.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ipv6 vrrp-group** *group-ID* to remove a specific IPv6 VRRPv3 group. If you remove a group, you cannot retrieve it. You would have to redo the configuration procedure.

IPv6 VRRPv3 must be enabled on the device before the IPv6 VRRP group is configured.

Examples

The following example shows how to assign an Ethernet interface to the VRRPv3 group with the ID of 18.

```
device# configure terminal
device(config)# ipv6 protocol vrrp
device(config)# interface ethernet 1/6
device(config-if-eth-1/6)# ipv6 address 2001:2019:8192::125/64
device(config-if-eth-1/6)# ipv6 vrrp-group 18
device(config-vrrp-group-18)#
```

ipv6 vrrp-suppress-interface-ra

Suppresses interface router advertisement (RA) when VRRPv3 is configured on an interface.

Syntax

ipv6 vrrp-suppress-interface-ra

no ipv6 vrrp-suppress-interface-ra

Command Default

Interface RA is enabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no ipv6 vrrp-suppress-interface-ra** to remove the suppression of interface RA.

Router advertisements are sent by the VRRP master device and contain the link-local virtual IP address and the virtual MAC address. For network security reasons, if you do not want the MAC addresses of interfaces to be viewed, you can disable RA messages.

Examples

This example suppresses interface RA on a virtual Ethernet (VE) interface:

```
device# configure terminal
device(config)# ipv6 protocol vrrp
device(config)# interface ve 2019
device(config-Ve-2019)# ipv6 vrrp-suppress-interface-ra
```

is-type

Changes the Intermediate System-to-Intermediate System (IS-IS) level globally.

Syntax

is-type { **level-1** | **level-1-2** | **level-2** }

no is-type { **level-1** | **level-1-2** | **level-2** }

Command Default

The device operates as both a Level 1 (intra-area) and a Level 2 (interarea) device.

Parameters

level-1

Specifies that the device performs only Level 1 (intra-area) routing.

level-1-2

Specifies that the device performs both Level 1 and Level 2 routing.

level-2

Specifies that the device performs only Level 2 (interarea) routing.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command enables support for both IS-IS levels, if one level has been disabled. Alternatively, the **level-1-2** parameter can be used.

Examples

The following example changes the IS-IS level globally to Level-1 only.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# is-type level-1
```

The following example changes the IS-IS level globally to Level-2 only.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# is-type level-2
```

The following example changes the IS-IS level globally to Level-1 and Level-2 if support for one level has previously been disabled.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# is-type level-1-2
```

isis auth-check

Enables authentication checking for an IS-IS interface.

Syntax

isis auth-check { **level-1** | **level-2** } **disable**

no isis auth-check { **level-1** | **level-2** } **disable**

Command Default

IS-IS authentication checking is enabled by default.

Parameters

level-1

Specifies Level 1 packets.

level-2

Specifies Level 2 packets.

disable

Disables authentication checking.

Modes

Interface subtype configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only..

The **no** form of the command disables IS-IS authentication checking for an IS-IS interface.

Examples

The following example disables IS-IS authentication checking for Level 1 packets for an IS-IS Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# isis auth-check disable
```

The following example re-enables IS-IS authentication checking for Level 2 packets for an IS-IS loopback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# isis auth-check
```

isis auth-key

Configures an authentication key for a specified Intermediate System-to-Intermediate System (IS-IS) interface.

Syntax

isis auth-key { **level-1** | **level-2** } *string*

no isis auth-key { **level-1** | **level-2** } *string*

Command Default

Disabled.

Parameters

level-1

Specifies Level 1 packets only.

level-2

Specifies Level 2 packets only.

string

Specifies a text string that is used as an authentication password. The string can be from 1 through 63 ASCII characters in length.

Modes

Interface subtype configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only..

The authentication mode must be configured on the interface using the **isis auth-mode** command before a *string* can be configured. If the authentication mode is reset, the authentication key must also be reset.

The **no** form of the command removes the configured authentication key for the IS-IS interface.

Note
MD5 passwords cannot have ASCII character 32 ('SPACE') as a part of the password string.

Examples

The following example configures an authentication key for Level 1 packets on an IS-IS Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# isis auth-key level-1 mykey
```

isis auth-mode

Specifies the type of authentication used for an Intermediate System-to-Intermediate System (IS-IS) interface.

Syntax

isis auth-mode md5 { **level-1** | **level-2** }

no isis auth-mode md5 { **level-1** | **level-2** }

Command Default

Disabled.

Parameters

md5

Specifies message Digest 5 (MD5) authentication.

level-1

Specifies Level 1 packets only.

level-2

Specifies Level 2 packets only.

Modes

Interface subtype configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command removes the configured authentication mode.

Examples

The following example specifies that MD5 authentication is performed on Level 1 packets on an IS-IS Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# isis auth-mode MD5 level-1
```

isis bfd

Enables Bidirectional Forwarding Detection (BFD) on a specific Intermediate System to Intermediate System (IS-IS) interface.

Syntax

isis bfd

no isis bfd

Modes

Interface subtype configuration mode

Usage Guidelines

IS-IS is supported only on devices based on the DNX chipset family. For a list of such devices, see "Supported Hardware".

BFD sessions are initiated only if BFD is also enabled globally using the **bfd** command in IS-IS router configuration mode. If BFD is disabled using the **no bfd** command in IS-IS router configuration mode, BFD sessions on specific IS-IS interfaces are deregistered.

The **no** form of the command removes all BFD sessions from a specified interface.

Examples

The following example enables BFD on an IS-IS Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/4
device(conf-if-eth-1/4)# isis bfd
```

The following example disables BFD on an IS-IS virtual Ethernet (VE) interface.

```
device# configure terminal
device(config)# interface ve 24
device(config-if-ve-24)# no isis bfd
```

isis circut-type

Configures the type of adjacency used for an Intermediate System-to-Intermediate System (IS-IS) interface.

Syntax

isis circut-type { **level-1** | **level-1-2** | **level-2** }

no circut-type { **level-1** | **level-1-2** | **level-2** }

Command Default

Level 1 and Level 2 adjacency is configured by default.

Parameters

level-1

Specifies Level 1 packets only.

level-1-2

Specifies Level 1 and Level 2 packets.

level-2

Specifies Level 2 packets only.

Modes

Interface subtype configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command resets the type of adjacency to the default value of Level 1 and Level 2 adjacency.

Examples

The following example configures Level 1 adjacency on an IS-IS Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-eth-1/1)# isis circut-type level-1
```

isis hello-interval

Specifies how often an Intermediate System-to-Intermediate System (IS-IS) interface sends hello messages to its IS-IS neighbors.

Syntax

isis hello-interval { **level-1** | **level-2** } *value*

no isis hello-interval { **level-1** | **level-2** } *value*

Command Default

Disabled.

Parameters

level-1

Configures the hello interval for Level 1 only.

level-2

Configures the hello interval for Level 2 only.

value

Specifies the interval. Valid values range from 1 through 63 seconds. The default is 10.

Modes

Interface subtype configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command resets the hello interval to the default value of 10 seconds.

Examples

The following example changes the hello interval for Level 1 packets to 20 on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# isis hello-interval level-1 20
```

The following example changes the hello interval for Level 2 packets to 40 on a loopback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# isis hello-interval level-2 20
```

isis hello-multiplier

Specifies the number of Intermediate System-to-Intermediate System (IS-IS) hello packets a neighbor must miss before the device declares adjacency as down.

Syntax

isis hello-multiplier { **level-1** | **level-2** } *multiplier*

no isis multiplier { **level-1** | **level-2** } *multiplier*

Command Default

The default is 3.

Parameters

level-1

Configures the hello multiplier for Level 1 adjacencies.

level-2

Configures the hello multiplier for Level 2 adjacencies.

multiplier

Specifies the multiplier. Valid values range from 3 through 1000. The default is 3.

Modes

Interface subtype configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The hello multiplier is the number by which an IS-IS interface multiplies the hello interval to obtain the hold time for Level-1 and Level-2 IS-IS hello PDUs.

The **no** form of the command restores the default of 10 seconds.

Examples

The following example changes the hello multiplier for Level 1 packets for an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# isis hello-multiplier level-1 10
```

The following example changes the hello multiplier for Level 2 packets for a loopback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# isis hello-mulitplier level-2 20
```

isis hello padding

Re-enables Intermediate System-to-Intermediate System (IS-IS) hello padding at the interface level.

Syntax

isis hello padding [**disable**]

no isis hello padding [**disable**]

Command Default

IS-IS hello padding is enabled.

Parameters

disable

Disables hello padding on the interface.

Modes

Interface subtype configuration mode

Usage Guidelines

IS-ISis supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Generally, you do not need to disable padding unless a link is experiencing slow performance. If you enable or disable padding on an interface, the interface setting overrides the global setting configured using the **hello padding** command.

The **no** form of the command disables hello padding.

Examples

The following example re-enables IS-IS hello padding on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-if-eth-1/1)# isis hello padding
```

isis ipv6 metric

Configures the metric value for an interface under IPv6 Intermediate System-to-Intermediate System (IS-IS) MT.

Syntax

isis ipv6 metric { **level-1** | **level-2** } *metric*

no ipv6 metric { **level-1** | **level-2** } *metric*

Command Default

The default is 10.

Parameters

level-1

Specifies Level 1 only.

level-2

Specifies Level 2 only.

multiplier

Specifies the metric value. Valid values range from 1 through 16777215. The default is 10.

Modes

Interface subtype configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Each IS-IS interface has a separate metric value. In IPv6 IS-IS MT, different metrics are configured on an interface for IPv4 and IPv6. When the metric value is configured for an interface, it rebuilds the route LSP and triggers IPv6 IS-IS MT SPF calculation.

The **no** form of the command resets the metric value to the default value of 10.

Examples

The following example changes the metric value for Level 1 packets for an Ethernet interface under IPv6 IS-IS MT to 25.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# isis ipv6 metric level-1 25
```

The following example changes the metric value for Level 2 packets for a loopback interface under IPv6 IS-IS MT to 60.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# isis ipv6 metric level-2 60
```

isis ldp-sync

Enables synchronization with Intermediate System-to-Intermediate System (IS-IS) for an interface.

Syntax

isis ldp-sync { **disable** | **enable**}

no isis ldp-sync { **disable** | **enable**}

Command Default

Disabled.

Parameters

`disable`

Disables LDP synchronization.

`enable`

Enables LDP synchronization.

Modes

Interface subtype configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command disables synchronization with IS-IS for an interface.

Examples

The following example enables LDP synchronization for an ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# isis ldp-sync enable
```

The following example disables LDP synchronization for a loopback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Looback-1)# isis ldp-sync disable
```

isis metric

Configures the value of an Intermediate System-to-Intermediate System (IS-IS) metric.

Syntax

isis metric { **level-1** | **level-2** } *metric*

no metric { **level-1** | **level-2** } *metric*

Command Default

The default is 10.

Parameters

level-1

Specifies Level 1 only.

level-2

Specifies Level 2 only.

metric

Specifies the metric. Valid values range from 1 through 63 for the narrow metric style (the default metric style for IPv4 ISIS). Valid values range from 1 through 16777215 for the wide metric style (the default metric style for IPv4 ISIS).

Modes

Interface subtype configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Each IS-IS interface has a separate metric value.

The device applies the interface-level metric to routes originated on the interface and when calculating routes. The device does not apply the metric to link-state information received from one intermediate system and flooded to other intermediate systems.

If the metric value you want to use is higher than 63 but you have not changed the metric style to wide, you must change the metric style first, and then set the metric. The IS-IS neighbors that receive the advertisements must also be enabled to receive wide metrics.

The **no** form of the command resets the metric value the default value of 10.

Examples

The following example changes the metric for an Ethernet interface, specifying Level 1 packets.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# isis metric 25 level-1
```

isis passive

Disables adjacency formation and advertisements on an Intermediate System-to-Intermediate System (IS-IS) interface.

Syntax

isis passive

no isis passive

Command Default

Adjacency formation and advertisements is disabled on loopback interfaces. Adjacency formation and advertisements is enabled on all other interfaces.

Modes

Interface subtype configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

A device advertises an IS-IS interface to its area regardless of whether adjacency formation is enabled.

The **no** form of the command re-enables adjacency formation and advertisements on the IS-IS interface.

Examples

The following example disables adjacency formation and advertisements on an Ethernet interface.

```
device#configure terminal
device(config)# interface ethernet 2/2
device(conf-if-eth-2/2)# isis passive
```

The following example enables adjacency formation and advertisements on a loopback interface.

```
device#configure terminal
device(config)# interface looback 1
device(config-Loopback-1)# no isis passive
```

isis point-to-point

Configures the network type for the Intermediate System-to-Intermediate System (IS-IS) interface as point-to-point.

Syntax

isis point-to-point

no isis point-to-point

Command Default

Disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command removes the configured point-to-point network type.

Examples

The following example configures a network type of point-to-point for an Ethernet interface.

```
device#configure terminal
device(config)# interface ethernet 2/2
device(conf-if-eth-2/2)# isis point-to-point
```

isis priority

Determines the priority of the interface for being elected as a Designated IS.

Syntax

isis priority { **level-1** | **level-2** } *value*

no isis priority { **level-1** | **level-2** } *value*

Command Default

The default is 64.

Parameters

level-1

Sets the priority for Level 1 only.

level-2

Sets the priority for Level 2 only.

value

Specifies the priority. Valid values range from 0 through 127. The default is 64.

Modes

Interface subtype configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

You can configure the same priority for both Level-1 and Level-2 or you can configure a different priority for each level. If two or more devices have the highest priority within a given level, the device with the highest MAC address becomes the Designated IS for that level.

You can set the IS-IS priority on an individual interface basis only. You cannot set the priority globally.

The **no** form of the command resets the priority value to the default value of 64.

Examples

The following example changes the priority for Level 1 packets for an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# isis priority level-1 100
```

The following example changes the hello multiplier for Level 2 packets for a loopback interface.

```
device# configure terminal
device(config)# interface loopback 1
device(config-Loopback-1)# isis priority level-2 80
```

isis reverse-metric

Configures the reverse metric value on a single Intermediate System-to-Intermediate System (IS-IS) interface.

Syntax

isis reverse-metric [*value*] [**te-def-metric**] [**whole-lan**]

no isis reverse-metric [*value*] [**te-def-metric**] [**whole-lan**]

Command Default

Disabled.

Parameters

value

Specifies the reverse metric value in metric style. The narrow metric range is from 1 through 63. The wide metric range is from 1 through 16777215. The default value is 16777214 irrespective of the metric style configured.

whole-lan

Specifies that the configured reverse metric value affects the entire LAN.

te-def-metric

Specifies that the device sends a traffic engineering (TE) default metric sub-type-length-value (TLV) within the reverse metric TLV.

Modes

Interface subtype configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

When the reverse metric value is configured, the local LSP is updated with the sum of the default metric and the reverse metric value. When the IS-IS neighbor routing device receives the reverse metric value through the IS hello, the neighbor router updates the cost to reach the original IS-IS router with the sum of default metric and the reverse metric value. This helps in shifting traffic to the other alternate paths.

If the **whole-lan** option is not enabled, the reverse metric value affects only the neighbor router. The **whole-lan** option takes effect only on the multi-access LAN. IS-IS point-to-point interfaces are not affected when the **whole-lan** option is enabled.

The **no** form of the command removes the entire reverse metric configuration. The no form of the command specified with the configured value resets the metric value to the default value of 16777214.

Examples

The following example configures a reverse metric value of 40 on an Ethernet interface. The **whole-lan** option is enabled to include the entire LAN.

```
device#configure terminal
device(config)# interface ethernet 2/2
device(conf-if-eth-2/2)# isis reverse-metric 40 whole-lan
```

iterations

For an implementation of an event-handler profile, specifies the number of times an event-handler action is run, when triggered.

Syntax

iterations *num-iterations*

no iterations

Command Default

When the trigger condition occurs, the event-handler actions runs once.

Parameters

num-iterations

Specifies the number of times an event-handler action is run, when triggered. Valid values are any positive integer.

Modes

Event-handler activation mode

Usage Guidelines

The **no** form of this command resets the **iterations** setting to the default 1 iteration.

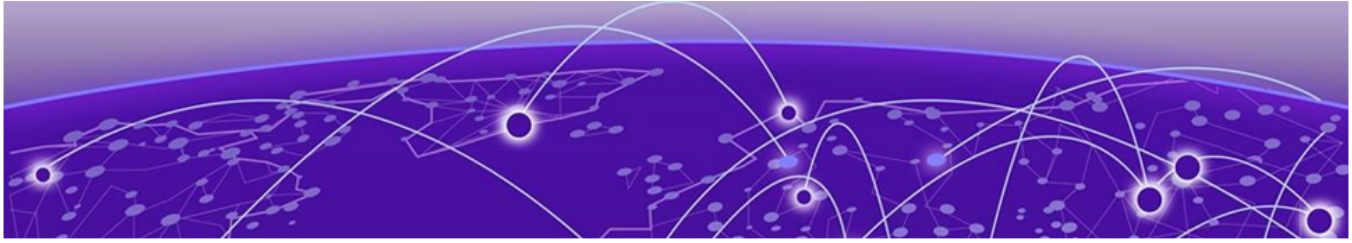
Examples

The following example specifies 5 iterations.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# iterations 5
```

The following example resets **iterations** to the default value of 1 iteration.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# no iterations
```



Commands K - M

ka-int-count on page 962
ka-interval on page 963
ka-timeout on page 965
key on page 967
key (keychain) on page 968
key-add-remove-interval on page 969
key-algorithm on page 970
key-rollover-interval on page 971
key-string on page 972
keychain on page 973
keypair on page 974
label-withdrawal-delay on page 975
lacp auto on page 977
lacp default-up on page 978
lacp port-priority on page 979
lacp system-id on page 980
lacp system-priority on page 981
lacp timeout on page 982
lacp-pdu-forward enable on page 983
lag hash on page 985
ldap-server host on page 989
ldap-server maprole on page 992
ldp on page 993
ldp-enable on page 994
ldp-params on page 995
ldp-sync on page 996
left-interface vlan on page 998
license add on page 1000
license eula on page 1002
line vty exec-timeout on page 1004
link-error-disable on page 1005
link-fault-signal on page 1007
link-oam allow-loopback on page 1009
link-oam enable on page 1010

link-oam remote-failure on page 1011
link-oam remote-loop-back on page 1012
listen-limit on page 1013
listen-range on page 1015
lldp profile on page 1017
load-balance hash on page 1018
load-sharing on page 1022
local-as on page 1023
local-switching on page 1024
log (OSPFv2) on page 1025
log (OSPFv3) on page 1027
log adjacency on page 1029
log invalid-lsp-packets on page 1030
log-dampening-debug on page 1031
log-shell on page 1032
logging auditlog class on page 1033
logging raslog console on page 1034
logging raslog console stop on page 1035
logging syslog-facility local on page 1036
logging syslog-server on page 1037
logging syslog-server-host on page 1039
logging utility on page 1041
logical-interface on page 1043
loopback phy on page 1046
loop-detection on page 1047
loop-detection shutdown-disable on page 1049
loop-detection vlan on page 1051
lsp on page 1052
lsp (Telemetry) on page 1053
lsp-gen-interval on page 1054
lsp-interval on page 1055
lsp-refresh-interval on page 1056
lsr-id on page 1057
lvtep broadcast-local-bias on page 1058
ma-name on page 1060
mac access-group on page 1062
mac access-list extended on page 1064
mac access-list standard on page 1065
mac-address withdrawal on page 1066
mac-address-table aging-time on page 1068
mac-address-table mac-move on page 1069
mac-address-table static on page 1071

maid-format on page 1073
maintenance-mode (Interface) on page 1074
management-heartbeat manager (management-heartbeat) on page 1075
management-security on page 1077
manual-switch vlan on page 1078
map bridge-domain (overlay gateway) on page 1079
map cos to cos on page 1080
map dscp on page 1082
map vlan on page 1084
map vni auto (VXLAN gateway) on page 1086
master-vlan (STP) on page 1087
match (route maps) on page 1088
match access-group on page 1092
match additional-paths advertise-set on page 1093
match as-path on page 1095
match bridge-domain on page 1096
match community on page 1097
match destination-port on page 1098
match dscp on page 1100
match extcommunity on page 1102
match fragment-type on page 1103
match ip on page 1105
match ip address acl on page 1106
match ip icmp-code on page 1107
match ip icmp-type on page 1109
match ipv6 address on page 1111
match ipv6 address acl on page 1112
match large-community on page 1113
match packet-length on page 1114
match port on page 1116
match protocol on page 1118
match rpki on page 1121
match source-port on page 1123
match tcp-flags on page 1125
match vlan on page 1128
max-age on page 1129
max-bypasses on page 1131
max-bypasses-per-mp on page 1133
max-lsp-lifetime on page 1135
max-mcache on page 1136
max-metric router-lsa on page 1137
max-metric router-lsa (OSPFv3) on page 1139

max-neighbor-reconnect-time on page 1141
max-neighbor-recovery-time on page 1142
maxas-limit on page 1143
maximum-paths (BGP) on page 1144
maximum-paths (IS-IS) on page 1146
maximum-paths (OSPF) on page 1147
maximum-paths ebgp ibgp on page 1148
measured-boot on page 1150
measurement-interval on page 1151
med-missing-as-worst on page 1152
member (cluster) on page 1153
member-bridge-domain on page 1155
member-vlan (STP) on page 1156
mep on page 1157
message-interval on page 1159
message-interval on page 1160
metric on page 1161
metric-style wide on page 1162
metric-type on page 1163
minimum-links on page 1164
mip-policy on page 1166
mode (LLDP) on page 1167
mode gre ip on page 1168
monitor session on page 1169
mpls reoptimize on page 1171
mpls-interface on page 1172
mtu (interface) on page 1173
mtu (PW) on page 1175
mtu-enforce on page 1176
multipath on page 1177
multiplier (LLDP) on page 1179
multiplier (UDLD) on page 1180
multi-topology on page 1181
mvrp applicant-mode on page 1182
mvrp enable on page 1184
mvrp registration-mode forbidden vlan on page 1186
mvrp timer on page 1188

ka-int-count

Configures the number of keepalive intervals after which the session is terminated when no session keepalive or other LDP protocol message is received from the LDP peer.

Syntax

ka-int-count *number*

no ka-int-count *number*

Command Default

The default is a count of six intervals.

Parameters

number

Specifies the number of keepalive time intervals. Enter an integer from 1 to 65535.

Modes

MPLS LDP configuration mode

Usage Guidelines

Use the **no** form of the command to reset the default count of six intervals.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures a keepalive interval count of three.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# ka-int-count 3
```

ka-interval

Sets the keepalive time interval at which the session keepalive message is sent when no other LDP protocol message is sent to the LDP peer.

Syntax

ka-interval *seconds*

no ka-interval *seconds*

Command Default

The default is six seconds.

Parameters

seconds

Specifies the keepalive time interval in seconds. Enter an integer from 1 throughk 65535.

Modes

MPLS LDP configuration mode

Usage Guidelines

The **ka-interval** and the **ka-timeout** configurations are mutually exclusive and you may have only one configured at a time. You must explicitly remove the configuration for one in order to change to the other configuration.

When the keepalive timeout value is configured, the **show mpls ldp** command displays keepalive interval as keepalive timeout divided by the keepalive interval count (ka-timeout/ka-in-count).

A message is displayed whenever the **ka-interval** value is changed.

```
"Please clear LDP sessions for the new KA parameter value to take effect on existing
sessions"
```

Use the **no** form of the command to reset the default of six seconds.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures a keepalive interval of 10 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# ka-interval 10
```

ka-timeout

Sets the keepalive timeout after which the session is terminated when the keepalive or LDP protocol message is not received.

Syntax

ka-timeout *seconds*

no ka-timeout *seconds*

Command Default

The default is six seconds.

Parameters

seconds

Specifies the keepalive timeout in seconds. Enter an integer from 1 to 65535.

Modes

MPLS LDP configuration mode

Usage Guidelines

After an LDP session is established, an LSR maintains the integrity of the session by sending keepalive messages. The keepalive timer for each peer session resets whenever it receives any LDP protocol message or a keepalive message on that session. When the keepalive timer expires, LDP concludes that the TCP connection is bad or the peer is dead and terminates the session.

When the keepalive timeout value is configured, the **show mpls ldp** command displays keepalive interval as keepalive timeout divided by the keepalive interval count (ka-timeout/ka-in-count).

The **ka-interval** and the **ka-timeout** configurations are mutually exclusive and you may have only one configured at a time. You must explicitly remove the configuration for one in order to change to the other configuration.

A message is displayed whenever the **ka-timeout** value is changed.

```
"Please clear LDP sessions for the new KA parameter value to take effect on existing
sessions"
```

Use the **no** form of the command to reset the default timeout of six seconds.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures a keepalive timeout of 180 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# ka-timeout 180
```

key

Specifies a text string to be used as a shared secret between the device and the Remote Authentication Dial-In User Service (RADIUS) server.

Syntax

key *shared_secret*

no key

Command Default

The default value is "sharedsecret".

Parameters

shared_secret

The text string that is used as the shared secret between the device and the RADIUS server. The default string is "sharedsecret". The exclamation mark (!) is supported for RADIUS servers, and you can specify the shared secret string in either double quotation marks or by using the escape character (\); for example, **"secret!key"** or **secret\!key**.

Modes

RADIUS server host VRF configuration mode

Usage Guidelines

The **key** command does not support an empty string.

The **no** form of the command restores the command default value.

Examples

The following example shows how to configure the text string "new#radius*secret" as the shared secret between the device and the RADIUS server.

```
device# configure terminal
device(config)# radius-server host 10.37.73.180 use-vrf green-vrf
device(config-host-10.37.73.180/green-vrf)# key "new#radius*secret"
```

key (keychain)

Configures a unique key ID in a key chain and enters key configuration mode.

Syntax

key *key-id*

no key *key-id*

Command Default

By default, a key ID is not configured.

Parameters

key-id

Specifies a unique key ID. Valid values range from 1 to 65535.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of the command to remove the specified key and all associated configuration.

You can configure no more than 8 keys per key chain.

Examples

The following example configures a key with an ID of 10 in key chain 1.

```
device# configure terminal
device(config)# keychain keychain1
device(config-keychain1)# key 10
device(config-keychain1-key10)#
```

key-add-remove-interval

Alters the timing of the authentication key add-remove interval.

Syntax

key-add-remove-interval *interval*

no key-add-remove-interval *interval*

Parameters

interval

Specifies the add-remove interval in seconds. Valid values range from 0 through 14400. The default is 300 seconds.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The **no** form of the command resets the add-remove interval to the default value of 300 seconds.

Examples

The following example sets the key add-remove interval to 240 seconds.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# key-add-remove-interval 240
```

key-algorithm

Defines the hash algorithm type for a specified key.

Syntax

key-algorithm { **HMAC-SHA-1** | **HMAC-SHA-256** | **HMAC-SHA-384** | **HMAC-SHA-512** }

no key-algorithm

Command Default

The default algorithm is HMAC SHA-256.

Parameters

HMAC-SHA-1 | **HMAC-SHA-256** | **HMAC-SHA-384** | **HMAC-SHA-512**

Specifies the hash algorithm for the selected key.

Modes

Key configuration mode

Usage Guidelines

Use the **no** form of the command to remove the hash algorithm configuration and revert to the default value.

Examples

The following example configures SHA-256 for key 10 in key chain 1.

```
device# configure terminal
device(config)# keychain keychain1
device(config-keychain1)# key 10
device(config-keychain1-key10)# key-algorithm HMAC-SHA-256
```

key-rollover-interval

Alters the timing of the existing configuration changeover.

Syntax

key-rollover-interval *interval*

no key-rollover-interval *interval*

Parameters

interval

Specifies the key-rollover-interval in seconds. Valid values range from 0 through 14400. The default is 300 seconds.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

In order to have consistent security parameters, rekeying should be done on all nodes at the same time. Use the **key-rollover-interval** command to facilitate this. The key rollover timer waits for a specified period of time before switching to the new set of keys. Use this command to ensure that all the nodes switch to the new set of keys at the same time.

The **no** form of the command resets the rollover interval to the default value of 300 seconds.

Examples

The following example sets the key rollover interval to 420 seconds.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# key-rollover-interval 420
```

The following example re-sets the key rollover interval to the default value.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# no key-rollover-interval 420
```

key-string

Configures a string of text to describe a key and, optionally, encrypts or decrypts the text string.

Syntax

key-string *text-string* [**encryption-level** { **0** | **7**}]

no key-string

Command Default

By default, no text string is configured.

Parameters

text-string

Describes the key with a maximum of 128 ASCII characters.

encryption-level { **0** | **7**}

Defines the encryption level for the text string. Enter 0 for plain text or 7 for encrypted. The default is 7.

Modes

Key configuration mode

Usage Guidelines

Use the **no** form of the command to remove the specified key and all associated configuration.You can remove a key only if it is not used by an application.

Examples

The following example configures a key string of Mystring1 for key 10 in key chain 1.

```
device# configure terminal
device(config)# keychain keychain1
device(config-keychain1)# key 10
device(config-keychain1-key10)# key-string Mystring1
```

The following example configures a key string of Mystring1 with an encryption level of 0 for key 10 in key chain 1.

```
device# configure terminal
device(config)# keychain keychain1
device(config-keychain1)# key 10
device(config-keychain1-key10)# key-string Mystring1 encryption-level 0
```

keychain

Creates a key chain and enters keychain configuration mode.

Syntax

keychain *chain-name*

no keychain *chain-name*

Command Default

By default, a key chain is not created.

Parameters

chain-name

Specifies an alphanumeric key chain name, with a minimum of 4 characters and a maximum of 32 characters.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of the command to remove the configuration for the key chain.

You can remove a key chain only if it is not used by any application.

You can create no more than 128 key chains.

Examples

The following example creates 3 key chains.

```
device# configure terminal
device(config)# keychain keychain1
device(config-keychain1)# exit
device(config)# keychain keychain2
device(config-keychain2)# exit
device(config)# keychain keychain3
device(config-keychain3)#
```

keypair

Associates the generated RSA/ECDSA/DSA key pair with a trust point for security protocol exchanges for applications.

Syntax

Associates the generated RSA/ECDSA/DSA key pair with the trust point.

keypair *key_label*

no keypair

Parameters

key_label

Specifies the name of the key pair to associate with the trust point.

Modes

Trust point configuration mode

Usage Guidelines

Use the **no keypair** command to remove the key pair association.

Examples

Typical command usage:

```
device(config)# crypto ca trustpoint t1
device(config-ca-t1)# keypair k1
device(config-ca-t1)# do show running-config crypto
 crypto key label k1 rsa modulus 2048
 crypto ca trustpoint t1
  keypair k1
!
device# show crypto ca trustpoint
trustpoint: t1; key-pair: k1
```

label-withdrawal-delay

CLI_section_description

Delays sending a label withdrawal message for a FEC to a neighbor in order to allow the IGP and LDP to converge.

Syntax

label-withdrawal-delay *secs*

no label-withdrawal-delay

Command Default

The default is 60.

Parameters

secs

Specifies the delay period in seconds for the label withdrawal delay timer. Enter value from 0 to 300.

Modes

MPLS LDP configuration mode.

Usage Guidelines

Setting the *secs* variable to zero (0) disables the feature for subsequent events.

Setting the *secs* variable to a value from 1 to 300, updates the configured value.

When using the **no** form of the command to restore the default behavior.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example sets the label withdrawal delay timer to 30 seconds.

```
device(config-router-mpls-ldp)# label-withdrawal-delay 30
```

The following example restores the command default behavior.

```
device(config-mpls-router-ldp)# no label-withdrawal-delay
```

The following example disables the label withdrawal delay timer.

```
device(config-mpls-router-ldp)# label-withdrawal-delay 0
```

lacp auto

Link Aggregation Control Protocol (LACP) enables bundling of multiple ethernet links into a single logical bundle that provides better performance and redundancy than single links. LCAP can only be configured on port-channel interfaces. Use this command to enable auto generation of ESI for these LACP configured port-channel interfaces. The ESI is a 10-octet Hexadecimal identifier based on LACP partner system identifier and port key. The same local port-channel id should be used by the multi-homed leaf peers on links connected to the same host.

Syntax

lacp auto

[no] lacp auto

Parameters

auto

Enable auto assignment of ESI to the LACP enabled port-channel interface.

Modes

Ethernet Segment mode within the port-channel interface mode.

This command is only available for Port Channels.

Usage Guidelines

Generates a 10-octet hexadecimal ESI value based on LACP partner system identifier and port key.

The *no* format of this command removes the ethernet segment identifier associated with this LACP port-channel.

Examples

The following example shows how to enable auto assignment of ESI for a LACP enabled port-channel interface.

```
SLX(config)# interface Port-channel 1
SLX(config-Port-channel-1)# ethernet-segment
SLX(config-Port-channel-1-es)# lacp auto
```

lacp default-up

Activates an Link Aggregation Control Protocol (LACP) link in the absence of PDUs.

Syntax

lacp default-up

no lacp default-up

Modes

Interface subtype configuration mode

Usage Guidelines

This command forces the port to activate an LACP link if there are no PDUs available on the interface port.

This command is supported on all physical interfaces.

This command is visible only if the interface is a dynamic and standard member of a port-channel.

This command is not supported on static LAGs.

Examples

The following example activates an LACP link in the absence of PDUs on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/11
device(conf-if-eth-0/11)# lacp default-up
```

lacp port-priority

Configures the Link Aggregation Control Protocol (LACP) port priority of a member port of a port-channel.

Syntax

lacp port-priority *value*

no lacp port-priority

Parameters

value

Specifies the priority. Valid values range from 1 through 65535. A lower number takes priority over a higher number. The default value is 32768.

Modes

Interface subtype configuration mode.

Usage Guidelines

An LACP port priority is configured on each port using LACP. The port priority determines which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

A link with higher priority (smaller in value) gets preference over a link with lower priority (greater in value).

The **no** form of the command returns the default value.

Examples

The following example sets the LACP port priority to 1000 for an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# lacp port-priority 1000
```

lacp system-id

The command is used to assign local LACP System ID. The same System ID should be used by both peers on the EVPN Multi-homing nodes.

Syntax

lacp system-id

[no] lacp system-id

Command Default

There are no defaults for this command.

Modes

Ethernet Segment mode. Allowed only under port-channel interface.

Usage Guidelines

This command is used to assign local LACP System ID. The same local port-channel id should be used by the peers (on EVPN Multi-homing nodes).

The **no** function removes the local ethernet segment identifier.

Examples

The following example enables the Ethernet Segment mode which is allowed only under port-channel interface.

```
SLX(config)# interface port-channel 1
SLX(config-Port-channel-1)# ethernet-segment
SLX(config-Port-channel-1-es)# lacp system-id 0011.2233.4455
```

lacp system-priority

Sets the Link Aggregation Control Protocol (LACP) system priority. The LACP priority determines which system is responsible for resolving conflicts in the choice of aggregation groups.

Syntax

lacp system-priority *value*

no lacp system-priority

Command Default

The default value is 32768.

Parameters

value

Specifies the value of the LACP system priority. Valid values range from 1 through 65535.

Modes

Global configuration mode

Usage Guidelines

Lower numerical values have higher priorities.

Enter **no lacp system-priority** to reset the system priority to the default value.

Examples

The following example sets the LACP system priority value to 68.

```
device# configure terminal
device(config)# lacp system-priority 68
```

lacp timeout

Sets the timeout value used by the Link Aggregation Control Protocol (LACP) to exchange packets on an interface before invalidating a received data unit (DU).

Syntax

lacp timeout { **long** | **short** }

no lacp timeout

Command Default

Tkhe default value is the **short** timeout.

Parameters

long

Specifies that a long-timeout value of 30 seconds will be used. With this value, the port waits three times this long (90 seconds) before invalidating the information received earlier on this PDU.

short

Specifies that a short-timeout value of one second will be used. With this value, the port waits three times this long (three seconds) before invalidating the information received earlier on this PDU.

Modes

Interface subtype configuration mode

Usage Guidelines

Use this command to set the timeout value based on how frequently you think the switch will receive LACP PDUs from the partner device.

Make sure that the LACP timeout is the same for all connected devices.

The **no** form of the command restores the default values.

Examples

The following example sets the LACP long-timeout value on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# lacp timeout long
```

lacp-pdu-forward enable

Configures the device to forward LACP PDUs received on an interface where LACP is not configured, to the VLAN on which the LACP PDUs are received.

Syntax

lacp-pdu-forward enable

no lacp-pdu-forward enable

Command Default

LACP PDUs received on an interface where LACP is not configured are discarded.

Modes

Interface subtype configuration mode

Usage Guidelines

LACP PDUs are forwarded only when they are received on a physical interface or static port channel interface. LACP PDUs cannot be forwarded if they are received on a LACP based dynamic port channel.

LACP PDU forwarding enabled on a static port channel applies to all the member ports.

When LACP is enabled on a port, it overrides LACP PDU forwarding configuration and the PDUs are trapped to CPU.

Enabling and disabling of BPDU drop on a bridge domain does not impact LACP PDU forwarding.

Caution
When using this command on a physical port or a static port-channel, consider the need and the use case. Using this command will flood PDUs and may affect other existing port-channels in the network.

lacp-pdu-forward cannot be enabled on any interface that is not a physical port or a static port-channel. When attempted, the message **%Error: Cannot enable LACP PDU Forwarding on a non-static Port-Channel.** is displayed.

Use the no form of the command to disable LACP PDU forwarding.

Examples

The following example configures LACP PDU forwarding on a physical interface.

```
device# configure terminal
device(config)# interface ethernet 4/1
device(conf-if-eth-4/1)# lacp-pdu-forward enable
```

The following example configures LACP PDU forwarding on a static port channel interface.

```
device# configure terminal
device(config)# interface port-channel 10
device(config-Port-channel-10)# lacp-pdu-forward enable
```

lag hash

Configures LAG and Layer 3 ECMP hashing parameters such as where to start picking headers for key generation, the number of headers to be considered, and so forth.

Syntax

lag hash { **bos** | **hdr-count** | **hdr-start** | **normalize** | **pwctrlword** | **rotate** | **speculate-mpls** | **srcport** }

lag hash bos { **skip** | **start** }

lag hash hdr-count *count*

lag hash hdr-start { **fwd** | **term** }

lag hash normalize

lag hash pwctrlword

lag hash rotate *rotate-number*

lag hash speculate-mpls { **enable** | **inner-eth** | **inner-ip-raw** | **inner-ip-tag** | **inner-ipv6-raw** | **inner-ipv6-tag** }

lag hash srcport

no lag hash bos

no lag hash hdr-count

no lag hash hdr-start

no lag hash normalize

no lag hash pwctrlword

no lag hash rotate

no lag hash speculate-mpls

no lag hash srcport

Parameters

bos

Ignore the entire MPLS label stack and use only the BOS label for hashing.

skip

Hash from the label following the BOS label.

start

(Default) Start the hash from the BOS label.

hdr-count *count*

Configures the number of headers to be considered for LAG hashing. Values range from 1 through 3. The default is 3.

hdr-start

Specifies where to start picking headers for the key generation.

fwd

(Default) Start from the inner header, which is used for forwarding the packet.

term

Start from the outer header, which is the header below the forwarding header and is the last terminated header.

normalize

Configures using the same hash in both directions. The default is disabled.

pwctrlword

Include the PW control word in hashing. The default is disabled.

rotate *rotate-number*

Configures hashing randomness. Values range from 0 through 15. The default is 3.

speculate-mpls

Enable MPLS speculate or Ethernet/IP.

enable

Enable Speculative MPLS.

inner-eth

Enable inner Ethernet header hash for L2VPN.

inner-ip-raw

Enable inner IPv4 header hash for L2VPN raw mode.

inner-ip-tag

Enable inner IPv4 header hash for L2VPN tag mode

inner-ipv6-raw

Enable inner IPv6 header hash for L2VPN raw mode

inner-ipv6-tag

Enable inner IPv6 header hash for L2VPN tag mode

srcport

Includes the source port in the hashing configuration. The default is not to include it.

Modes

Global configuration mode

Usage Guidelines

To restore default settings, use the **no** forms of these commands.

Table 13: Support Matrix

Command	Supported In	Not Supported In
lag hash bos	• SLX 9540 • SLX 9640	All other platforms
lag hash hdr-count	• SLX 9150 • SLX 9250 • SLX 9540 • SLX 9640 • Extreme 8520 • Extreme 8720	• SLX 9740 • Extreme 8820
lag hash hdr-start	• SLX 9150 • SLX 9250 • SLX 9540 • SLX 9640 • Extreme 8520 • Extreme 8720	• SLX 9740 • Extreme 8820
lag hash normalize	• SLX 9540 • SLX 9640 • SLX 9740 • Extreme 8820	All other platforms
lag hash pwctrlword	• SLX 9540 • SLX 9640	All other platforms
lag hash rotate	• SLX 9540 • SLX 9640 • SLX 9740 • Extreme 8820	All other platforms
lag hash speculate-mpls	• SLX 9540 • SLX 9640	All other platforms
lag hash srcport	• SLX 9150 • SLX 9250 • SLX 9540 • SLX 9640 • Extreme 8520 • Extreme 8720	• SLX 9740 • Extreme 8820

Examples

The following example changes the **hdr-count** value to 2.

```
device# configure terminal
device(config)# lag hash hdr-count 2
```

The following example changes the **hdr-start** value to term.

```
device# configure terminal
device(config)# lag hash hdr-start term
```

This following example is the output of the allowed configuration on an Extreme 8820 device.

```
SLX (config)# # lag hash ?
Possible completions:
 normalize  Enable/Disable using the same hash in both directions of a flow
 rotate   Hash Rotate
SLX (config)#
```

ldap-server host

Configures an LDAP server to connect for external or remote authentication.

Syntax

ldap-server host [**use-vrf** { **mgmt-vrf** | **default-vrf** |*vrf-name* }]

ldap-server host { *ipaddr* | *hostname* } [**port** *portnum*] [**ldaps**][**domain** *basedn*] [**timeout** *secs*] [**retries** *num*]

ldap-server host { *ipaddr* | *hostname* }[**source-interface** { **ethernet** *eth-id* | **loopback** *loopback-id* | **management** *mgmt-addr* | **ve** *ve-id* }]

no ldap-server host{ *ipaddr* | *hostname* }[**source-interface** { **ethernet** *eth-id* | **loopback** *loopback-id* | **management** *mgmt-addr* | **ve** *ve-id* }]

no ldap-server host { *ipaddr* | *hostname* } [**use-vrf** *vrf-name*]

Command Default

By default, the LDAP server is not configured.

Parameters

use-vrf

Specifies a VRF though which to communicate with the LDAP server.

mgmt-vrf

(Default) Specifies the management VRF.

default-vrf

Specifies the default-vrf.

vrf-name

Specifies a VRF name.

ipaddr | *hostname*

Specifies the IPv4 or IPv6 address or host name of the LDAP server. IPv6 is supported for Windows 2008 AD server only. The maximum supported length for the LDAP host name is 40 characters.

port *portnum*

Specifies the TCP port used to connect the LDAP server for authentication. The port range is from 1024 through 65535. By default, port 389 is used for the startTLS method and port 636 is used for LDAP over TLS.

ldaps

Specifies that LDAP over TLS is to be used instead of startTLS.

domain *basedn*

Describes the base domain name of the host.

timeout *secs*

Specifies the wait time for a server to respond. The range is 1 through 60 seconds. The default is 5 seconds.

retries *num*

Specifies the number of retries for the server connection. The range is 0 through 100. The default is 5.

source-interface

Indicates the type of interface to use as the source interface or address.
ethernet *eth-id*

Specifies the Ethernet interface to use as the source interface, in slot/port format (0/1).

loopback *loopback-id*

Specifies the Loopback interface to use as the source interface.

management *mgmt-addr*

Specifies the management address (active MM or chassis IP) to use as the source address.

ve *ve-id*

Specifies the VE interface to use as the source interface.

Modes

Global configuration mode

Usage Guidelines

Use this command to set up or change a connection to the Lightweight Directory Access Protocol (LDAP) server host. A maximum of 5 LDAP servers can be configured on a device.

Use the **no ldap-server host** form of the command to delete the server configuration.

When a source interface is not specified, the default source is the IP address of the interface from which the packet egresses.

If, at run time, the source interface is not up or the IP address for the source interface was not configured, the command behaves as though the source interface was not configured.

Invoking no on an attribute sets the attribute with its default value.

Examples

This example adds an LDAP server on port 3890 with retries set to 3.

```
device(config)# ldap-server host 10.24.65.6
device(config-host-10.24.65.6/mgmt-vrf)# domain sec.extreme.com port 3890 retries 3
```

This example changes the domain in an existing configuration.

```
device(config)# ldap-server host 10.24.65.6
 device(config-host-10.24.65.6/mgmt-vrf)# domain security.extreme.com
```

This example deletes an LDAP server.

```
device(config)# no ldap-server host 10.24.65.6
```

This example resets the retries attribute to the default value.

```
device(config)# ldap-server host 10.24.65.6
device(config-host-10.24.65.6/mgmt-vrf)# no retries
```

This example shows how attributes that hold default values are not displayed.

```
device(config-host-10.24.65.6/mgmt-vrf)# do show running-config ldap-server host
10.24.65.6
ldap-server host 10.24.65.6 use-vrf mgmt-vrf
port 3890 retries 3 timeout 8 basedn security.extreme.com
```

This example configures an Ethernet interface as the source interface.

```
device(config)# ldap-server host 10.1.1.100
 device(config-host-10.1.1.100/mgmt-vrf)# source-interface ethernet 0/1
```

This example configures a VE interface as the source interface.

```
device(config)# ldap-server host 10.1.1.100
 device(config-host-10.1.1.100/mgmt-vrf)# source-interface ve 10
```

ldap-server maprole

Maps an Active Directory (AD) group to a device role.

Syntax

ldap-server maprole group *group_name* **role** *role_name*

no ldap-server maprole group *group_name*

Parameters

group *group_name*

The name of the AD group.

role *role_name*

The name of the device role.

Modes

Global configuration mode

Usage Guidelines

Enter **no ldap-server maprolegroup** *group_name* without the **role** *role_name* parameter to remove the mapping of the AD group to a role.

Examples

To map the AD group "Administrator" to the device role "admin":

```
device(config)# ldap-server maprole group Administrator role admin
```

To remove the mapping:

```
device(config)# no ldap-server maprole group Administrator
```

ldp

Enables the Label Distribution Protocol (LDP) mode to configure LDP global parameters.

Syntax

ldp

no ldp

Modes

MPLS configuration mode

Usage Guidelines

Use the **no** form of this command to remove the LDP configurations from the device.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example enables LDP configuration mode.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
```

ldp-enable

Enables LDP on an interface.

Syntax

ldp-enable

no ldp-enable

Modes

MPLS interface configuration mode

Usage Guidelines

For an LDP session between routers, you must configure LDP on an interface to allow the device to advertise its loopback interface to the peers.

To use LDP, configure a loopback address with a 32-bit mask on the LSR. The first loopback address configured on the device is used in its LDP identifier. When the loopback address used in the LDP identifier is removed, all LDP functions on the LSR are shut down. LDP sessions between the LSR and its peers are terminated, and LDP-created tunnels are removed. When other loopback interfaces are configured on the device, the lowest-numbered loopback address is used as a new LDP identifier. LDP sessions and tunnels are set up using this new LDP identifier.

Configure LDP on the same set of interfaces that IGP routing protocols such as OSPF and IS-IS are enabled.

Use the **no** form of the command to disable LDP on the interface.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures LDP on an interface.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/2
device(config-router-mpls-interface-0/2)# ldp-enable
```

ldp-params

Allows you to access ldp-params subconfiguration mode to configure LDP parameters on an interface.

Syntax

ldp-params

no ldp-params

Modes

MPLS interface configuration mode

Usage Guidelines

When you use this command, you can configure the LDP Hello interval and timeout parameters on the interface.

Use the **no** form of the command to remove the LDP parameter configuration.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example accesses ldp-params subconfiguration mode.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/2
device(config-router-mpls-interface-0/2)# ldp-params
device(config-router-mpls-interface-0/2-ldp-params)#
```

ldp-sync

Enables Multiprotocol Label Switching (MPLS) Label Distribution Protocol-Interior Gateway Protocol (LDP-IGP) synchronization globally with Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF), and configures the hold-down time interval.

Syntax

ldp-sync [**hold-down** *seconds*]

no ldp-sync [**hold-down**]

Command Default

Disabled.

Parameters

hold-down *seconds*

Sets the LDP-IGP synchronization hold-down time interval in seconds. The IGP must advertise the maximum IP metric while waiting for an update from the LDP. Valid values range from 1 through 65535 seconds. The default is 30.

Modes

OSPF router configuration mode

IS-IS address-family IPv4 unicast configuration mode

Usage Guidelines

The **ldp-sync** command supports point-to-point interfaces, but not tunnel interfaces.

This command affects IPv4 metrics only.

When enabled on IS-IS, consider the following:

- The feature applies to both level-1 and level-2 metrics.
- The wide metric-style is required.

The **no ldp-sync** command disables LDP-IGP synchronization.

The **no ldp-sync hold-down** command resets the hold down time interval to the default setting of 30 seconds.

MPLS and IS-IS are supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example enables MPLS LDP-IGP synchronization globally with OSPF and IS-IS, and sets the hold-down time interval to 100 seconds.

```
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# ldp-sync
device(config-router-ospf-vrf-default-vrf)# ldp-sync hold-down 100
device(config-router-ospf-vrf-default-vrf)# exit
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# metric-style wide
device(config-router-isis-ipv4u)# ldp-sync
device(config-router-isis-ipv4u)# ldp-sync hold-down 100
```

left-interface vlan

Configures an Ethernet Ring Protection (ERP) left interface.

Syntax

left-interface vlan *vlan_id* { **ethernet** *slot/port* | **port-channel** *number* }

no left-interface vlan *vlan_id* { **ethernet** *slot/port* | **port-channel** *number* }

Command Default

No ERP left interface is configured by default.

Parameters

vlan_id

Specifies the VLAN ID of the ERP left ring interface. Range is from 1 through 4090.

ethernet *slot/port*

Specifies an Ethernet interface.

port-channel *number*

Specifies a port-channel.

Modes

ERP configuration mode

Usage Guidelines

Each Ethernet Ring Node (ERN) in a major ring must have explicitly defined left and right interfaces so that ERP can function properly. ERNs in a sub-ring must have at least one interface defined so that ERP can function properly.

For proper operation you must configure the interfaces following the same manner on each ERN, such as left/ right, left/ right, and so on.

The left interface is interface 0.

You must configure the VLAN and configure the Ethernet or port-channel interfaces as switchport, and then add the VLAN to the interfaces either in trunk or access mode. This is a prerequisite to configuring the ERP left interface.

Use the **no** form of this command to delete the configuration.

Examples

The following example configures a left interface on an Ethernet interface.

```
device# configure terminal
device(config)# erp 1
device(config-erp-1)# left-interface vlan 5 ethernet 0/1
```

license add

Adds a license key to a switch.

Syntax

license add { **licstr** *licenseString* | **FTP-URL** *ftpPath* | **SCP-URL** *scpPath* }
[**slot** *slot-number*]

Command Default

This command is executed on the local switch.

Parameters

licstr *licenseString*

Specifies the license string to be added to the switch. The license string must be enclosed in double quotation marks. A maximum of 256 characters is allowed.

FTP-URL *ftpPath*

Specifies a URL from which to transfer license information using FTP. ftp://*username*:*password*@*hostname filepath*

SCP-URL *scpPath*

Specifies a URL from which to transfer license information using SCP. scp://*username*:*password*@*hostname*/ *filepath*

slot *slot-number*

Specifies the LC slot number where the license key is added. The slot zero refers to the chassis license. The non-zero slot number refer to the physical slot number on the LC, as displayed in the output of the **show slot** command.

Modes

Privileged EXEC mode

Usage Guidelines

Depending on the feature being added, you may need to disable and re-enable the affected ports for this command to take effect. Follow the instructions in the command output.

If you install a license on an unsupported platform, the operation succeeds, but the **show license** output indicates that the license is not supported.

Examples

To add a license on slot 1:

```
device# license add SCP-URL scp://fvt:pray4green@10.70.5.58//users/home40/"pray4green/
20141113164801170PORT_UPGRADE.xml slot 1

License Added [*B
OXw:jFQ0IZc,t1D12:fZVuQByBOJMeqIoPhjpHK9gJLrcLzYIbEXVmDCd8N4nRyTfdxoGQI93gRS9ylO:cf00If68J
A1flHZzMQs4:eiIlC,VbOpx4E6UG8YeXWcaVIBSTVv#] Successfully - For license change to take
effect, it may be necessary to enable ports...
```

license eula

Enables the user to accept or decline the EULA for a SAU licensed feature.

Syntax

license eula { **accept** *feature* | **decline** *feature* }

Command Default

This command is executed on the local switch.

Parameters

accept

Specifies that the user wants to use the feature without an installed license.

feature

Specifies the displayed license feature name.

decline

Specifies that the user no longer want to use the unlicensed SAU feature.

Modes

Privileged EXEC mode.

Usage Guidelines

When the **license eula accept** command is entered, you are agreeing to purchase a license within a specific timeframe. You can begin using the features immediately. Use the **show license** command to display the SAU license when the EULA is accepted.

When the **license eula decline** command is entered, you are no longer able to use the licensed features. Before you can decline the licensed features, all configuration settings related to the feature must be restored to default settings.

Examples

The following example shows how to accept the EULA for the SAU license (Advanced Features).

```
device# license eula accept ADVANCED_FEATURES
2016/11/24-23:58:11, [SEC-1120], 41,, INFO, SLX9540, License EULA entry added for
ADVANCED_FEATURES feature (capacity 0).

EULA accepted for feature [ADVANCED_FEATURES]

Use of the ADVANCED_FEATURES feature requires a license to be purchased within 30 days.
By accepting the EULA you indicate that you have read and accept the Extreme End USER
```

```
License Agreement found at the following URL
[https://learn.extremenetworks.com/rs/641-VMV-602/images/Extreme-Networks-End-User-
License-Agreement.pdf].
You can decline the EULA acceptance now by entering "license
eula decline ADVANCED_FEATURES"
at the CLI prompt; declining the EULA will prevent use of the licensed feature.
```

The following example displays removing a SAU license (Advanced features).

```
device# license eula decline ADVANCED_FEATURES

 EULA removed for feature [ADVANCED_FEATURES]
```

The following CLI message is displayed when you attempt to configure a feature that requires a SAU license, and you have not accepted the EULA and there is no SAU license installed for that feature.

```
No ADVANCED_FEATURES EULA accepted for this feature
```

line vty exec-timeout

Sets the recurrent CLI idle timeout period.

Syntax

line vty exec-timeout *timeout*

no line vty exec-timeout

Command Default

If no value is specified, the timeout value is 10 minutes.

Parameters

timeout

Specifies the CLI session timeout period in minutes. The timeout value specifies the amount of time a CLI session can be idle before it logs you out. Valid values range from 0 through 136. The default is 10.

Modes

Global configuration mode

Usage Guidelines

The **line vty exec timeout** command is a recurrent command, applying to all login sessions. The **terminal timeout** command applies only to the current session.

Even if other keys are pressed during the timeout period, the only keystroke that prevents logout is **Enter**.

This command is supported only on the local device.

To restore the default timeout value of 10 minutes, enter **no line vty exec-timeout**.

Examples

The following example sets the terminal timeout to 60 minutes.

```
device(config)# line vty exec-timeout 60
device(config-line-vty)# exit
device(config)# exit
device# show running-config line vty
line vty
exec-timeout 60
!
```

link-error-disable

Configures port flap dampening for the interface, including the threshold of link flapping to shut down the port and the time interval in which it remains shut down.

Syntax

link-error-disable *toggle-threshold sampling-time-in-sec wait-time-in-sec*

no link-error-disable

Command Default

Port flap dampening is disabled on the device.

Parameters

toggle-threshold

Specifies the number of times a port link state goes from up to down and down to up before the wait period is activated. The value ranges from 1 through 50.

sampling-time-in-sec

Specifies the amount of time, in seconds, during which the specified toggle threshold can occur before the wait period is activated. Enter an integer from 1 through 65535.

wait-time-in-sec

Specifies the amount of time, in seconds, for which the port remains disabled (down) before it becomes enabled. The value ranges from 0 through 65535. A value of 0 indicates that the port will stay down until an administrative override occurs.

Modes

Interface Ethernet configuration mode

Usage Guidelines

Use the **no** form of the command to disable port flap dampening.

Port flap dampening allows you to configure a wait period before a port, whose link goes down then up, becomes enabled. This feature is available for all front ports on the device.

If the port link state toggles, from down to up or from up to down, for a specified number of times within a specified period, the interface is physically disabled for the specified wait period. Once the wait period expires, the port's link state is re-enabled. However, if the wait period is set to zero (0) seconds, or you want to re-enable the port before the wait period expires, the port must be manually re-enabled. To re-enable the port, reenter the **link-error-disable** command on the disabled port.

Examples

The following example shows the configuration of port flap dampening. The toggle threshold is set to 10 times. The sampling time is set to 3 seconds. The wait time is set to 10 seconds.

```
device# configure terminal
device(config)# interface Ethernet 1/4
device(conf-if-eth-1/4)# link-error-disable 10 3 10
```

link-fault-signal

Configures RX and TX Link Fault Signaling (LFS) detection globally or on an interface port.

Syntax

link-fault-signal rx { **off** | **on** } **tx** { **off** | **on**

no link-fault-signal

Command Default

Both TX and RX LFS are enabled.

Parameters

rx

Configure RX LFS detection.

off

Disables LFS.

on

Enables LFS.

tx

Configure TX LFS detection.

Modes

Global and interface configuration modes

Usage Guidelines

Use the **no** form of the command to reset RX and TX LFS to their default settings of enabled.

The interface must be in the shutdown state before you disable or enable TX LFS.

All SLX devices support LFS detection for interface types of 10G, 40G, 100G, and 40G breakout ports. It detects local and remote faults.

LFS is not supported in 1G mode.

When the device detects a local fault, it returns a remote fault to the link partner. When the device detects a remote fault, it returns an idle state.

A port's physical link detection is independent of LFS detection. When either of these link fault signals is detected, the following behaviors occur:

- The link is declared as DOWN and the management interface should display Protocol Down on the SLX-OS CLI.
- The physical link is not bought down in both of the previous cases. The peer side based on its implementation might display that the link is UP when the device displays that the link is DOWN due to a fault detection.
- The transmit (TX) packets, if any, are dropped at the MAC layer. The receive (RX) packets, if any, are dropped in the software.
- The detected signal is reported as a RASTRACE message. The same information is reported on the management interface as a RASLOG. The same behavior occurs when the signal is cleared.

You can enable or disable LFS globally and on the interface level for both RX and TX directions:

- If the LFS is enabled for RX, the normal local and remote fault detection and processing described previously occur. If it is disabled for RX, local and remote fault detection are ignored.
- If the LFS is enabled for TX and a local fault occurs, a remote fault (pause frame) is generated to the remote side. If it is disabled for TX, the remote fault is not generated.

The interface configuration overrides the global configuration.

Examples

The following example shows the global and interface configuration of LFS. In this example, the global LFS is disabled for the link fault RX and enabled for link fault TX. The LFS for the interface is enabled for the link fault RX and disabled for the link fault TX, overriding the global configuration.

```
device# configure terminal
device(config)# link-fault-signaling rx off tx on
device(config)# interface Ethernet 0/1
device(conf-if-eth-0/1)# shutdown
device(conf-if-eth-0/1)# link-fault-signaling rx on tx off
device(conf-if-eth-0/1)# no shutdown
```

link-oam allow-loopback

Enables an interface to accept remote loopback.

Syntax

link-oam allow-loopback

no link-oam allow-loopback

Command Default

Allow loopback is disabled.

Modes

Ethernet interface configuration mode

Usage Guidelines

You can allow loopback on one device port only.

To run this command, link OAM must be configured.

The **no** form of the command disables the interface from accepting loopback.

Examples

```
device# configure terminal
device(config)# interface ethernet 0/1
device(config-int-eth-0/1)# link-oam allow-loopback
```

link-oam enable

Enables link oam on an ethernet interface and sets the mode to active or passive.

Syntax

link-oam enable [**active** | **passive**]

no link-oam enable

Command Default

Please refer the usage guidelines.

Parameters

active

Configures link-oam in active mode.

passive

Configures link-oam in passive mode.

Modes

Ethernet interface configuration mode

Usage Guidelines

By default, link oam is disabled on the interface. Once this CLI is configured, it cannot be modified. In order to reconfigure, link-oam has to be deconfigured using **no link-oam enable** command.

Examples

```
device# configure terminal
device(config)# interface ethernet 1/1
device(config-int-eth1/1)# link-oam enable passive
```

link-oam remote-failure

Blocks the interface on receipt of a remote failure message, in addition to the syslog generation.

Syntax

link-oam remote-failure {**link-fault** | **dying-gasp** | **critical-event**} **action** *block-interface*

Command Default

Please refer the usage guidelines.

Parameters

link-fault

Blocks the interface on receipt of a link failure message.

dying-gasp

Blocks the interface on receipt of a dying-gasp message.

critical-event

Blocks the interface on receipt of a critical event message.

Modes

Ethernet interface configuration mode

Usage Guidelines

To run this command, the Link OAM must be configured. By default, on receipt of a remote failure message, the device will only log the event through syslog. This command allows block-interface action to be configured for each of the three events that the protocol supports.

Examples

```
device(config-int-eth1/1)# link-oam remote-failure link-fault action block-interface
device(config-int-eth1/1)# link-oam remote-failure dying-gasp action block-interface
```

link-oam remote-loop-back

Starts and stops the remote loopback on peer that is connected to a local ethernet interface.

Syntax

link-oam remote-loop-back ethernet *slot-number / port-number* [**start** | **stop**]

Parameters

slot-number

Specifies the slot number. For devices without linecards, specify `0`.

port-number

Specifies the port number.

start

Start the remote loopback on peer that is connected to the interface.

stop

Stops the remote loopback on peer that is connected to the interface.

Modes

Privileged EXEC mode

Examples

```
device# link-oam remote-loop-back ethernet 0/1 start
```

listen-limit

Sets a global limit for BGP4 or BGP4+ dynamic subnet range neighbors.

Syntax

listen-limit *max-num*

no listen-limit

Command Default

The default listen limit value is 100.

Parameters

max-num

Specifies the listen limit value. Valid values range from 1 through 255.

Modes

BGP configuration mode

Usage Guidelines

The **no** form of the command restores the default value.

When the global or peer level limit is increased, any new connection is accepted when it comes in from the remote end and falls under the range.

If the limit has been reached and you reduce the global or peer-group limit, the previously ESTABLISHED dynamic neighbors are not destroyed. You must use the **clear neighbor** command.

When the new sessions are created, the device uses the updated limit. If the limit has been reached and a request for new connection is received, the connections are not accepted and the information is logged.

Examples

The following example limits the number of BGP4 dynamic neighbors that can be created to 150 globally.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# listen-limit 150
**Warning: The dynamic neighbor range limit has been changed. Please use
clear bgp neighbor dynamic command for limit to take effect.
device(config-bgp-router)# clear ip bgp neighbor dynamic all
```

The following example restores the number of BGP4+ dynamic neighbors that can be created to the default value of 100.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# no listen-limit
**Warning: The dynamic neighbor range limit has been changed. Please use
clear bgp neighbor dynamic command for limit to take effect.
device(config-bgp-router)# clear ipv6 bgp neighbor dynamic all
```

listen-range

Associates a subnet range with a BGP4 or BGP4+ peer group and sets the maximum number of BGP dynamic neighbors that can be created for this range.

Syntax

listen-range *ip address/mask* **peer-group** *peer-group-name* [**limit** *num*]

no listen-range *ip address/mask* **peer-group** *peer-group-name*

Command Default

Disabled.

Parameters

ip address/mask

Specifies an IPv4 or IPv6 address and network mask.

peer-group *peer-group-name*

Specifies a peer group.

limit *num*

Specifies the listen limit value. Valid values range from 1 through 255.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command deletes the listen range and tears down all dynamic neighbors formed for this range.

Examples

This example associates a subnet range of 10.1.0.0/16 with a peer group called “mypeergroup” and sets the maximum number of BGP4 dynamic neighbors that can be created to 80.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# listen-range 10.1.0.0/16 peer-group mypeergroup limit 80
```

This example associates a subnet range of 2000:1:1::/48 with a peer group called "leaf-group."

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# listen-range 2000:1:1::/48 peer-group leaf-group
```

lldp profile

Applies a Link Layer Discovery Protocol (LLDP) profile to an interface.

Syntax

lldp profile *name*

no lldp profile

Command Default

LLDP profile name.

Parameters

name

Specifies the profile name. Valid profile name length is between 1 and 32 characters.

Modes

Interface subtype configuration mode

Usage Guidelines

You must use the **lldp profile** command to create an LLDP profile before you can apply the profile to the interface. Only one LLDP profile can exist at any time for a particular interface. When this command is not present, the parameters defined in the global LLDP configuration are used.

Enter **no lldp profile** to delete the profile from the interface.

Examples

To apply an LLDP profile called *test* on an specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 0/9
device(conf-if-eth-0/9)# lldp profile test
```

load-balance hash

For supported header types, selects the fields used for LAG and Layer 3 ECMP hashing.

Syntax

load-balance hash [**ethernet** | **ip** | **ipv6** | **l4** | **mpls**]

load-balance hash ethernet { **da-mac** | **etype** | **sa-mac** | **smac-dmac** | **vlan** }

load-balance hash ip { **dst-ip** | **dst-l4-port** | **protocol** | **sip-dip** | **src-ip** | **src-l4-port** }

load-balance hash ipv6 { **ipv6-dst-ip** | **ipv6-dst-l4-port** | **ipv6-next-hdr** | **ipv6-src-ip** | **ipv6-src-l4-port** | **sipv6-dipv6** }

load-balance hash l4 src-dst-port

load-balance hash mpls { **label1** | **label2** | **label3** | **all-labels** }

no load-balance hash [**ethernet** | **ip** | **ipv6** | **l4** | **mpls**]

no load-balance hash ethernet { **da-mac** | **etype** | **sa-mac** | **smac-dmac** | **vlan** }

no load-balance hash ip { **dst-ip** | **dst-l4-port** | **protocol** | **sip-dip** | **src-ip** | **src-l4-port** }

no load-balance hash ipv6 { **ipv6-dst-ip** | **ipv6-dst-l4-port** | **ipv6-next-hdr** | **ipv6-src-ip** | **ipv6-src-l4-port** | **sipv6-dipv6** }

no load-balance hash l4 src-dst-port

no load-balance hash mpls { **label1** | **label2** | **label3** | **all-labels** }

Command Default

All header parameters are enabled.

Parameters

ethernet

da-mac

Use Layer 2 destination address for hashing.

etype

Use **etype** option for hashing.

sa-mac

Use Layer 2 source address for hashing.

vlan

Use the **vlan** option for hashing.

smac-dmac

Use the source and destination MACs of the inner and outer headers for hashing.

ip

dst-ip

Use the destination IP address for hashing.

dst-l4-port

Use the destination Layer 4 port for hashing.

protocol

Use the IP protocol value for hashing.

sip-dip

Use the IPv4 Source IP and IPv4 Destination IP addresses of the inner and outer headers for hashing.

src-ip

Use the source IP address for hashing.

src-l4-port

Use the source Layer 4 port for hashing.

ipv6

ipv6-dst-ip

Use the destination IPv6 address for hashing.

ipv6-dst-l4-port

Use the IPv6 destination Layer 4 port for hashing.

ipv6-next-hdr

Use the next IPv6 header for hashing.

ipv6-src-ip

Use the source IPv6 address for hashing.

ipv6-src-l4-port

Use the IPv6 source Layer 4 port for hashing.

sipv6-dipv6

Use the IPv6 Source IP and IPv6 Destination IP addresses for hashing.

l4 src-dst-port

Use both the source and the destination ports in L4 header for calculating hash.

mpls

Not supported on SLX 9150 or SLX 9250 platforms

label1

Use only the MPLS label 1 for hashing.

label2

Use only the MPLS label 2 for hashing.

label3

Use only the MPLS label 3 for hashing.

all-labels

Use all the MPLS labels for hashing.

Modes

Global configuration mode

Usage Guidelines

The **no** forms of these commands cancel selection of the relevant protocol headers for LAG hashing.

Table 14: Support Matrix

Command	Supported In	Not Supported In
• load-balance hash ethernet etype • load-balance hash ethernet vlan	• All platforms	None
• load-balance hash ethernet da-mac • load-balance hash ethernet sa-mac	• Extreme 8720 • Extreme 8520 • SLX 9640 • SLX 9540 • SLX 9250 • SLX 9150	• Extreme 8820 • SLX 9740
• load-balance hash ethernet smac-dmac	• Extreme 8820 • SLX 9740	All other platforms
• load-balance hash ip protocol	• All platforms	None
• load-balance hash ip dst-ip • load-balance hash ip dst-l4-port • load-balance hash ip src-ip • load-balance hash ip src-l4-port	• Extreme 8720 • Extreme 8520 • SLX 9640 • SLX 9540 • SLX 9250 • SLX 9150	• Extreme 8820 • SLX 9740
• load-balance hash ip sip-dip	• Extreme 8820 • SLX 9740	All other platforms
• load-balance hash ipv6 ipv6-next-hdr	• All platforms	None
• load-balance hash ipv6 ipv6-dst-ip • load-balance hash ipv6 ipv6-dst-l4-port • load-balance hash ipv6 ipv6-src-ip • load-balance hash ipv6 ipv6-src-l4-port	• Extreme 8720 • Extreme 8520 • SLX 9640 • SLX 9540 • SLX 9250 • SLX 9150	• Extreme 8820 • SLX 9740
• load-balance hash ipv6 sipv6-dipv6	• Extreme 8820 • SLX 9740	All other platforms

Table 14: Support Matrix (continued)

Command	Supported In	Not Supported In
• load-balance hash l4 src-dst-port	• Extreme 8820 • SLX 9740	All other platforms
• load-balance hash mpls label1 • load-balance hash mpls label2 • load-balance hash mpls label3	• SLX 9540 • SLX 9640	All other platforms
• load-balance hash mpls all-labels	• Extreme 8820 • SLX 9740	All other platforms

Examples

The following example specifies Layer 2 destination address.

```
device# configure terminal
device(config)# load-balance hash ethernet da-mac
```

The following example cancels the default enablement of IPv4 headers for hashing. It then enables IPv4 source IP address only.

```
device# configure terminal
device(config)# no load-balance hash ip
device(config)# load-balance hash ip src-ip
```

load-sharing

Configures the maximum number of LDP ECMP paths.

Syntax

load-sharing *number*

no load-sharing

Command Default

The default number of ECMP paths is one.

Parameters

number

Specifies the maximum number of LDP ECMP paths. Enter an integer from 1 to 16.

Modes

MPLS LDP configuration mode

Usage Guidelines

The number of LDP ECMP paths for transit LSR depends on the number of eligible paths that are available, and the maximum number of LDP ECMP paths that you can configure.

Use the **no** form of this command to reset the default of one.

Examples

The following example configures a maximum of four LDP ECMP paths.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# load-sharing 4
```

local-as

Specifies the BGP autonomous system number (ASN) where the device resides.

Syntax

local-as *num*

no local-as *num*

Command Default

No ASN is specified.

Parameters

num

The local ASN. The range is from 1 through 4294967295.

Modes

BGP configuration mode

Usage Guidelines

ASNs in the range from 64512 through 65535 are private numbers that are not advertised to the external community.

The **no** form of the command removes the ASN from the device.

Examples

This example assigns a separate local AS number.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# local-as 777
```

local-switching

Configures the local switching mode for a bridge domain.

Syntax

local-switching

no local-switching

Command Default

Local switching is enabled.

Parameters

local-switching

Enables local switching.

Modes

Bridge-domain configuration mode.

Usage Guidelines

This feature is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Local switching allows packets to be switched within a VPLS bridge domain. This command only applies to multipoint-service bridge domains; that is, bridge domains configured with the **p2mp** option.

The **no** form of the command disables local switching in a VPLS bridge domain.

To avoid receipt of traffic with different VLAN tags on local endpoints in a bridge domain that has a PW profile with VC mode set to **raw-passthrough**, it is recommended that local switching is disabled. Raw passthorugh mode is designed to forward packets between two VPLS peer devices and is not intended for use with local switching.

Examples

The following example disables local switching in VPLS bridge domain 10.

```
device# configure terminal
device(config)# bridge-domain 10
device(config-bridge-domain-10)# no local-switching
```

log (OSPFv2)

Controls the generation of OSPFv2 logs.

Syntax

log { **adjacency** [**dr-only**] | **all** | **bad-packet** [**checksum**] | **database** | **retransmit** }

no log { **adjacency** [**dr-only**] | **all** | **bad-packet** [**checksum**] | **database** | **retransmit** }

Command Default

Only OSPFv2 messages indicating possible system errors are logged.

Parameters

adjacency

Specifies the logging of essential OSPFv2 neighbor state changes.

dr-only

Specifies the logging of essential OSPF neighbor state changes where the interface state is designated router (DR).

all

Specifies the logging of all syslog messages.

bad-packet

Specifies the logging of bad OSPFv2 packets.

checksum

Specifies all OSPFv2 packets that have checksum errors.

database

Specifies the logging of OSPFv2 LSA-related information.

retransmit

Specifies the logging of OSPFv2 retransmission activities.

Modes

OSPF router configuration mode

OSPF VRF router configuration mode

Usage Guidelines

Use this command to disable or re-enable the logging of specific events related to OSPFv2. If this command is not enabled only OSPFv2 messages indicating possible system errors are logged.

A limitation with the **dr-only** sub-option is that when a DR/BDR election is underway, OSPF neighbor state changes pertaining to non-DR/BDR routers are not logged. Logging resumes once a DR is elected on that network.

The **no** form of this command restores the default.

Examples

The following example enables the logging of all OSPFv2-related syslog events.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# log all
```

The following example enables the logging of OSPFv2 retransmission activities.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# log retransmit
```

log (OSPFv3)

Controls the generation of OSPFv3 logs.

Syntax

log { **adjacency** [**dr-only**] | **all** | **bad-packet** [**checksum**] | **database** | **retransmit** }

no log { **adjacency** | **all** | **bad-packet** [**checksum**] | **database** | **retransmit** }

Command Default

Only OSPFv3 messages indicating possible system errors are logged.

Parameters

adjacency

Specifies the logging of essential OSPFv3 neighbor state changes.

dr-only

Specifies the logging only of designated router (DR) interface adjacency changes.

all

Specifies the logging of all syslog messages.

bad-packet

Specifies the logging of bad OSPFv3 packets.

checksum

Specifies all OSPFv3 packets that have checksum errors.

database

Specifies the logging of OSPFv3 LSA-related information.

retransmit

Specifies the logging of OSPFv3 retransmission activities.

Modes

OSPFv3 router configuration mode

OSPFv3 VRF router configuration mode

Usage Guidelines

Use this command to disable or re-enable the logging of specific events related to OSPFv3. If this command is not enabled, only OSPFv3 messages indicating possible system errors are logged.

The **no** form of the command restores the default.

Examples

The following example enables the logging of all OSPFv3-related syslog events.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# log all
```

The following example enables the logging of OSPFv3 retransmission activities.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# log retransmit
```

log adjacency

Logs changes in the status of an adjacency with another intermediate system (IS).

Syntax

log adjacency

no log adjacency

Command Default

Disabled.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command disables the logging of adjacency changes.

Examples

The following example enables logging of adjacency changes.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# log adjacency
```

The following example disables logging of adjacency changes.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no log adjacency
```

log invalid-lsp-packets

Logs invalid Link State PDUs (LSPs) packets.

Syntax

log invalid-lsp-packets

no log invalid-lsp-packets

Command Default

Disabled.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command disables the logging of invalid LSP packets.

Examples

The following example enables logging of invalid LSP packets.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# log invalid-lsp-packets
```

The following example disables logging of invalid LSP packets.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no log invalid-lsp-packets
```

log-dampening-debug

Logs dampening debug messages.

Syntax

log-dampening-debug

no log-dampening-debug

Command Default

This option is disabled.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

The following example logs dampening debug messages.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# log-dampening-debug
```

log-shell

Controls the remote logging of SLXVM Linux shell command activities.

Syntax

log-shell { **start** | **status** | **stop** }

Command Default

By default, the device logs the SLXVM Linux shell access and all commands executed at the SLXVM Linux shell locally.

Parameters

start

Restarts remote logging.

status

Checks the remote logging status.

stop

Disables remote logging.

Modes

Privileged EXEC mode

Usage Guidelines

Changes of the **log-shell stop** and **log-shell start** commands are applicable only on new SLXVM Linux shell sessions.

If you configure a remote Syslog server, the same logs can be seen on this server.

When you disable remote logging, local logging of user activities continues.

Examples

The following example disables remote logging.

```
device# log-shell stop
```

The following example restarts remote logging.

```
device# log-shell start
```

logging auditlog class

Activates audit logging for various categories and classes of actions.

Syntax

logging auditlog class *class*

no logging auditlog class *class*

Command Default

CONFIGURATION, FIRMWARE, and SECURITY audit log classes are enabled.

Parameters

class

Specifies the class name of the audit log. Valid classes are CONFIGURATION, FIRMWARE, and SECURITY.

Modes

Global configuration mode

Usage Guidelines

The total message storage available is 2048 messages.

Enter **no logging auditlog class** *class* to disable the audit logging for the specified class.

Examples

To enable a specific audit log class:

```
device# configure terminal
device(config)# logging auditlog class security
device(config)#
```

logging raslog console

Sets the severity levels for the RASLog console.

Syntax

logging raslog console *severity*

no logging raslog console *severity*

Command Default

Severity level is INFO.

Parameters

severity

Specifies the minimum severity level of the message to pass through the filter. Valid values consist of one of the following: INFO, WARNING, ERROR, or CRITICAL. Input values are case-sensitive.

Modes

Global configuration mode

Usage Guidelines

The total message storage available is 2048 messages.

Examples

To reset the RASLog severity levels to the default value.

```
device# configure terminal
device(config)# no logging raslog console
2013/11/14-08:42:57, [RAS-3008], 5348, M2 | Active, INFO, VDX8770-4, Logging messages to
console has been reset by user.
```

logging raslog console stop

Temporarily stops displaying RASLog messages on the console.

Syntax

logging raslog console { **start** | **stop** [*minutes*] }

Command Default

RASlog messages display on the console

Parameters

start

Initiates RASLog messages.

stop *minutes*

Stops RASLog messages for a designated number of minutes.

Modes

Privileged EXEC mode

Usage Guidelines

When stopping or starting RASLog messages, the commands are not configuration commands and therefore are not persistent.

If the command **logging raslog console stop** *minutes* is invoked before the previous time value expires, the latest CLI duration applies.

Examples

To stop RASLog messages for 1 minute:

```
device# logging raslog console stop 1
Logging message have been blocked on console for 1 minutes
```

To start RASLog messages:

```
device# logging raslog console start
```

logging syslog-facility local

Configures the syslog facility.

Syntax

logging syslog-facility local *log_level*

Command Default

Syslog level is LOG_LOCAL7.

Parameters

log_level

Specifies the syslog facility level. Valid log levels include the following: LOG_LOCAL0, LOG_LOCAL1, LOG_LOCAL2, LOG_LOCAL3, LOG_LOCAL4, LOG_LOCAL5, LOG_LOCAL6, LOG_LOCAL7

Modes

Global configuration mode

Usage Guidelines

Use this command to configure the log level for all error log entries to forward to one or more specified syslog servers. You can configure up to four syslog servers.

Examples

To configure the syslog facility level:

```
device# configure terminal
device(config)# logging syslog-facility local LOG_LOCAL5
```

logging syslog-server

Configures a switch to forward system messages to the specified syslog servers.

Syntax

logging syslog-server *ip_address* [**use-vrf** *vrf-name*]

no logging syslog-server *ip_address* [**use-vrf** *vrf-name*]

Parameters

ip_address

Specifies the IP address of the syslog server in IPv4 or IPv6 format.

use-vrf *vrf-name*

Specifies a VRF through which to communicate with the server. See the Usage Guidelines.

Modes

Global configuration mode

Usage Guidelines

Use this command to configure a switch to forward all error log entries to the specified servers. You can configure up to four syslog servers; this includes all VRFs. You must execute the command for each server.

The **certutil import syslogca** command is required for a secure syslog to be fully functional.

After specifying the **ip_address** and **vrf-name**, the **secure** sub-command can be used to specify the secure default port (6514) or specify a secure non-default syslog server port. These sub-commands are only available after specifying the **ip_address** and **vrf-name** parameters.

Use the **no logging syslog-server** command with the optional use-vrf keyword to remove the specified IP address and VRF.

By default, all management services are enabled on the management VRF ("mgmt-vrf") and the default VRF ("default-vrf").

Examples

To configure a server IPv4 address to which system messages are sent on a user-specified VRF:

```
device# configure terminal
device(config)# logging syslog-server 192.168.163.233 use-vrf myvrf
device(config-syslog-server-192.168.163.233/myvrf)#
```

To configure a secure server with a non-default port nunber:

```
device(config)# logging syslog-server 1.1.1.1 use-vrf mgmt-vrf
device(config-syslog-server-1.1.1.1/mgmt-vrf)# secure port 6502
device(config-syslog-server-1.1.1.1/mgmt-vrf)#
```

Examples

To configure a CLI **source-interface** in the **logging syslog-server** option:

```
device (config-syslog-server-1.1.1.1/mgmt-vrf)# source-interface
Possible completions:
  ethernet     Use Ethernet interface as source interface
  loopback     Use Loopback interface as source interface
  management   Use Managment (Active MM or Chassis ip) as source address
  ve           Use ve interface as source interface
device (config-syslog-server-1.1.1.1/mgmt-vrf)# source-interface management
Possible completions:
  <NUMBER: 0-1>     1=Active-MM-IP 0=Chassis-IP
device (config-syslog-server-1.1.1.1/mgmt-vrf)#
```

To remove a configured syslog server:

```
device# configure terminal
device(config)# no logging syslog-server 192.168.163.233
```

logging syslog-server-host

Configures a switch to forward system messages to a specified syslog server using its host name.

Syntax

logging syslog-server-host *host-name* [**use-vrf** *vrf-name*]

no logging syslog-server-host *host-name* [**use-vrf** *vrf-name*]

Parameters

host-name

Specifies the hostname of the syslog server. This hostname must be resolved by the configured DNS server.

use-vrf *vrf-name*

Specifies a VRF through which to communicate with the server. See the Usage Guidelines.

Modes

Global configuration mode

Usage Guidelines

Use this command to configure a switch to forward all error log entries to a specified server using the server's host name. You can configure only one syslog server using hostname, this includes all VRFs.

The **crypto import syslogca** command is required for a secure syslog to be fully functional.

After specifying the **host-name** and **vrf-name**, the **secure** sub-command can be used to specify the secure default port (6514) or specify a secure non-default syslog server port. These sub-commands are only available after specifying the **ip_address** and **vrf-name** parameters.

Use the **no logging syslog-server-host** command with the optional use-vrf keyword to remove the specified hostname and VRF.

By default, all management services are enabled on the management VRF ("mgmt-vrf") and the default VRF ("default-vrf").

Examples

To configure a server (using its hostname) to which system messages are sent on a user-specified VRF:

```
device# configure terminal
device(config)# logging syslog-server-host test.server.com use-vrf myvrf
device(config-syslog-server-192.168.163.233/myvrf)#
```

To configure a secure server with a non-default port number:

```
device(config)# logging syslog-server-host test.server.com use-vrf mgmt-vrf
device(config-syslog-server-192.168.163.233/mgmt-vrf)# secure port 6502
device(config-syslog-server-192.168.163.233/mgmt-vrf)#
```

To remove a configured syslog server:

```
device# configure terminal
device(config)# no logging syslog-server-host test.server.com use-vrf myvrf
```

logging utility

Configures a switch to forward system messages to the configured syslog server(s) using RELP (Reliable Event Logging Protocol).

Syntax

logging utility enable relp

no logging utility enable

Parameters

relp

Specifies that the logging entries must be forwarded to the configured logging servers using RELP.

Modes

Global configuration mode

Usage Guidelines

Use this command to configure forwarding all system logs entries to the configured logging servers using *Reliable Event Logging Protocol* (RELP).

You can configure up to four SYSLOG servers; this includes all VRFs. You must execute the command for each server. The **crypto import syslogca** command is required for secure SYSLOG to be fully functional. After specifying the **ip_address** and **vrf-name** parameters, the **secure** sub-command can be used to specify the secure default port (6514) or to specify a secure non-default SYSLOG server port.

These sub-commands are only available after specifying the **ip_address** and **vrf-name** parameters. Use the **no logging syslog-server** command with the optional **use-vrf** keyword to remove the specified IP address and VRF.

By default, all management services are enabled on the management VRF (*mgmt-vrf*) and the default VRF (*default-vrf*).

Usage Guidelines

When enabling logging over RELP, keep the following in mind.

- When *rsyslog* over is RELP is configured as secured with TLS, the certificates that are used for securing SYSLOG are used by *rsyslog* over RELP.
- After turning on logging over RELP, and when you use the login credentials of the *SYSLOG* server, then the same credentials are used for logging over RELP.
- RELP mode does not support *syslog-server host* configuration. This configuration is automatically blocked in the RELP mode. An error message is displayed.

Examples

To enable forwarding all system logs entries to the configured logging servers using *Reliable Event Logging Protocol* (RELP).

```
SLX # config terminal
SLX (config)# logging utility enable relp
```

To disable forwarding all system logs entries to the configured logging servers using *Reliable Event Logging Protocol* (RELP).

```
SLX # config terminal
SLX (config)# no logging utility enable
```

logical-interface

Configures a logical interface on a physical port or a port-channel (LAG) on an edge port, entering LIF configuration mode, and optionally binds the interface to a bridge domain (BD).

Syntax

logical-interface { **ethernet** *slot/port.service_instance* | **port-channel** *num.service_instance* }

no logical-interface { **ethernet** *slot/port.service_instance* | **port-channel** *num.service_instance* }

Command Default

See the Usage Guidelines.

Parameters

ethernet *slot/port*

Specifies an Ethernet interface.

port-channel *num*

Specifies a port-channel interface.

service_instance

Specifies a service instance ID. Range is from 1 through 12288.

Modes

Interface subtype configuration mode

Bridge domain configuration mode

Usage Guidelines

The following are some common rules to consider in configuring logical interfaces:

- This command is applicable to an edge port only.
- This command by itself does not create the LIF as it requires more classifications as to what VLAN(s) should be specified and whether the classifying VLAN is untagged or tagged.
- By default, when the LIF is created it is enabled. it is also "tagged" unless it is explicitly configured with the "untagged" option.
- The user must specify a service instance ID. If the service instance ID has already been configured, this command allows the user to specify the VLAN classification for this LIF. Allowed LIF service instance ranges are from 1 through 12288 (12K LIFs are

allowed per interface type). Currently, up to 100K LIFs are supported in the system, with 12K for physical port or LAG combined and 8K for PW based.

- A LIF service instance ID has no correlation to the VLAN ID of the LIF.
- Each physical/LAG-based LIF must have an associated VLAN configured or else it will not be usable when the user attempts to add it to a service. Such a configuration request to add the LIF to a service will be rejected.
- Once the LIF is associated with a Layer 2 service, its VLAN value cannot be changed or deleted unless it is first removed from the associated service. In case the LIF is not yet associated to a service, the user is free to remove the VLAN configuration or change the VLAN assignment.
- The "untagged" configuration can only be allowed for one LIF under the same physical port or LAG. If one LIF is already configured as untagged, all subsequent attempts on the same physical port or LAG will be rejected.
- Once the "untagged" option is selected, it will only have one VLAN as the next classification option. There is no dual-tag support for the untagged case.
- In order to configure an untagged LIF, the main interface must be set as "switchport mode trunk-no-default-native". If it is only set to regular trunk mode, the native VLAN is already associated with a regular Layer 2 VLAN LIF and no explicit untagged LIF can be configured on that interface.
- Once the LIF is associated with a service (Layer 2) such as bridge domain, its "untagged/tagged" configuration cannot be changed. The service instance or its current VLAN classification must be deleted by user first and then added back with the proper "untagged/tagged" option.
- VLANs 4091 through 4095 are reserved VLANs and these should not be used as the VLAN ID for either the inner or outer VLAN of the LIF.
- The VLAN specified under the LIF ensures that such a VLAN is not already configured under the **switchport** command for a regular Layer 2 allowed VLAN.

The **no** version of the command removes the LIF from the BD configuration. This can be applied any time if the LIF is not yet associated with (bound to) a service. If it is already associated with a service, the LIF is also implicitly removed from the BD configuration.

Examples

The following example sets "trunk-no-default-native" mode on an Ethernet interface, so that an untagged LIF can be configured on service instance 120.

```
device(config)# interface ethernet 2/6
device(conf-if-eth-2/6)# switchport mode trunk-no-default-native
device(conf-if-eth-2/6)# logical-interface ethernet 2/6.120
device(conf-if-eth-lif-2/6.120)#
```

The following examples illustrate how up to command options can be configured in a single line.

```
device(conf-if-eth-2/6)# logical-interface ethernet 2/6.120 name myLIF120
device(conf-if-eth-lif-2/6.120)#
```

```
device(conf-if-eth-2/6)# logical-interface ethernet 2/6.120 vlan 120
device(conf-if-eth-lif-2/6.120)#
```

The following example sets "trunk-no-default-native" mode on a port-channel (LAG) interface, so that an untagged LIF can be configured on service instance 3.

```
device(config)# int port-channel 10
device(config-port-channel-10)# switchport mode trunk-no-default-native
device(config-port-channel-10)# logical-interface port-channel 10.3
device(config-if-po-lif-10.3)# untagged vlan 3
```

The following example shows how to create a logical Ethernet interface service instance (1/5.10) and bind it to bridge domain 4 by means of the **bridge-domain** command.

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# logical-interface ethernet 1/5.10
device(conf-if-eth-lif-1/5.10)# vlan 50
device(conf-if-eth-lif-1/5.10)# exit

device(config)# bridge-domain 4
device(config-bridge-domain-4)# logical-interface ethernet 1/5.10
```

The following example shows how to bind a logical port-channel interface service instance (2.200) to bridge domain 4 by means of the **bridge-domain** command.

```
device# configure terminal
device(config)# bridge-domain 4
device(config-bridge-domain-4)# logical-interface port-channel 2.200
```

The following example shows the error message that displays when an attempt is made to bind a logical interface that was not previously created to a bridge domain.

```
device# configure terminal
device(config)# bridge-domain 4
device(config-bridge-domain-4)# logical-interface ethernet 1/3.100
Error: Logical Interface not yet created
```

The following example shows the error message that displays when an attempt is made to bind a logical interface that is previously bound to another bridge domain.

```
device>enable
device# configure terminal
device(config)# bridge-domain 4
device(config-bridge-domain-4)# logical-interface ethernet 1/3.100
 Error: LIF already Binded
```

loopback phy

Implements transparent loopback on a physical interface.

Syntax

loopback phy

no loopback phy

Command Default

Transparent loopback is not implemented.

Modes

Ethernet interface configuration mode

Usage Guidelines

Transparent loopback enables a transmission-only link from a network device into an NPB device.

Transparent loopback is often required on a non-NPB (Network Packet Broker) device that forwards traffic to an NPB. It enables egress traffic to the NPB with no ingress cable.

To disable transparent loopback on an interface, use the **no** form of this command.

Examples

The following example implements transparent loopback on a physical interface.

```
device# configure terminal
device(config)# interface ethernet 1/2
device(conf-if-eth-1/2)# loopback phy
```

The following example disables transparent loopback on a physical interface.

```
device# configure terminal
device(config)# interface ethernet 1/2
device(conf-if-eth-1/2)# no loopback phy
```

loop-detection

Enables the loop detection (LD) feature at the interface level, VLAN, or bridge domain (BD) level, and enters Protocol Loop Detection configuration mode.

Syntax

loop-detection

no loop-detection

Command Default

This feature is disabled.

Modes

Interface subtype configuration mode (Ethernet or port-channel)

VLAN configuration mode

Bridge domain configuration mode

Usage Guidelines

When configured at the interface level, this command applies to LD strict mode.

When configured at the VLAN level, this command is applied to all ports in the VLAN.

When configured at the bridge domain (BD) level this command is applied to all the attachment circuit (AC) logical interfaces (LIFs) and VXLAN tunnels under the BD.

Use the no form of this command to disable loop detection at the interface, VLAN, or BD level.

Examples

The following example enables loop detection on an Ethernet interface and enters Protocol Loop Detection configuration mode:

```
device# configure terminal
device(config)# interface ethernet 2/6
device(conf-if-eth-2/6)# loop-detection
device(config-loop-detect)#
```

The following example disables loop detection on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 2/6
device(conf-if-eth-2/6)# no loop-detection
```

The following example enables loop detection on a port-channel interface and enters Protocol Loop Detection configuration mode.

```
device# configure terminal
device(config)# interface port-channel 20
device(config-port-channel-20)# loop-detection
device(config-loop-detect)#
```

The following example enables loop detection on a VLAN and enters Protocol Loop Detection configuration mode.

```
device# configure terminal
device(config)# vlan 5
device(config-vlan-5)# loop-detection
device(config-loop-detect)#
```

The following example enables loop detection on a BD and enters Protocol Loop Detection configuration mode.

```
device# configure terminal
device(config)# bridge-domain 8
device(config-bridge-domain-8)# loop-detection
device(config-loop-detect)#
```

loop-detection shutdown-disable

Disables the shutting down of an interface (Ethernet or port-channel), a VLAN VXLAN tunnel, or a bridge domain (BD) VXLAN tunnel as a result of the loop detection (LD) protocol.

Syntax

loop-detection shutdown-disable

no loop-detection shutdown-disable

Command Default

This feature is disabled.

Modes

Interface subtype configuration mode (Ethernet or port-channel)

VLAN configuration mode

Bridge domain configuration mode

Usage Guidelines

Use the no form of this command. to revert to default behavior. (LD protocol shuts down the interface.)

Examples

The following example disables the shutdown of an Ethernet interface as a result of LD protocol.

```
device# configure terminal
device(config)# interface ethernet 2/6
device(conf-if-eth-2/6)# loop-detection shutdown-disable
```

The following example reverts to default behavior.

```
device# configure terminal
device(config)# interface ethernet 2/6
device(conf-if-eth-2/6)# no loop-detection shutdown-disable
```

The following example disables the shutdown of a VLAN VXLAN tunnel.

```
device# configure terminal
device(config)# vlan 20
device(config-vlan-20)# loop-detection shutdown-disable
```

The following example disables the shutdown of a BD VXLAN tunnel.

```
device# configure terminal
device(config)# bridge-domain 8
device(config-bridge-domain-8)# loop-detection shutdown-disable
```

loop-detection vlan

Associates a VLAN at the interface level to support the loop detection (LD) protocol.

Syntax

loop-detection vlan *vlan-id*

no loop-detection vlan

Command Default

This feature is disabled.

Parameters

vlan-id

Specifies a created VLAN. Range is from 1 through 4090.

Modes

Interface subtype configuration mode (Ethernet or port-channel)

Usage Guidelines

The VLAN must already be created.

This command applies to LD loose mode.

The no form of this command deletes LD support for all previously configured VLANs, deleting all LD configurations at the interface level.

Examples

To associate a VLAN to an Ethernet interface for LD support:

```
device# configure terminal
device(config)# interface ethernet 2/6
device(conf-if-eth-2/6)# loop-detection vlan 20
```

To disassociate all previously configured VLANs from an Ethernet interface for LD support and delete all LD configurations at the Ethernet interface level:

```
device# configure terminal
device(config)# interface ethernet 2/6
device(conf-if-eth-2/6)# no loop-detection vlan 20
```

lsp

Accesses LSP subconfiguration mode to configure the LSP tunnel.

Syntax

lsp *name*

no lsp *name*

Parameters

name

Specifies the name of the LSP tunnel.

Modes

MPLS configuration mode

Usage Guidelines

Use the **no** form of this command to remove the LSP from the MPLS configuration.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures LSP to2 and accesses LSP subconfiguration mode.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# lsp to2
device(config-router-mpls-lsp-to2)#
```

lsp (Telemetry)

Indicates the MPLS LSP to be used for the mpls-traffic-lsp profile.

Syntax

lsp { *lsp-name* }

no lsp { *lsp-name* }

Parameters

lsp-name

Specifies the name of the target LSP for the profile.

Modes

Telemetry profile configuration mode

Usage Guidelines

The *lsp-name* variable must be unique among all regular LSPs and bypass LSPs.

The **no** form of the command deletes the LSP from the profile.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example selects the *xm2lsp* LSP as the LSP for the profile.

```
device(config)# telemetry profile mpls-traffic-lsp default_mpls_traffic_lsp_statistics
device(config-telemetry-profile)# lsp xm2lsp
```

lsp-gen-interval

Sets the minimum number of seconds the device waits between sending updated Link State PDUs (LSPs) to its Intermediate System-to-Intermediate System (IS-IS) neighbors.

Syntax

lsp-gen-interval *interval*

no lsp-gen-interval *interval*

Command Default

The default interval is 10 seconds.

Parameters

secs

Specifies the interval in seconds. Valid values range from 0 through 120 seconds. The default is 10 seconds.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command removes the configured interval.

Examples

The following example changes the LSP generation interval to 45 seconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# lsp-gen-interval 45
```

lsp-interval

Sets the rate of transmission, in milliseconds, of the Link State PDUs (LSPs).

Syntax

lsp-interval *interval*

no lsp-interval *interval*

Command Default

The default interval is 33 milliseconds.

Parameters

secs

Specifies the interval in milliseconds. Valid values range from 1 through 4294967295 milliseconds. The default is 33 milliseconds.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command removes the configured interval.

Examples

The following example changes the LSP interval to 45 milliseconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# lsp-interval 45
```

lsp-refresh-interval

Sets the maximum number of seconds a device waits between sending updated Link State PDUs (LSPs) to its Intermediate System-to-Intermediate System (IS-IS) neighbors.

Syntax

lsp-refresh-interval *interval*

no lsp-refresh-interval *interval*

Command Default

The default interval is 900 seconds (15 minutes).

Parameters

secs

Specifies the interval in seconds. Valid values range from 1 through 65535 seconds. The default is 900 seconds.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command removes the configured interval.

Examples

The following example changes the LSP refresh interval to 20000 seconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# lsp-refresh-interval 20000
```

lsr-id

Configures an IP address to be used as the LSR ID for the LDP identifier.

Syntax

lsr-id *ip_addr*

no lsr-id *ip_addr*

Command Default

The LSR-ID is the first available loopback interface address.

Parameters

ip_addr

Specifies the IP address to assign to the LSR identifier.

Modes

MPLS LDP configuration mode

Usage Guidelines

You can configure only an IPv4 address.

Use the **no** form of the command to reset the default behavior. When you enter the **no** form of the command and LDP protocol is in the enabled state, the device uses the same LSR-ID until the LDP protocol is disabled; the IP address selected as LSR-ID for the LDP protocol is still valid and is the operationally UP IP address on an enabled loopback interface.

When you enter the **no** form of the command and LDP protocol is in the disabled state (this happens when the loopback interface on which IP address is configured is in the disabled state), the device falls back to default behavior which tries to enable LDP protocol when it finds a valid IP address on any one of the enabled loopback interfaces.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures an IP address for the LSR identifier.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# lsr-id 10.22.22.22
```

lvtep broadcast-local-bias

Enables Local Bias for LVTEP BUM traffic.

Syntax

lvtep broadcast-local-bias

no lvtep broadcast-local-bias

Command Default

By default, Local Bias is disabled for LVTEP for Broadcast,Unknown Unicast, and Multicast (BUM) traffic.

Parameters

broadcast-local-bias

Enables broadcasting Local Bias for LVTEP BUM traffic.

Modes

Global Configuration

Usage Guidelines

This command cannot be used when cluster is configured. To change the mode from Designated Forwarder to Local Bias, all cluster configuration must be removed.

This command cannot be used when the node is configured for EVPN Multi-homing. You cannot use EVPN Multi-homing if this mode is configured.

The *no* format of this command removes Local Bias for LVTEP BUM traffic. The cluster configuration must be removed before executing this command.

Examples

The following example enables Local Bias for LVTEP BUM traffic.

```
SLX(config)# lvtep broadcast-local-bias
SLX(config)# cluster test
SLX(config-cluster-test)# exit
SLX(config)# do show running-config lvtep broadcast-local-bias
lvtep broadcast-local-bias

SLX(config)# do show running-config cluster
cluster test

SLX(config)# do show running-config
...
lvtep broadcast-local-bias
cluster test
...
```

The following example shows the error message that is displayed when trying to configure Local Bias when a cluster is already configured on the node.

```
SLX(config)# cluster test
SLX(config-cluster-test)# ex
SLX(config)# lvtep broadcast-local-bias
%%Error: Local Bias cannot be configured for LVTEP broadcast as MCT cluster is configured
on the system.
```

ma-name

Creates a maintenance association (MA) within a specified domain. The command changes the maintenance domain mode to the specified maintenance association mode.

Syntax

ma-name *ma-name* [**id** *ma-id*] [**vlan-id** *vlan-id*] [**bridge-domain** *bridge-domain*] { **priority** *priority* }

no ma-name *ma-name*

Command Default

There are no MA configured.

Parameters

ma-name

Specifies the maintenance association name. The name attribute is case-sensitive.

ma-id

Specifies the short maid that is transmitted in the CCM PDU. This ID is unique. The range is 1 - 4090.

vlan-id

Specifies a unique VLAN identifier of the maintenance association in the range 1-4090. To create a MA, a vlan id must be set.

bridge-domain

Specifies a unique L2VPN domain of the maintenance association. This option supports only Virtual Private LAN Services (VPLS) in this release. VLL is not currently supported for CFM.

priority

Specifies the priority of the CCM messages sent by MEPs, in the range 0-7.

Modes

CFM protocol configuration mode

Usage Guidelines

The no form of the command removes the maintenance association.

Examples

This example demonstrates associating the MA "ma1" to VLAN 30.

```
device# configure terminal
device(config)# protocol cfm
device(config-cfm)# domain name md1 level 4
device(config-cfm-md-md1)# ma-name ma1 id 1 vlan-id 30 priority 4
device(config-cfm-md-ma-ma1)#
```

mac access-group

Applies rules specified in a MAC access control list (ACL) to traffic entering or exiting an interface.

Syntax

mac access-group *ACLname* { **in** | **out** }

no mac access-group *ACLname* { **in** | **out** }

Parameters

ACLname

Specifies the name of the standard or extended MAC access list.

in

Applies the ACL to incoming switched and routed traffic.

out

Applies the ACL to outgoing routed and (is supported on the Extreme 8720, Extreme 8520, SLX 9250, and SLX 9150 devices only.) also to switched traffic.

Modes

Interface-subtype configuration mode

Usage Guidelines

You can apply a maximum of five ACLs to a user interface, as follows:

- One ingress MAC ACL—if the interface is in switchport mode
- One egress MAC ACL—if the interface is in switchport mode
- One ingress IPv4 ACL
- One egress IPv4 ACL
- One ingress IPv6 ACL

On the Extreme 8720, Extreme 8520, SLX 9250, and SLX 9150 devices only, you can apply MAC ACLs to port-channels (LAGs) only ingress.

You can apply an ACL to multiple interfaces. And you can apply an ACL twice—ingress and egress—to a given user interface.

To remove an ACL from an interface, enter the **no** form of this command.

Examples

The following example applies a MAC ACL to filter inbound packets only, on a specified Ethernet interface.

```
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# mac access-group macacl2 in
```

The following example removes a MAC ACL from a specified port-channel interface.

```
device(config)# interface port-channel 62
device(config-Port-channel-62)# no mac access-group macacl2 in
```

mac access-list extended

Creates a MAC extended access control list (ACL).

Syntax

mac access-list extended *ACL-name*

no mac access-list extended *ACL-name*

Parameters

ACL-name

Specifies an ACL name unique among all ACLs (Layer 2 and Layer 3). The name can be up to 63 characters in length, and must begin with an alphanumeric character. No special characters are allowed, except for the underscore (_) and hyphen (-).

Modes

Global configuration mode

Usage Guidelines

If the ACL is already created, this command puts the device in MAC extended ACL configuration mode.

An extended ACL contains rules that permit or deny traffic according to source and destination addresses, as well as other parameters. Extended ACLs allow you to filter traffic based on the following:

- Source MAC address
- Destination MAC address
- EtherType

You can apply MAC extended ACLs to VLANs and to Layer 2 interfaces.

To enable ARP Guard, you also use a MAC extended ACL.

The **no** form of the command removes a MAC extended ACL from an interface.

Examples

The following example creates a MAC extended ACL named mac1.

```
device(config)# mac access-list extended mac1
```

The following example deletes a MAC extended ACL named mac1.

```
device(conf-macl-ext)# no mac access-list extended mac1
```

mac access-list standard

Creates a standard MAC access control list (ACL). Standard ACLs contain rules that permit or deny traffic based on source addresses that you specify.

Syntax

mac access-list standard *ACLname*

no mac access-list standard *ACLname*

Parameters

ACLname

Specifies an ACL name unique among all ACLs (Layer 2 and Layer 3). The name can be up to 63 characters in length, and must begin with an alphanumeric character. No special characters are allowed, except for the underscore and hyphen.

Modes

Global configuration mode

Usage Guidelines

Use this command to create a standard MAC access list. If ACL is already created, this command puts the device in the standard MAC access-list configuration mode.

To remove a MAC ACL from an interface, enter the **no** form of this command.

Examples

The following command creates a MAC standard ACL named mac1.

```
device(config)# mac access-list standard mac1
device(conf-macl-std)#
```

The following command deletes a MAC standard ACL named mac1.

```
device(conf-macl-std)# no mac access-list standard mac1
```

mac-address withdrawal

In a VPLS context on a bridge domain (BD), removes MAC addresses that have been dynamically learned, thus providing faster convergence.

Syntax

mac-address withdrawal

no mac-address withdrawal

Command Default

MAC address withdrawal is disabled.

Modes

Bridge-domain configuration mode

Usage Guidelines

A MAC address withdrawal message is sent with a MAC list Type Length Value (TLV). 200 MAC addresses are bulked and sent in one MAC TLV message.

Note
The MAC withdrawal support is only for explicit MAC addresses in a MAC withdrawal TLV. An empty MAC list, as well as the sending of a MAC withdrawal TLV to a specific subset of peers, is not supported.

The maximum number of MAC addresses supported is 5000 in a 5-second interval. The remaining MAC addresses in the attachment circuit (AC) logical interface (LIF) are not sent. After the 5-second interval, another LIF "down" event triggers a MAC withdrawal message for a new-5 second interval.

MAC withdrawal is supported for both VPLS and MCT-VPLS. MPLS signals the MAC withdraw TLV to all the peers.

Use the **no** form of this command to disable MAC address withdrawal.

Examples

The following example enables MAC address withdrawal on a BD.

```
device# configure terminal
device(config)# bridge-domain 10
device(config-bridge-domain-10)# mac-address withdrawal
```

The following example illustrates output of the **show bridge-domain** command confirming that withdrawal is enabled.

```
device# show bridge-domain
Bridge-domain 1
-------------------------------
Bridge-domain Type: MP , VC-ID: 0
Number of configured end-points: 0 , Number of Active end-points: 0
VE if-indx: 0, Local switching: TRUE, bpdu-drop-enable: TRUE
MAC Withdrawal: Enabled
PW-profile: default, mac-limit: 0
Total VPLS peers: 0 (0 Operational):
```

mac-address-table aging-time

Configures the aging time for dynamic MAC address entries in the MAC address table.

Syntax

mac-address-table aging-time *seconds*

no mac-address-table aging-time

Command Default

Default aging time is 1800 seconds.

Parameters

aging-time *seconds*

To disable MAC address aging, specify `0`. To enable MAC address aging, specify a value from 60 through 86400.

Modes

Global configuration mode

Usage Guidelines

MAC address aging configuration per VLAN is not supported.

The **no** form of the command restores the default value.

Examples

The following example configures the MAC aging period as 400 seconds.

```
device# configure terminal
device(config)#  mac-address-table aging-time 400
```

mac-address-table mac-move

Configures the MAC movement detection parameters

Syntax

mac-address-table mac-move detect

mac-address-table mac-move action{ **shutdown** | **raslog** }

mac-address-table mac-move limit

mac-address-table mac-move auto-recovery enable{ **time** } [**minutes**]

Command Default

MAC movement detection is disabled by default

Parameters

action

Defines the action taken when the MAC movement exceeds the threshold. RASLOG is the default.

limit

Sets the threshold for MAC movement action. Default is 20. Range is 3 through 500.

auto-recovery

Enables auto-recovery on the port. Default is disabled.
time

Sets the recovery time in minutes. Default is 5 minutes. Range is 3 through 30 minutes.

Modes

Global configuration mode

Usage Guidelines

The no form of the command restores the default value.

Examples

The following example enables MAC movement detection

```
device# config
device (config)# mac-address-table mac-move detect
```

The following example configures auto-recovery and sets the recovery time for 3 minutes.

```
device# config
device (config)# mac-address-table mac-move auto-recovery enable
device (config)#  mac-address-table mac-move auto-recovery time 3
device (config)#
```

mac-address-table static

Adds static addresses to the MAC address table.

Syntax

mac-address-table static *mac-addr* **forward ethernet** *slot/port* **vlan** *vlan-id*

no mac-address-table static *mac-addr* **forward ethernet** *slot/port* **vlan** *vlan-id*

mac-address-table static *mac-addr* **forward logical-interface ethernet** *logical-interface*

no mac-address-table static *mac-addr* **forward logical-interface ethernet** *logical-interface*

mac-address-table static *mac-addr* **forward port-channel** *port-channel-number* **vlan**

no mac-address-table static *mac-addr* **forward port-channel** *port-channel-number* **vlan**

Command Default

Aging time is 1800 seconds.

The MAC-move limit is 20 moves.

Parameters

static *mac-addr* **forward**

Specifies the Media Access Control (MAC) address (unicast or multicast) to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface.

ethernet

Specifies an Ethernet interface.

slot

Specifies a valid slot number. The slot must be 0 for devices that do not support line cards.

port

Specifies a valid port number.

logical-interface *logical-interface*

Specifies a logical interface. Logical interfaces are the attachment circuit end-points bound to a bridge domain.

port-channel *number*

Specifies the port-channel number. Valid values range from 1 through 63.

vlan *vlan-id*

Specifies an active VLAN. Values range from 1 through 4090.

Modes

Global configuration mode

Usage Guidelines

The **vlan** keyword is mandatory because the switch only supports independent VLAN learning (IVL).

To delete a static MAC address for forwarding to a physical interface, use the **no mac-address-table static** *mac-addr* **forward ethernet** *slot/port* **vlan** *vlan-id* option.

To delete a static MAC address for forwarding to a logical interface, use the **no mac-address-table static** *mac-addr* **forward logical-interface ethernet** *logical-interface* **vlan** *vlan-id* option.

To delete a static MAC address for forwarding to a port-channel interface, use the **no mac-address-table static** *mac-addr* **forward port-channel** *port-channel-number* **vlan** option.

Examples

The following example adds a static address to the MAC address table, with forwarding to a physical interface.

```
device# configure terminal
device(config)# mac-address-table static 0011.2222.3333 forward ethernet 0/1 vlan 100
```

The following example adds a static address to the MAC address table, with forwarding to a logical interface.

```
device# configure terminal
device(config)#mac-address-table static 0000.1111.2222 forward logical-interface ethernet
0/43.100
```

The following example deletes a static MAC address forwarding on a physical interface.

```
device# configure terminal
device(config)# no mac-address-table static aaaa.bbbb.cccc forward ethernet 0/1 vlan 10
```

maid-format

Sets the Maintenance Association Identifier (MAID) format for a particular maintenance association (MA).

Syntax

maid format [**long** | **default**]

Command Default

The default maid format is short.

Parameters

long

Specifies maid format as long.

default

Specifies maid format as default.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command reverts back the maid format to short.

You cannot change the MAID format after a MEP is configured under an MA. You must first delete the MEP and then change the MAID format.

Examples

The following example sets the MAID format to long.

```
device# configure terminal
device(config)# protocol cfm
device(config-cfm)# domain name md1 level 4
device(config-cfm-md-md1)# ma-name ma1 id 30 vlan-id 30 priority 7
device(config-cfm-md-md1)# maid-format long
```

maintenance-mode (Interface)

Navigates into the interface's Maintenance sub-mode.

Syntax

maintenance-mode

[no] maintenance-mode

Command Default

There are no defaults for this command.

Modes

Interface Configuration context. Navigates into the maintenance sub-mode for the selected interface.

Usage Guidelines

This mode is a sub-mode of the interface's configuration mode. Use this command to navigate into the interface's maintenance sub-mode.

This command cannot be run on interfaces that are configured as ICL, CCEP, or cluster-tracked.

When the device's firmware is downgraded to a version that does not support this maintenance sub-mode, this configuration setting is dropped.

Examples

This example navigates into an interface's maintenance mode.

```
SLX (config)# interface Ethernet 0/1
SLX(conf-if-eth-0/1)# maintenance-mode
SLX(config-maintenance-mode)#
```

management-heartbeat manager (management-heartbeat)

The *heartbeat-manager* sub mode, under the *Global Configuration* mode, enables configuration of the various parameters associated with SLX devices listening for heartbeat message from EFA. Use this mode to enable heartbeat monitoring, to configure threshold time for listening to heartbeat messages, to configure actions to be performed on expiration of the configured threshold time.

Syntax

management-heartbeat manager

no management-heartbeat manager

Command Default

Heartbeat monitoring must be enabled explicitly using the `enable` command from within this mode.

When this command is executed, an entry for this mode is created in the *running-config*.

```
SLX(config-management-heartbeat-manage)# do show running-config management-heartbeat
manager
management-heartbeat manager
 threshold-timer 5
 action maintenance-mode-enable
!
SLX(config-management-heartbeat-manage)#
```

The `no` form of this command removes the `management-heartbeat manager` configuration from the *running-config*.

```
SLX(config-management-heartbeat-manage)# do show running-config management-heartbeat
manager
management-heartbeat manager
 threshold-timer 5
 action maintenance-mode-enable
!
SLX(config-management-heartbeat-manage)# exit
SLX(config)#
SLX(config)# no management-heartbeat manager
SLX(config)#
SLX(config)# do show running-config management-heartbeat manager
% No entries found.
SLX(config)#
```

Examples

The following example changes the context to *management-heartbeat-manage* mode and lists all the commands within this context.

```
SLX# configure terminal
Entering configuration mode terminal
SLX(config)# management-heartbeat manager
Possible completions:
```

```
SLX(config)# management-heartbeat manager
SLX(config-management-heartbeat-manage)#
SLX(config-management-heartbeat-manage)# ?
Possible completions:
  action            Action taken by switch on expiration of threshold time
  describe          Display transparent command information
  do                Run an operational-mode command
  enable            Enable manageability heartbeat in admin up state
  exit              Exit from current mode
  help              Provide help information
  no                Negate a command or set its defaults
  pwd               Display current mode path
  threshold-timer   Threshold timer for heartbeat miss
  top               Exit to top level and optionally run command
SLX(config-management-heartbeat-manage)#
```

management-security

The *management-security* sub mode, under the *Global Configuration* mode, enables configuring the lowest TLS version supported by the SLX software. SLX uses OpenSSL to provide transport layer security and the current version of OpenSSL supports TLS v 1.1 to TLS v 1.2. Since the SLX box can be considered as both a client as well as a server, you can apply different supported TLS versions for each of these types. The **ssl-profile** command within this mode allows you to configure these values.

Syntax

management-security

Modes

Configuration Terminal mode

Examples

The following example shows how to navigate into the **management-security** mode and view the available commands under this mode.

```
SLX # configure terminal
Entering configuration mode terminal

SLX (config)# management-security ?
Possible completions:
  <cr>

SLX (config)# management-security
SLX (mgmt-security)#
SLX (mgmt-security)# ?
```

manual-switch vlan

Blocks a specified link manually for an Ethernet Ring Protection (ERP) instance.

Syntax

manual-switch vlan *vlan_id* [**ethernet** *slot/port* | **port-channel** *number*]

no manual-switch vlan *vlan_id* [**ethernet** *slot/port* | **port-channel** *number*]

Command Default

This feature is not configured by default.

Parameters

vlan_id

Specifies a VLAN.

ethernet *slot/port*

Specifies an Ethernet interface.

port-channel *number*

Specifies a port-channel.

Modes

ERP configuration mode

Usage Guidelines

Manual Switch (MS) is an operator-initiated process that manually blocks a specified interface in a ring. It can be configured only in an error-free topology. There can be only one MS configuration in a ring.

Use the **no** form of this command to remove the configuration.

Examples

The following example configures MS for a specified interface.

```
device# configure terminal
device(config)# erp 1
device(config-erp-1)# manual-switch vlan 5 ethernet 0/1
```

map bridge-domain (overlay gateway)

Maps a bridge domain (BD) to a Virtual Network Identifier (VNI) for a VXLAN overlay gateway.

Syntax

map bridge-domain *bridge_domain_id* **vni** *vni*

no map bridge-domain *bridge_domain_id* **vni** *vni*

Parameters

bridge_domain_id

Specifies a bridge domain.

vni *vni*

Specifies a VNI. Enter an integer from 1 through 16777215.

Modes

Overlay gateway configuration mode

Usage Guidelines

Use the **no** form of this command to remove the mapping.

Examples

The following example maps a bridge domain to a VNI.

```
device# configure terminal
device(config)# overlay-gateway gateway1
device(config-overlay-gw-gateway1)# map bridge-domain 1 vni 999
```

map cos to cos

Changes an incoming CoS value to another value before sending the packet out.

Syntax

map cos *in-cos-value* **to cos** *out-cos-value*

no map cos *in-cos-value*

Parameters

cos *in-cos-value*

The incoming CoS value that will be mapped to another value. The valid values are 0-7.

to cos *out-cos-value*

Indicates that the incoming CoS will be mapped to another value. The CoS value to be applied to the outgoing packet. The valid values are 0-7.

Modes

QoS to CoS Mutation Map mode.

Usage Guidelines

None

Supported In

SLX 9740 and Extreme 8820

Examples

This example configures the mapping of 3 incoming CoS values to different ones.

```
 SLX# configure terminal
SLX (config)# qos map cos-mutation test-map
SLX (cos-mutation-test-cos-mut-map-1)# map cos 1 to cos 3
SLX (cos-mutation-test-cos-mut-map-1)# map cos 2 to cos 1
SLX (cos-mutation-test-cos-mut-map-1)# map cos 3 to cos 0
SLX (cos-mutation-test-cos-mut-map-1)# exit
SLX (config)#
```

This example disables a configured CoS mutation mapping.

```
SLX# configure terminal
SLX (config)# qos map cos-mutation test-cos-mut-map-1
SLX (cos-mutation-test-cos-mut-map-1)# no map cos 3
SLX (cos-mutation-test-cos-mut-map-1)# exit
SLX (config)#
```

Related Commands

- qos map cos-mutation on page 1437
- qos cos-mutation on page 1424
- show qos maps cos-mutation on page 2259

map dscp

Maps an ingress DSCP value to an outbound CoS, DSCP, or traffic-class value for a QoS DSCP-to-CoS, DSCP-mutation, or DSCP-to-traffic class map.

Syntax

map dscp *dscp-value* **to** { **cos** *cos-value* } | { **dscp** *dscp-out* } | { **traffic-class** *tc-value* }

no map dscp *dscp-value*

Command Default

The default values for DSCP to CoS, DSCP mutation, or DSCP to traffic class mapping.

Parameters

dscp-value

Specifies the ingress DSCP value or range. Enter an integer from 0 to 63.

cos *cos-value*

Specifies the outbound CoS value. Enter an integer from 0 to 7.

dscp *dscp-out*

Specifies the outbound DSCP value or range. Enter an integer from 0 to 63.

traffic-class *tc-value*

Specifies the outbound Traffic Class value. Enter an integer from 0 to 7.

Modes

DSCP CoS configuration mode

DSCP mutation configuration mode

DSCP traffic-class configuration mode

Usage Guidelines

Use the **no** form of the command to reset the default mapping values.

Examples

In DSCP COS configuration mode, the following example maps an ingress DSCP value to an egress CoS value.

```
device# configure terminal
device(config)# qos map dscp-cos test
device(dscp-cos-test)# map dscp 43 to cos 4
```

In DSCP mutation configuration mode, the following example maps the ingress DSCP values to an egress DSCP value.

```
device# configure terminal
device(config)# qos map dscp-mutation test
device(dscp-mutation-test)# map dscp 1,3,5,7 to dscp 40
```

In DSCP traffic configuration mode, the following example maps the ingress DSCP values to a traffic class.

```
device# configure terminal
device(config)# qos map dscp-traffic-class test
device(dscp-traffic-class-test)# map dscp 1,3,5,7 to traffic-class 1
```

map vlan

In a VXLAN overlay gateway configuration that uses Layer 2 extension, associates VLANs with VXLAN Network Identifiers (VNIs).

Syntax

map vlan [*vlan_id*] **vni** [*vni*] [**auto**]

no map vlan *vlan_id*

no map vlan vni

Parameters

vlan_id

A single VLAN ID or range of VLAN IDs. The range is from 1 through 8191. See the Usage Guidelines.

vni

Specifies the VNI (VXLAN Network Identifier) token.
vni

A single VXLAN VNI or range of VXLAN VNIs. Range is from 1 through 16777215. See the Usage Guidelines.

auto

Enables automatic VLAN-to-VNI mapping for every VLAN associated with the tunnel.

Modes

VXLAN overlay gateway configuration mode

Usage Guidelines

Note the following conditions:

- Before using this command, you must first set the VXLAN overlay gateway to layer2-extension, by means of the **type** command.
- Before using this command, you must first configure the appropriate VLANs to be used by the gateway.
- Before mapping VLANs to VNIs manually, you cannot have automatic mapping configured (by means of the **map vlan vni auto** command).
- You cannot map one VLAN to multiple VNIs. Similarly, you cannot map a single VNI to multiple VLANs. For example, VLAN-to-VNI mapping should be one to one.
- A single VLAN ID and a range of VLAN IDs can both be specified in a single command as follows: *x,y-z*. The same applies to VNIs.
- When using ranges, you must ensure that the number of values in a VLAN ID range corresponds to the number of values in a VNI range.

- The **no** forms of this command are allowed only if no VLANs are referenced by means of the **extend vlan** command (under a submode of the **site** command). For example, VLANs extended to a site should have a VNI mapping.
- The **no map vlan vni auto** command disables the automatic assignment of VNIs. It is not allowed if manual VLAN-to-VNI mappings have been configured. For example, "auto" VLAN-to-VNI mapping and "explicit" VLAN-to-VNI mapping are mutually exclusive.
- The **no map vlan** *vlan_id* command removes the VNI mappings for one or more VLANs.
- You cannot delete a VLAN (by means of the **no interface vlan** command) that is referenced by means of the **map vlan vni** command.
- This command does not trigger VLAN provisioning, unlike the behavior of the **attach vlan** command.
- Either automatic or manual VLAN mapping is supported. Hybrid mode is not supported.

Examples

To configure a manual mapping of VLANs to VNIs in "gateway1":

```
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# map vlan 10,20-22 vni 5000-5002,6000
```

This results in the following in the running configuration:

```
overlay-gateway gateway1
  type layer2-extension mode vxlan-ipv4
  map vlan 10 vni 5000
  map vlan 20 vni 5001
  map vlan 21 vni 5002
  map vlan 22 vni 6000
```

To configure an automatic mapping of VLANs to VNIs in "gateway1":

```
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# map vlan vni auto
```

map vni auto (VXLAN gateway)

Configures an automatic mapping of VLANs/bridge domains (BDs) to Virtual Network Identifiers (VNIs).

Syntax

map vni auto

no map vni auto

Command Default

This feature is not enabled.

Modes

VXLAN overlay gateway configuration mode

Usage Guidelines

Use the **no** form of this command to undo the automatic mapping.

Examples

The following example configures the automatic mapping of VLANs/BDs) to VNIs.

```
device# configure terminal
device(config)# overlay-gateway mygateway
device(config-overlay-gateway-mygateway)# map vni auto
```

The following example undoes the mapping.

```
device# configure terminal
device(config)# overlay-gateway mygateway
device(config-overlay-gateway-mygateway)# no map vni auto
```

master-vlan (STP)

Selects a master VLAN for a topology group.

Syntax

master-vlan *vlan_id*

Command Default

The master VLAN is not configured.

Parameters

vlan_id

The master VLAN ID.

Modes

Topology group configuration mode.

Usage Guidelines

To configure a master VLAN, the VLAN must already be configured. The master VLAN contains the STP settings for all the VLANs in the STP per VLAN group. An STP group can have only one master VLAN. If you add a new master VLAN to an STP group that already has a master VLAN, the new master VLAN replaces the older master VLAN.

If you remove the master VLAN (by entering the **no master-vlan** command), the software selects the new master VLAN from member VLANs. A new candidate master VLAN will be in configured as a member VLAN so that the first added member VLAN will be a new candidate master VLAN. Once you save and reload, a member VLAN with the youngest VLAN ID will be the new candidate master.

Examples

The following example adds the member VLANs to the STP topology group.

```
device# configure terminal
device(config)# topology-group 10
device(config-topo-group-10)# master-vlan 15
```

match (route maps)

Defines a variety of match conditions for a route map.

Syntax

match as-path *name*

match community *name* **exact-match**]

match extcommunity *number*

match interface { **ethernet** *slot* **/** *port* | **loopback** *num*| **ve-interface** *vlan_id* }

match ip address { **acl** *name* [**prefix-list** *string*] | **prefix-list** *string* [**acl** *name* }

match ip next-hop prefix-list *string*

match ip route-source prefix-list *string*

match ipv6 next-hop prefix-list *string*

match ipv6 route-source prefix-list *string*

match metric *num*

match protocol bgp { **external** | **internal** | **static-network** }

match protocol static

match route-type { **internal** | **type-1** | **type-2** }

match tag *num*

match vrf *name*

no match as-path

no match community

no match extcommunity

no match interface

no match ip address

no match ip next-hop

no match ip route-source

no match ipv6 address

no match ipv6 next-hop

no match ipv6 route-source

no match metric

no match protocol

no match route-type

no match tag

Command Default

This option is disabled.

Parameters

as-path

Matches an AS-path access list name in a route-map instance.
name

Name of an AS-path access list. Range is from 1 through 32 ASCII characters.

community

Matches a BGP community access list name in a route-map instance.
name

Name of a BGP community access list. Values range from 1 through 32 ASCII characters.

exact-match

Matches a route only if the route community attributes field contains the same community numbers specified in the **match** statement.

extcommunity *number*

Matches a BGP extended community list in a route-map instance and specifies an extended community list number. Valid values range from 1 through 99.

interface

Matches interface conditions in a route-map instance.

ethernet

Specifies an ethernet interface.
slot

Specifies a valid slot number. If the device does not have linecards, specify `0`.

port

Specifies a valid port number.

loopback *num*

Specifies a loopback interface.

ve-interface *vlan_id*

Specifies a virtual Ethernet VLAN interface.

ip address

Matches an IP address in a route-map instance.
acl *name*

Name of the access list. Range is from 1 through 32 ASCII characters.

prefix-list *string*

Specifies an IP prefix list. Range is from 1 through 32 ASCII characters.

ip next-hop

Matches IP next-hop match conditions in a route-map instance.

ip route-source

Matches an IP route source in a route-map instance.

ipv6 address

Matches an IPv6 address in a route-map instance.

ipv6 next-hop

Matches IPv6 next-hop match conditions in a route-map instance.

ipv6 route-source

Matches an IPv6 route source in a route-map instance.

metric *num*

Matches a route metric in a route-map instance. Values range from 0 through 4294967295.

protocol bgp external

Matches on BGP routes.

protocol bgp internal

Matches on iBGP routes.

protocol bgp static-network

Matches on BGP4 static network routes. This is applicable only for BGP outbound policy.

protocol static

Matches on static routes.

route-type

Matches a route type in a route-map instance.

internal

Internal route type

type-1

OSPF external route type 1

type-2

OSPF external route type 2

tag *tag-value*

Specifies a route tag and route tag value.

vrf *name*

Specifies a non-default VRF. Valid values range from 0 through 4294967295.

Modes

Route-map configuration mode

Usage Guidelines

For non-BGP route-maps, refer to the following topics:

- **match ip address acl**
- **match ipv6 address acl**

The **no** form of the command restores the default.

Examples

The following example matches AS-path ACL 1 in route-map instance “myroutes”.

```
device#configure terminal
device(config)# route-map myroutes permit 10
device(config-route-map myroutes/permit/10)# match as-path 1
```

match access-group

Matches an ACL to a class map.

Syntax

match access-group *name*

Parameters

name

The ACL name.

Modes

Class map configuration mode.

Usage Guidelines

The command is used after the **class-map** command is entered.

Examples

Use this command to match an ACL to a class map.

```
device(config)# class-map default
device(config-classmap)# match access-group class_acl
```

match additional-paths advertise-set

Enables filtering of additional-paths to be advertised for a route map.

Syntax

match additional-paths advertise-set [**all**] [**best** *num*] [**best-range** *start-num end-num*] [**group-best**]

no match additional-paths [**all**] **advertise-set** [**best** *num*] [**best-range** *start-num end-num*] [**group-best**]

Command Default

By default, a route map is not configured to filter advertised paths.

Parameters

all

Causes all (up to a maximum of 16) routes to be advertised.

best *num*

Specifies the number of best routes to advertise.

best-range

Causes advertisement of routes within a number range.

start-num

Specifies the start number of the range of routes to advertise. The number ranges from 1 through 16.

end-num

Specifies the end number of the range of routes to advertise. The number ranges from 1 through 16.

group-best

Advertises the group-best path.

Modes

Route-map configuration mode

Usage Guidelines

A match occurs when an additional path that is a candidate for advertisement has the same path marking (tag) as the marking configured by using the **match additional-paths advertise-set** command.

Only one **match additional-paths advertise-set** command configuration is allowed for each route map; any subsequent **match additional-paths advertise-set** command configuration overwrites the previous configuration.

The **no** form of the command restores the default configuration.

Examples

The following example shows how to configure route map (rm_example) to advertise the group-best route.

```
device# configure terminal
device(config)# route-map rm_example permit 123
device(config-routemap-rm_example/permit/123)# match additional-paths advertise-set group-
best
```

match as-path

Syntax

```
{ | } [ ]
```

Command Default

Parameters

Modes

.

Usage Guidelines

.

.

Examples

match bridge-domain

Matches a bridge domain to a class map.

Syntax

match bridge-domain *BD-number*

Parameters

BD-number

Specifies a valid bridge-domain number.

Modes

Class map configuration mode.

Usage Guidelines

The command is used after the **class-map** command is entered.

Examples

The following example matches a bridge domain to a class map.

```
device(config)# class-map BD-1000
device(config-classmap)# match bridge-domain 1000
```

match community

Matches a community access list name in a route-map instance.

Syntax

match community *name*

no match community

Parameters

name

Name of a community access list. Values range from 1 through 32 ASCII characters.

Modes

Route-map configuration mode

Usage Guidelines

Enter **no match community** *name* to disable this feature.

You can configure up to five match community directives within a single stanza.

Examples

Typical command example:

```
device# config terminal
device(config)# route-map myroutes permit 10
device(config-route-map myroutes/permit/10)# match community ABCPath
```

match destination-port

Configures matching based on UDP or TCP destination port for a route-map sequence number.

Syntax

match destination-port { **eq** | **gt** | **lt** } *port-num-1*

match destination-port neq *port-num-1* [... *port-num-32*]

match destination-port range *port-num-1 port-num-2*

no match destination-port { **eq** | **gt** | **lt** } *port-num-1*

no match destination-port neq *port-num-1* [... *port-num-32*]

no match destination-port range *port-num-1 port-num-2*

Command Default

Matching based on destination port is not configured.

Parameters

eq *port-num-1*

Specifies that matching occurs when the packet destination port is equal to the specified port number, which must be a valid UDP or TCP port number in the range from 0 through 65535.

gt *port-num-1*

Specifies that matching occurs when the packet destination port is greater than the specified port number, which must be a valid UDP or TCP port number in the range from 0 through 65535.

lt *port-num-1*

Specifies that matching occurs when the packet destination port is less than the specified port number, which must be a valid UDP or TCP port number in the range from 0 through 65535.

neq *port-num-1* [... *port-num-32*]

Specifies that matching occurs when the packet destination port is not equal to all of the specified ports. You can specify a maximum of 32 ports. Specified ports must be valid UDP or TCP port numbers in the range from 0 through 65535.

range *port-num-1 port-num-2*

Specifies that matching occurs when the packet destination port is within the specified range of port numbers, which must be valid UDP or TCP port numbers in the range from 0 through 65535.

Modes

Route-map configuration mode

Usage Guidelines

When **match protocol** and **match destination-port** are specified in the same stanza, the protocol specified by the **match protocol** command must be either TCP or UDP.

Up to 128 **match destination-port** statements are allowed per route-map sequence number for the following options:

- **eq**
- **range**

When multiple **match destination-port** statements of the same type exist, matching occurs when traffic matches any one of the statements.

Only one **match destination-port** statement is allowed per route-map sequence number for the following options:

- **lt**
- **gt**
- **neq**

Note
Configuring the **range** option may create a lot of TCAM entries (due to rule expansion).

The **no** form of the command disables the configuration.

Examples

The following example shows how to configure matching based on destination port number 45 for sequence number 4 in a route-map named rm.

```
device# configure terminal
device(config)# route-map rm permit 4
device(config-route-map-rm/permit/4)# match destination-port eq 45
```

The following example shows how to configure matching based on destination port for sequence number 4 in a route-map named rm; a match occurs when traffic destination port is not equal to 34 and 56 and 67.

```
device# configure terminal
device(config)# route-map rm permit 4
device(config-route-map-rm/permit/4)# match destination-port neq 34 56 67
```

match dscp

Configures matching based on a Differentiated Services Code Point (DSCP) value or range of values for a route-map sequence number.

Syntax

match dscp { **eq** | **gt** | **lt** } *value-1*

match dscp neq *value-1* [… *value-32*]

match dscp range *value-1 value-2*

no match dscp { **eq** | **gt** | **lt** } *value-1*

no match dscp neq *value-1* [… *value-32*]

no match dscp range *value-1 value-2*

Command Default

Matching based on DSCP value is not configured.

Parameters

eq *value-1*

Specifies that matching occurs when the packet DSCP value is equal to the specified DSCP value.

gt *value-1*

Specifies that matching occurs when the packet DSCP value is greater than the specified DSCP value.

lt *value-1*

Specifies that matching occurs when the packet DSCP value is less than the specified DSCP value.

neq *value-1* [… *value-32*]

Specifies that matching occurs when the packet DSCP value is not equal to all of the specified DSCP values. You can specify a maximum of 32 values.

range *value-1 value-2*

Specifies that matching occurs when the packet DSCP value is within the specified range of DSCP values.

Modes

Route-map configuration mode

Usage Guidelines

Up to 128 **match dscp** statements are allowed per route-map sequence number for the following options:

- **eq**
- **range**

When multiple **match dscp** statements of the same type exist, matching occurs when traffic matches any one of the statements.

Only one **match dscp** statement is allowed per route-map sequence number for the following options:

- **lt**
- **gt**
- **neq**

Note
Configuring the **range** option may create a lot of TCAM entries (due to rule expansion).

The **no** form of the command disables the configuration.

Examples

The following example shows how to configure matching based on DSCP value (23) for sequence number 4 under a route map named rm.

```
device# configure terminal
device(config)# route-map rm permit 4
device(config-route-map-rm/permit/4)# match dscp eq 23
```

match extcommunity

Matches an extended community list in a route-map instance.

Syntax

match extcommunity *number*

no match extcommunity

Command Default

BGP extended community access list names are not matched.

Parameters

name

Extended community list number. Values range from 1 through 99.

Modes

Route-map configuration mode.

Usage Guidelines

Enter **no match extcommunity** to remove the community match statement from the configuration file.

You can configure up to five match extcommunity directives within a single stanza.

Examples

To configure a route map that matches on extended community ACL 1.

```
device# configure terminal
device(config)# ip extcommunity-list 1 permit 123:2
device(config)# route-map extComRmap permit 10
device(config-route-map-extComRmap/permit/10)# match extcommunity 1
```

match fragment-type

Configures matching based on fragmentation type for a route-map sequence number.

Syntax

match fragment-type { **all** | **any** } [**dont-fragment**] [**first-fragment** | **not-first-fragment**] [**fragment** | **not-fragment**] [**last-fragment** | **not-last-fragment**]

no match fragment-type { **all** | **any** } [**dont-fragment**] [**first-fragment** | **not-first-fragment**] [**fragment** | **not-fragment**] [**last-fragment** | **not-last-fragment**]

Command Default

Matching based on fragmentation type is not configured.

Parameters

all

Specfies that matching occurs when traffic matches all of the subsequent specified options.

any

Specfies that matching occurs when traffic matches any of the subsequent specified options.

dont-fragment

Specifies matching based on fragmentation type being equal to DF

first-fragment

Specifies matching based fragmentation type being equal to FF.

not-first-fragment

Specifies matching based on fragmentation type not being equal to FF.

fragment

Specifies that matching occurs when the packet is an IP fragment.

not-fragment

Specifies that matching occurs when the packet is not an IP fragment.

last-fragment

Specifies matching based on fragmentation type being equal to LF.

not-last-fragment

Specifies matching based on fragmentation type not being equal to FF.

Modes

Route-map configuration mode

Usage Guidelines

When issuing the **match fragment-type** command, you must specify either **all** or **any** and at least one other option.

You can configure multiple options by using the **match fragment-type** command.

Up to 128 **match fragment-type** configurations are allowed per route-map sequence number.

When multiple **match fragment-type** configurations exist, matching occurs when traffic matches any one of the configured fragment type configurations.

The **no** form of the command removes the configuration.

Examples

The following example shows how to configure matching based on fragmentation type being equal to **first-fragment** or not equal to **last-fragment** for sequence number 4 in a route-map named rm.

```
device# configure terminal
device(config)# route-map rm permit 4
device(config-route-map-rm/permit/4)# match fragment-type any first-fragment not-last-
fragment
```

The following example shows how to configure matching based on fragmentation type equal to **last-fragment** for sequence number 4 in a route-map named rm.

```
device# configure terminal
device(config)# route-map rm permit 4
device(config-route-map-rm/permit/4)# match fragment-type all last-fragment
```

match ip

Configures matching based on an IPv4 source or destination prefix for a route-map sequence number.

Syntax

match ip { **source-address** | **destination-address** } *ip-address/ip-mask*

no match ip { **source-address** | **destination-address** } *ip-address/ip-mask*

Command Default

IPv4 source or destination prefix matching is not configured.

Parameters

source-address

Specifies matching based on source IP address.

destination-address

Specifies matching based on destination IP address.

ip-address/ip-mask

Specifies an IPv4 address and mask.

Modes

Route-map configuration mode

Usage Guidelines

Only one **match ip** configuration is allowed per route-map sequence number.

When both **match ip source-address** and **match ip destination-address** are configured, a match occurs when traffic matches both the configured source address and the configured destination address.

The **no** form of the command disables the configuration.

Examples

The following example shows how to configure matching based on a source address (10.2.0.1/16) for sequence number 4 in a route-map named rm.

```
device# configure terminal
device(config)# route-map rm permit 4
device(config-route-map-rm/permit/4)# match ip source-address 10.2.0.0/16
```

match ip address acl

In a route-map stanza, matches IPv4 address conditions specified in an IPv4 ACL.

Syntax

match ip address acl *acl-name*

no match ip address acl *acl-name*

Parameters

acl-name

Specifies an IPv4 ACL name unique among all ACLs (Layer 2 and Layer 3). The name can from 1 through 63 characters in length and must begin with an alphanumeric character. No special characters are allowed, except for the underscore and hyphen.

Modes

Route-map configuration mode

Usage Guidelines

The absence of a **match** statement is treated as "match any"; all traffic is forwarded according to the **set** statement.

Use the **no** form of this command to remove the match.

Examples

The following example creates an IPv4 ACL that permits traffic from a specific source IP and then includes that ACL in a route-map stanza.

```
device# configure terminal
device(config)# ip access-list standard acl_01
device(conf-ipacl-std)# permit host 192.1.1.1 count
device(conf-ipacl-std)# exit
device(config)# route-map example1 permit 1
device(config-route-map-example1/permit/1)# match ip address acl acl_01
```

match ip icmp-code

Configures matching based on Internet Control Message Protocol (ICMP) code for a route-map sequence number.

Syntax

match ip icmp-code { **eq** | **gt** | **lt** } *icmp-code-1*

match ip icmp-code neq *icmp-code-1* [… *icmp-code-32*]

match ip icmp-code range *icmp-code-1 icmp-code-2*

no match ip icmp-code { **eq** | **gt** | **lt** } *icmp-code-1*

no match ip icmp-code neq *icmp-code-1* [… *icmp-code-32*]

no match ip icmp-code range *icmp-code-1 icmp-code-2*

Command Default

Matching based on ICMP code is not configured.

Parameters

eq *icmp-code-1*

Specifies that matching occurs when the packet ICMP code is equal to the specified ICMP code or well-known ICMP code value.

gt *icmp-code-1*

Specifies that matching occurs when the packet ICMP code is greater than the specified ICMP code or well-known ICMP code value.

lt *icmp-code-1*

Specifies that matching occurs when the packet ICMP code is less than the specified ICMP code or well-known ICMP code value.

neq *icmp-code-1* [… *icmp-code-32*]

Specifies that matching occurs when the packet ICMP code is not equal to all of the specified ICMP codes or well-known ICMP code values. You can specify a maximum of 32 codes or code values.

range *icmp-code-1 icmp-code-2*

Specifies that matching occurs when the packet ICMP code is within the range of specified ICMP codes or well-known ICMP code values.

Modes

Route-map configuration mode

Usage Guidelines

When **match protocol** and **match ip icmp-code** are specified in the same stanza, the protocol specified by the **match protocol** command must be ICMP; specifying any other protocol value using the **match protocol** command results in the rule being evaluated as false and it becomes inactive.

Up to 128 **match ip icmp-code** statements are allowed per route-map sequence number for the following options:

- **eq**
- **range**

When multiple **match ip icmp-code** statements of the same type exist, matching occurs when traffic matches any one of the statements.

Only one **match ip icmp-code** statement is allowed per route-map sequence number for the following options:

- **lt**
- **gt**
- **neq**

Note
Configuring the **range** option may create a lot of TCAM entries (due to rule expansion).

The **no** form of the command disables the configuration.

Examples

The following example shows how to configure matching based on ICMP codes in the range from 3 through 5.

```
device# configure terminal
device(config)# route-map rm permit 4
device(config-route-map-rm/permit/4)# match ip icmp-code range 3 5
```

match ip icmp-type

Configures matching based on Internet Control Message Protocol (ICMP) type for a route-map sequence number.

Syntax

match ip icmp-type { **eq** | **gt** | **lt** } *icmp-type-1*

match ip icmp-type neq *icmp-type-1* [… *icmp-type-32*]

match ip icmp-type range *icmp-type-1 icmp-type-2*

no match ip icmp-type { **eq** | **gt** | **lt** } *icmp-type-1*

no match ip icmp-type neq *icmp-type-1* [… *icmp-type-32*]

no match ip icmp-type range *icmp-type-1 icmp-type-2*

Command Default

Matching based on ICMP type is not configured.

Parameters

eq *icmp-type-1*

Specifies that matching occurs when the packet ICMP type is equal to the specified ICMP type or well-known ICMP type value.

gt *icmp-type-1*

Specifies that matching occurs when the packet ICMP type is greater than the specified ICMP type or well-known ICMP type value.

lt *icmp-type-1*

Specifies that matching occurs when the packet ICMP code is less than the specified ICMP type or well-known ICMP type value.

neq *icmp-type-1* [… *icmp-type-32*]

Specifies that matching occurs when the packet ICMP type (or ICMP type value) is not equal to all of the specified ICMP types. You can specify a maximum of 32 ICMP types. S

range *icmp-type-1 icmp-type-2*

Specifies that matching occurs when the packet ICMP type is within the range of specified ICMP types or well-known ICMP type values.

Modes

Route-map configuration mode

Usage Guidelines

When **match protocol** and **match ip icmp-type** are specified in the same stanza, the protocol specified by the **match protocol** command must be ICMP; specifying any other protocol value using the **match protocol** command results in the rule being evaluated as false and it becomes inactive.

Up to 128 **match ip icmp-type** statements are allowed per route-map sequence number for the following options:

- **eq**
- **range**

When multiple **match ip icmp-type** statements of the same type exist, matching occurs when traffic matches any one of the statements.

Only one **match ip icmp-type** statement is allowed per route-map sequence number for the following options:

- **lt**
- **gt**
- **neq**

Note
Configuring the **range** option may create a lot of TCAM entries (due to rule expansion).

The **no** form of the command disables the configuration.

Examples

The following example shows how to configure matching when the packet ICMP type is not equal to 5.

```
device# configure terminal
device(config)# route-map rm permit 4
device(config-route-map-rm/permit/4)# match ip icmp-type neq 5
```

match ipv6 address

Matches IPv6 address conditions in a route map instance.

Syntax

match ipv6 address { **prefix-list** *prefix-list-name* }

no match ipv6 address

Command Default

No routes are distributed based on destination network number.

Parameters

prefix-list *prefix-list-name*

Specifies the name of an IPv6 prefix list.

Modes

Route-map configuration mode

Usage Guidelines

Use the **no** form of this command to remove the **match ipv6 address** entry.

Examples

match ipv6 address acl

In a route map instance, matches IPv6 address conditions specified in an IPv6 ACL.

Syntax

match ipv6 address acl *acl-name*

no match ipv6 address acl *acl-name*

Parameters

acl-name

Specifies an IPv6 ACL name unique among all ACLs (Layer 2 and Layer 3). The name can from 1 through 63 characters in length and and must begin with an alphanumeric character. No special characters are allowed, except for the underscore and hyphen.

Modes

Route-map configuration mode

Usage Guidelines

The absence of a **match** statement is treated as "match any"; all traffic is forwarded according to the **set** statement.

Use the **no** form of this command to remove the match.

Examples

The following example creates an IPv6 ACL that permits traffic from specific sources and denies traffic from another source. The example then includes that ACL in a route-map stanza.

```
device# configure terminal
device(config)# ipv6 access-list extended acl6_01
device(conf-ip6acl-ext)# seq 10 permit ipv6 any host 2000::1 count
device(conf-ip6acl-ext)# seq 20 permit ipv6 any host 2000::2 count
device(conf-ip6acl-ext)# seq 30 deny ipv6 any host 2000::3 count
device(conf-ip6acl-ext)# exit
device(config)# route-map example2 permit 1
device(config-route-map-example2/permit/1)# match ipv6 address acl acl6_01
```

match large-community

Filters routes by BGP Large Community attributes, using a partial or exact match with Large Community ACLs.

Syntax

match large-community *name* [**exact-match**]

no match large-community *name*

Command Default

No matching is configured.

Parameters

name

Name of a large community access list. The format is from 1 through 32 ASCII characters.

exact-match

Filters routes by using an exact match.

Modes

Route-map configuration mode

Usage Guidelines

Use the **no** form of this command to disable matching based on a large-community list.

A maximum of five Large Community ACLs can be configured to do a partial or exact match.

Examples

The following example shows how to configure matching based on a large-community access list named ABCPath for a route map named myroutes.

```
device# config terminal
device(config)# route-map myroutes permit 10
device(config-route-map myroutes/permit/10)# match large-community ABCPath
```

The following example shows how to configure matching based on a large-community access list named lcstdacl1 with an exact match for a route map named myroutes.

```
device# config terminal
device(config)# route-map myroutes permit 10
device(config-route-map myroutes/permit/10)# match large-community lcstdacl1 exact-match
```

match packet-length

Configures matching based on packet length for a route-map sequence number.

Syntax

match packet-length { **eq** | **gt** | **lt** } *value-1*

match packet-length neq *value-1* [**...** *value-32*]

match packet-length range *value-1 value-2*

no match packet-length { **eq** | **gt** | **lt** } *value-1*

no match packet-length neq *value-1* [**...** *value-32*]

no match packet-length range *value-1 value-2*

Command Default

Matching based on packet length is not configured.

Parameters

eq *value-1*

Specifies that matching occurs when the packet length (including the IP header but excluding the Layer 2 header) is equal to the specified value.

gt *value-1*

Specifies that matching occurs when the packet length (including the IP header but excluding the Layer 2 header) is greater than the specified value.

lt *value-1*

Specifies that matching occurs when the packet length (including the IP header but excluding the Layer 2 header) is less than the specified value.

neq *value-1* [**...** *value-32*]

Specifies that matching occurs when the traffic packet length (including the IP header but excluding the Layer 2 header)is not equal to all of the specified values. You can specify a maximum of 32 values.

range *value-1 value-2*

Specifies that matching occurs when the packet length (including the IP header but excluding the Layer 2 header) is within the range of specified values.

Modes

Route-map configuration mode

Usage Guidelines

Up to 128 **match packet-length** statements are allowed per route-map sequence number for the following options:

- **eq**
- **range**

When multiple **match packet-length** statements of the same type exist, matching occurs when traffic matches any one of the statements.

Only one **match packet-length** statement is allowed per route-map sequence number for the following options:

- **lt**
- **gt**
- **neq**

Note
Configuring the **range** option may create a lot of TCAM entries (due to rule expansion).

The **no** form of the command disables the configuration.

Examples

The following example shows how to configure matching based on a packet length of 1500 for sequence number 4 in a route map named rm.

```
device# configure terminal
device(config)# route-map rm permit 4
device(config-route-map-rm/permit/4)# match packet-length eq 1500
```

match port

Configures matching based on TCP or UDP source or destination port for a route-map sequence number.

Syntax

match port { **eq** | **gt** | **lt** } *port-num-1*

match port neq*port-num-1* [… *port-num-32*]

match port range *port-num-1 port-num-2*

no match port { **eq** | **gt** | **lt** } *port-num-1*

no match port neq*port-num-1* [… *port-num-32*]

no match port range *port-num-1 port-num-2*

Command Default

Source port or destination port matching is not configured.

Parameters

eq *port-num-1*

Specifies that matching occurs when the packet source port or destination port is equal to the specified port number, which must be a valid UDP or TCP port number in the range from 0 through 65535.

gt *port-num-1*

Specifies that matching occurs when the packet source port or destination port is greater than the specified port number, which must be a valid UDP or TCP port number in the range from 0 through 65535.

lt *port-num-1*

Specifies that matching occurs when the packet source port or destination port is less than the specified port number, which must be a valid UDP or TCP port number in the range from 0 through 65535.

neq*port-num-1* [… *port-num-32*]

Specifies that matching occurs when *neither* the packet source port nor packet destination port is equal to all of the specified ports. Specified ports must be a valid UDP or TCP port number in the range from 0 through 65535.

range *port-num-1 port-num-2*

Specifies that matching occurs when the packet source port or destination port is within the specified range of port numbers, which must be valid UDP or TCP port numbers in the range from 0 through 65535.

Modes

Route-map configuration mode

Usage Guidelines

When **match protocol** and **match port** are specified in the same stanza, the protocol specified by the **match protocol** command must be either TCP or UDP.

Up to 128 **match port** statements are allowed per route-map sequence number for the following options:

- **eq**
- **range**

Only one **match port** statement is allowed per route-map sequence number for the following options:

- **lt**
- **gt**
- **neq**

When multiple **match port** configurations exist, matching occurs when traffic matches any one of the configured ports.

Note
Configuring the **range** option may create a lot of TCAM entries (due to rule expansion).

The **no** form of the command disables the configuration.

Examples

The following example shows how to configure matching based on port numbered 45 for sequence number 4 in a route-map named rm; a match occurs when either the packet source or destination port is in the range from 3 through 6000.

```
device# configure terminal
device(config)# route-map rm permit 4
device(config-route-map-rm/permit/4)# match port range 3 6000
```

The following example shows how to configure matching based on port for sequence number 4 in a route-map named rm; a match occurs when both the packet source port and packet destination port are not equal to 34 and 56 and 67.

```
device# configure terminal
device(config)# route-map rm permit 4
device(config-route-map-rm/permit/4)# match port neq 34 56 67
```

match protocol

Configures protocol-based matching for a route-map sequence number.

Syntax

match protocol { **eq** | **gt** | **lt** } *protocol-1*

match protocol neq *protocol-1* [… *protocol-32*]

match protocol range *protocol-1 protocol-2*

no match protocol { **eq** | **gt** | **lt** } *protocol-1*

no match protocol neq *protocol-1* [… *protocol-32*]

no match protocol range *protocol-1 protocol-2*

Command Default

Protocol-based matching is not configured.

Parameters

eq *protocol-1*

Specifies that matching occurs when the traffic IP protocol is equal to the specified protocol. The protocol can be specified in either name or number format.

gt *protocol-1*

Specifies that matching occurs when the traffic IP protocol is greater than the specified protocol. The protocol can be specified in either name or number format.

lt *protocol-1*

Specifies that matching occurs when the traffic IP protocol is less than the specified protocol. The protocol can be specified in either name or number format.

neq *protocol-1* [… *protocol-32*]

Specifies that matching occurs when the traffic IP protocol is not equal to all of the specified protocols. You can specify a maximum of 32 protocols. Protocols can be specified in either name or number format.

range *protocol-1 protocol-2*

Specifies that matching occurs when the traffic IP protocol is within the specified range of protocols. Protocols rotocol can be specified in either name or number format.

Modes

Route-map configuration mode

Usage Guidelines

When **match protocol** and **match ip icmp-code** are specified in the same stanza, the protocol specified by the **match protocol** command must be ICMP; specifying any other protocol value using the **match protocol** command results in the rule being evaluated as false and it becomes inactive.

When **match protocol** and **match ip icmp-type** are specified in the same stanza, the protocol specified by the **match protocol** command must be ICMP; specifying any other protocol value using the **match protocol** command results in the rule being evaluated as false and it becomes inactive.

When **match protocol** and **match port**, **match source-port**, or **match destination-port** are specified in the same stanza, the protocol specified by the **match protocol** command must be either TCP or UDP.

Up to 128 **match protocol** statements are allowed per route-map sequence number for the following options:

- **eq**
- **range**

When multiple **match protocol** statements of the same type exist, matching occurs when traffic matches any one of the statements.

Only one **match protocol** statement is allowed per route-map sequence number for the following options:

- **lt**
- **gt**
- **neq**

Note
Configuring the **range** option may create a lot of TCAM entries (due to rule expansion).

The **no** form of the command disables the configuration.

Examples

The following example shows how to configure protocol-based matching for sequence number 4 in a route-map named rm; a match occurs when traffic is not equal to 34 and 56 and 67.

```
device# configure terminal
device(config)# route-map rm permit 4
device(config-route-map-rm/permit/4)# match protocol neq 34 56 67
```

The following example shows how to configure matching based on a range of protocols (3 through 10) for sequence number 4 in a route-map named rm.

```
device# configure terminal
device(config)# route-map rm permit 4
device(config-route-map-rm/permit/4)# match protocol range 3 10
```

match rpki

In a route map configuration, this command is used to indicate what actions need to be performed for the validation state being configured. When a prefix is validated with the RPKI cache, the following three states are reported, *valid*, *invalid*, and *not found*. Use this command to configure the matching criteria. Once you have configured the matching parameter, you must configure the various actions that need to be performed when a prefix is received and is matched with the RPKI cache on the SLX device.

Syntax

match rpki { *valid* | *invalid* | *not-found* }

[no] match rpki { *valid* | *invalid* | *not-found* }

Parameters

valid

Indicates that the received prefix is valid when compared with the local RPKI cache.

invalid

Indicates that the received prefix is invalid when compared with the local RPKI cache.

not-found

Indicates that the received prefix is not-found when compared with the local RPKI cache.

Modes

Route Map

Usage Guidelines

Use the [no] format of this command to remove **match rpki** configured for a route map configuration.

Examples

This command shows the steps to create a **match rpki** configuration within the Route Map (BGP) permit entry.

This command creates a route map permit entry.

```
SLX(config)# route-map rm-bgp-p-test-01 permit 1
                    SLX(config-route-map-rm-bgp-p-test-01/permit/1)#
```

This command creates a match RPKI entry for valid prefixes.

```
SLX(config-route-map-rm-bgp-p-test-01/permit/1)#
SLX(config-route-map-rm-bgp-p-test-01/permit/1)# match rpki valid
SLX(config-route-map-rm-bgp-p-test-01/permit/1)#
```

This command adds the other configurations for this route map permit entry.

```
SLX(config-route-map-rm-bgp-p-test-01/permit/1)#
SLX(config-route-map-rm-bgp-p-test-01/permit/1)# match metric 10
SLX(config-route-map-rm-bgp-p-test-01/permit/1)# continue
SLX(config-route-map-rm-bgp-p-test-01/permit/1)# set weight 10
```

This example shows the steps to remove the match rpki configuration from an existing route-map configuration.

```
(1)SLX(config-route-map-rm-bgp-p-test-01/deny/1)#
SLX(config-route-map-rm-bgp-p-test-01/deny/1)# match rpki invalid
SLX(config-route-map-rm-bgp-p-test-01/permit/1)#
```

match source-port

Configures matching based on UDP or TCP source port for a route-map sequence number.

Syntax

match source-port { **eq** | **gt** | **lt** } *port-num-1*

match source-port neq *port-num-1* [… *port-num-32*]

match source-port range *port-num-1 port-num-2*

no match source-port { **eq** | **gt** | **lt** } *port-num-1*

no match source-port neq *port-num-1* [… *port-num-32*]

no match source-port range *port-num-1 port-num-2*

Command Default

Matching based on source port is not configured.

Parameters

eq *port-num-1*

Specifies that matching occurs when the packet source port is equal to the specified port number, which must be a valid UDP or TCP port number in the range from 0 through 65535.

gt *port-num-1*

Specifies that matching occurs when the packet source port is greater than the specified port number, which must be a valid UDP or TCP port number in the range from 0 through 65535.

lt *port-num-1*

Specifies that matching occurs when the packet source port is less than the specified port number, which must be a valid UDP or TCP port number in the range from 0 through 65535.

neq *port-num-1* [… *port-num-32*]

Specifies that matching occurs when the packet destination port is not equal to all of the specified ports. You can specify a maximum of 32 ports. Specified ports must be a valid UDP or TCP port number in the range from 0 through 65535.

range *port-num-1 port-num-2*

Specifies that matching occurs when the packet source is within the specified range of port numbers, which must be a valid UDP or TCP port numbers in the range from 0 through 65535.

Modes

Route-map configuration mode

Usage Guidelines

When **match protocol** and **match source-port** are specified in the same stanza, the protocol specified by the **match protocol** command must be either TCP or UDP.

Up to 128 **match source-port** statements are allowed per route-map sequence number for the following options:

- **eq**
- **range**

When multiple **match source-port** statements of the same type exist, matching occurs when traffic matches any one of the statements.

Only one **match source-port** statement is allowed per route-map sequence number for the following options:

- **lt**
- **gt**
- **neq**

Note
Configuring the **range** option may create a lot of TCAM entries (due to rule expansion).

The **no** form of the command disables the configuration.

Examples

The following example shows how to configure matching based on a source port numbered 45 for sequence number 4 in a route-map named rm.

```
device# configure terminal
device(config)# route-map rm permit 4
device(config-route-map-rm/permit/4)# match source-port eq 45
```

The following example shows how to configure matching based on source port for sequence number 4 in a route-map named rm; a match occurs when traffic source port is not equal to 34 and 56 and 67.

```
device# configure terminal
device(config)# route-map rm permit 4
device(config-route-map-rm/permit/4)# match source-port neq 34 56 67
```

match tcp-flags

Configures Transmission Control Protocol (TCP) flag-based matching for a route-map sequence number.

Syntax

```
match tcp-flags { any | all } [ ack | not-ack ] [ cwr | not-cwr ] [ ece
    | not-ece ] [ fin | not-fin ] [ push | not-push ] [ rst | not-rst ]
    [ syn | not-syn ] [ urg | not-urg ]

no match tcp-flags { any | all } [ ack | not-ack ] [ cwr | not-cwr ]
    [ ece | not-ece ] [ fin | not-fin ] [ push | not-push ] [ rst |
    not-rst ] [ syn | not-syn ] [ urg | not-urg ]
```

Command Default

Matching based on TCP flags is not configured.

Parameters

all

Specfies that matching occurs when traffic matches all of the subsequent specified options.

any

Specfies that matching occurs when traffic matches any of the subsequent specified options.

ack

Configures matching based on TCP Acknowledgement flag.

not-ack

Configures matching based on no TCP Acknowledgement flag.

cwr

Configures matching based on TCP Congestion Window Reduced (CWR) flag. This match criterion is not supported in the hardware but is still received and advertised by BGP.

not-cwr

Configures matching based on no TCP CWR flag. This match criterion is not supported in the hardware but is still received and advertised by BGP.

ece

Configures matching based on TCP Explicit Congestion Notification Echo (ECE) flag. This match criterion is not supported in the hardware but is still received and advertised by BGP.

not-ece

Configures matching based on no TCP ECE flag. This match criterion is not supported in the hardware but is still received and advertised by BGP.

fin

Configures matching based on TCP FIN (finish) flag.

not-fin

Configures matching based on no TCP FIN flag.

push

Configures matching based on TCP PUSH flag.

not-push

Configures matching based on no TCP PUSH flag.

rst

Configures matching based on TCP RST (reset) flag.

not-rst

Configures matching based on no TCP RST flag.

syn

Configures matching based on TCP Synchronization flag.

not-syn

Configures matching based on no TCP Synchronization flag.

urg

Configures matching based on TCP URG (urgent) flag.

not-urg

Configures matching based on no TCP URG flag.

Modes

Route-map configuration mode

Usage Guidelines

When **match protocol** and **match tcp-flags** are specified in the same stanza, the protocol specified by the **match protocol** command must be TCP; specifying any other protocol value using the **match protocol** command results in the rule being evaluated as false and it becomes inactive.

When it is possible to have multiple flag options together in a TCP packet header; for example SYN, ACK and so on, you can configure all options using one **match tcp-flags** command.

Up to 128 **match tcp-flags** configurations are allowed per route-map sequence number.

When multiple **match tcp-flags** configurations exist, matching occurs when traffic matches any one of the configurations.

The **no** form of the command removes the configuration.

Examples

The following example shows how to configure matching on the SYN and ACK TCP flags for sequence number 4 under a route-map named rm.

```
device# configure terminal
device(config)# route-map rm permit 4
device(config-route-map-rm/permit/4)# match tcp-flags any syn ack
```

The following example shows how to configure matching on both the PUSH and ACK TCP flags for sequence number 4 under a route-map named rm.

```
device# configure terminal
device(config)# route-map rm permit 4
device(config-route-map-rm/permit/4)# match tcp-flags all push ack
```

match vlan

Matches a VLAN to a class map.

Syntax

match vlan *VLAN-number*

Parameters

VLAN-number

Specifies a valid VLAN number.

Modes

Class map configuration mode.

Usage Guidelines

The command is used after the **class-map** command is entered.

Examples

The following example matches a VLAN to a class map.

```
device(config)# class-map p2
device(config-classmap)# match vlan 500
```

max-age

Sets the interval time in seconds between messages that the spanning tree receives from the interface.

Syntax

max-age *seconds*

no max-age

Command Default

20 seconds.

Parameters

seconds

Configures the STP interface maximum age. Valid values range from 6 through 40.

Modes

Spanning tree configuration mode

Usage Guidelines

Use this command to control the maximum length of time that passes before an interface saves its configuration Bridge Protocol Data Unit (BPDU) information.

If the **vlan** parameter is not provided, the *seconds* value is applied globally for all per-VLAN instances. However, for VLANs that have been configured explicitly, the per-VLAN configuration takes precedence over the global configuration.

When configuring the maximum age, the **max-age** command setting must be greater than the **hello-time** command setting. The following relationship should be kept:

```
(2 × (forward-delay - 1)) >= max-age >= (2 × (hello-time + 1))
```

Enter **no max-age** to return to the default configuration.

Examples

To configure the maximum age to 10 seconds:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# max-age 10

device# configure terminal
```

```
device(config)# protocol spanning-tree rstp
device(conf-rstp)# max-age 10

device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# max-age 10

device# configure terminal
device(config)# protocol spanning-tree pvst
device(conf-pvst)# max-age 10

device# configure terminal
device(config)# protocol spanning-tree rpvst
device(conf-rpvst)# max-age 10
```

max-bypasses

Use the **max-bypasses** command to configure the maximum number of dynamic bypass LSPs that can be created in the system or on a MPLS interface.

Syntax

max-bypasses { *max_bypass_count* }

no max-bypasses { *max_bypass_count* }

Command Default

The default value is 250.

Parameters

max_bypass-count

This number must be less than or equal to the global maximum number of bypass LSPs; that is, the total amount of static bypasses and dynamic bypasses that can be configured on a router or on an interface. The value can be between 1 and 500.

Modes

MPLS router dynamic bypass configuration mode (config-router-mpls-dynamic-bypass).

MPLS router MPLS interface dynamic bypass configuration mode (config-router-mpls-if ethernet-*slot/port*-dynamic-bypass)

Usage Guidelines

The maximum number of bypass LSPs supported on a router is limited to 500. The maximum number of dynamic bypass LSP that can be configured on a system is (500 - (current number of configured Bypass LSPs)).

When this parameter is not configured under interface mode, the global **max-bypasses** parameter value is considered for this parameter. This parameter value must be less than the globally set **max-bypasses** value.

The no form of the command removes the maximum bypass limit and falls back to the default value of 250.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures the maximum number of bypasses to 300.

```
device>configure
device(config)# router mpls
device9Config-router-mpls)# dynamic bypass
device(config-router-mpls-dynamic-bypass)# max-bypasses 300
```

the following example disables the max-bypasses command for MPLS Ethernet interface *0/8*.

```
device>configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/8
device(config-router-mpls-if-ethernet-0/8)# dynamic bypass
device(config-router-mpls-if-ethernet-0/8-dynamic-bypass)# disable
```

max-bypasses-per-mp

Use the **max-bypasses-per-mp** command in the global mode or interface mode to configure the maximum number of dynamic bypass LSPs that can be created to a merge point.

Syntax

max-bypasses-per-mp { *max_bypass_per_mp_count* }

no max-bypasses-per-mp { *max_bypass_per_mp_count* }

Command Default

The system inherits the configured **max-bypasses** command value.

Parameters

max_bypass_per_mp_count

Specifies the number of maximum bypasses for each merge point. The range is from 1 to 500.

Modes

MPLS router dynamic bypass configuration mode (config-router-mpls-dynamic-bypass).

MPLS router MPLS interface dynamic bypass configuration mode (config-router-mpls-if-ethernet-*slot/port*-dynamic-bypass).

Usage Guidelines

The global value is taken as the interface mode maximum bypasses per MP default value (when the user has not configured this value in the interface mode).

This is the limit for the total number of dynamic bypass LSPs that can be created to a MP corresponding to a protected interface. A PLR can have 'M' number of MP to a protected LSP. There can be 'N' number of protected LSPs riding on an interface with dynamic bypass enabled. The max-bypasses configuration limits the maximum number of dynamic bypass LSPs that can be sent to each Merge Point.

When the **max-bypasses-per-mp** changes to a value which is less than the current active number of dynamic bypasses, then the limit changes to the new value and this limit is considered for the next new creations. Existing exceeding number dynamic bypasses do not delete.

When the **max-bypasses-per-mp** changes to a value which is more than system max-bypasses limit, then there is a warning message.

The **no** form of the command removes the maximum bypasses per MP limit and falls back to its default value, which is the max-bypasses value at the time of issuing this command.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures the maximum number of bypasses per merge point to 300.

```
device>configure
device(config)# router mpls
device(config-router-mpls)# dynamic-bypass
device(config-router-mpls-dynamic-bypass)# max-bypasses-per-mp 100
```

The following example configures MPLS Ethernet interface 0/8 to a maximum number of bypasses per merge point to 5.

```
device>configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/8
device(config-router-mpls-if-ethernet-0/8)# dynamic-bypass
device(config-router-mpls-if-ethernet-0/8-dynamic-bypass)# max-bypasses-per-mp 5
```

max-lsp-lifetime

Sets the maximum number of seconds an unrefreshed Link State PDU (LSP) remains in the LSP database of a device.

Syntax

max-lsp-lifetime *secs*

max-lsp-lifetime *secs*

Command Default

The default maximum lifetime is 1200 seconds (20 minutes).

Parameters

secs

Specifies the maximum lifetime in seconds. Valid values range from 1 through 65535 seconds. The default is 1200 seconds.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **max-lsp-lifetime** and **lsp-refresh-interval** commands must be configured in such a way that the LSPs are refreshed before the maximum LSP lifetime is reached. Otherwise, the device's originated LSPs may be timed out by neighbors of the device.

The **no** form of the command removes the configured period of time.

Examples

The following example changes the maximum LSP lifetime to 2400 seconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# max-lsp-lifetime 2400
```

max-mcache

Configures the maximum size of the multicast cache.

Syntax

max-mcache *num*

no max-mcache

Command Default

By default, the size of the multicast cache is 32768 entries for IPv4 and 4096 entries for IPv6.

Parameters

num

Specifies the number of entries in the multicast cache. Valid values range from 1 through 32768 for IPv4 and from 1 through 4096 for IPv6.

Modes

Router PIM configuration mode

Usage Guidelines

If the max-mcache is changed to a value that is less than the current max-mcache value, the existing cache routes are not automatically deleted. The cache routes are deleted when new routes are added.

The **no max-mcache** form of the command restores the default size of the maximum multicast cache.

Examples

The following example changes the multicast cache to 500 entries for IPv4.

```
device(config)# router pim
device(config-pim-router)# max-mcache 500
```

The following example changes the multicast cache to 500 entries for IPv6.

```
device(config)# ipv6 router pim
device(config-ipv6-router-pim-vrf-default-vrf)# max-mcache 500
```

max-metric router-lsa

Advertises the maximum metric value in different Link State Advertisements (LSAs).

Syntax

max-metric router-lsa [**all-vrfs**] [**all-lsas** | **external-lsa** *metric-value* | **link** { **all** | **ptp** | **stub** | **transit** } | **summary-lsa** *metric-value* | **on-startup** { *time* | **wait-for-bgp** [**all-lsas** | **summary-lsa** *metric-value* | **external-lsa** *metric-value* | **link** { **all** | **ptp** | **stub** | **transit** }] }]

no max-metric router-lsa [**all-vrfs**] [**all-lsas** | **external-lsa** | **link** { **all** | **ptp** | **stub** | **transit** } | **summary-lsa** | **on-startup** { *time* | **wait-for-bgp** [**all-lsas** | **link** [**all**]] }]

Parameters

all-vrfs

Applies the configuration change to all instances of OSPF.

all-lsas

Sets the **summary-lsa** and **external-lsa** optional parameters to the corresponding default max-metric value. For a non-default instance of OSPF, only the summary-lsa and external-lsa parameters are set.

external-lsa *metric-value*

Modifies the metric of all external type 5 LSAs to equal the specified value or a default value. The range for metric value is 1 to 16777214 (0x00001 - 0x00FFFFFE), and the default is 16711680 (0x00FF0000).

link

Specifies the types of links for which the maximum metric is advertised. By default, the maximum metric is advertised only for transit links.

all

Advertises the maximum metric in Router LSAs for all supported link types.

ptp

Advertises the maximum metric in Router LSAs for point-to-point links.

stub

Advertises the maximum metric in Router LSAs for stub links.

transit

Advertises the maximum metric in Router LSAs for transit links. This is the default link type.

summary-lsa *metric-value*

Modifies the metric of all summary type 3 and type 4 LSAs to equal the specified value or a default value. The range for metric value is 1 to 16777215 (0x00001 - 0x00FFFFFE), and the default is 16711680 (0x00FF0000).

on-startup

Applies the configuration change at the next OSPF startup.
time

Sets the time (in seconds) for which the specified links in Router LSAs are advertised when the metric is set to the maximum value of 0xFFFF. The range for *time* is 5 to 86,400.

wait-for-bgp

Indicates that OSPF should wait for either 600 seconds or until BGP has finished route table convergence, whichever happens first, before advertising the links with the normal metric.

Modes

OSPF router configuration mode

OSPF VRF router configuration mode

Usage Guidelines

Use this command to set the maximum metric value advertised in different Link State Advertisements (LSAs). When enabled, the router configures the maximum value of the metric for routes and links advertised in various types of LSAs. Because the route metric is set to its maximum value, neighbors will not route traffic through this router except to directly connected networks. Thus, the device becomes a stub router, which is desirable when you want:

- Graceful removal of the router from the network for maintenance.
- Graceful introduction of a new router into the network.
- To avoid forwarding traffic through a router that is in critical condition.

Enter **no max-metric router-lsa all-lsas** to disable advertising the maximum metric value in different LSAs.

Examples

The following example advertises the maximum metric value using the **all-lsas** option.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# max-metric router-lsa all-lsas
```

max-metric router-lsa (OSPFv3)

Advertises the maximum metric value in different Link State Advertisements (LSAs).

Syntax

max-metric router-lsa [**all-lsas** | **external-lsa** *metric-value* | **include-stub** | **on-startup** { *time* | **wait-for-bgp** } | **summary-lsa** *metric-value*]

no max-metric router-lsa [**all-lsas** | **external-lsa** | **include-stub** | **on-startup** { *time* | **wait-for-bgp** } | **summary-lsa**]

Parameters

all-lsas

Sets the **summary-lsa** and **external-lsa** optional parameters to the corresponding default max-metric value. For a non-default instance of OSPFv3, only the summary-lsa and external-lsa parameters are set.

external-lsa *metric-value*

Configures the maximum metric value for all external type-5 and type-7 LSAs. The range for metric value is 1 to 16777214 (0x00001 - 0x00FFFFFE), and the default is 16711680 (0x00FF0000).

include-stub

Specifies the advertisement of the maximum metric value for point-to-point and broadcast stub links in the intra-area-prefix LSA..

on-startup

Applies the configuration change at the next OSPF startup.
time

Sets the time (in seconds) for which the specified links in Router LSAs are advertised when the metric is set to the maximum value of 0xFFFF. The range for *time* is 5 to 86400.

wait-for-bgp

Specifies that OSPFv3 should wait until BGP has finished route table convergence before advertising the links with the normal metric, or for no more than 600 seconds.

summary-lsa *metric-value*

Configures the maximum metric value for all summary type 3 and type 4 LSAs. The range for metric value is 1 to 16777215 (0x00001 - 0x00FFFFFE), and the default is 16711680 (0x00FF0000).

Modes

OSPFv3 router configuration mode

OSPFv3 VRF router configuration mode

Usage Guidelines

Use this command to set the maximum metric value advertised in different Link State Advertisements (LSAs). When enabled, the router configures the maximum value of the metric for routes and links advertised in various types of LSAs. Because the route metric is set to its maximum value, neighbors will not route traffic through this router except to directly connected networks. Thus, the device becomes a stub router, which is desirable when you want:

- Graceful removal of the router from the network for maintenance.
- Graceful introduction of a new router into the network.
- To avoid forwarding traffic through a router that is in critical condition.

Enter **no max-metric router-lsa** to disable advertising the maximum metric value in different LSAs.

Examples

The following example configures an OSPFv3 device to advertise a maximum metric and sets the maximum metric value for all external type-5 and type-7 LSAs to 1000.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# max-metric router-lsa external-lsa 1000
```

The following example configures an OSPFv3 device to advertise a maximum metric and specifies the advertisement of the maximum metric value for point-to-point and broadcast stub links in the intra-area-prefix LSA.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# max-metric router-lsa include-stub
```

The following example configures an OSPFv3 device to advertise a maximum metric until BGP routing tables converge or until the default timer of 600 seconds expires.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# max-metric router-lsa on-startup wait-
for-bgp
```

The following example configures an OSPFv3 device to advertise a maximum metric and sets the maximum metric value for all summary type-3 and type-4 LSAs to 100.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# max-metric router-lsa summary-lsa 100
```

max-neighbor-reconnect-time

Specifies the maximum time that this router must wait for a graceful restart (GR) neighbor to restore the LDP session.

Syntax

max-neighbor-reconnect-time *seconds*

no max-neighbor-reconnect-time *seconds*

Command Default

120 seconds

Parameters

seconds

Specifies the maximum time in seconds that this router must wait for a GR neighbor to restore the LDP session. Enter a integer from 60 to 300. The default setting is 120.

Modes

MPLS LDP GR configuration mode

Usage Guidelines

The **no** form of the command resets the default time of 120 seconds.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example sets the LDP GR timer to 180 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# graceful-restart
device(config-router-mpls-ldp-gr)# max-neighbor-reconnect-time 180
```

max-neighbor-recovery-time

Specifies the maximum amount of time that this router waits for a graceful restart (GR) neighbor to complete its GR recovery after the LDP session has been reestablished.

Syntax

max-neighbor-recovery-time *seconds*

no max-neighbor-recovery-time *seconds*

Command Default

The default maximum time is120 seconds.

Parameters

seconds

Specifies the maximum amount of time in seconds that this router waits for a GR neighbor to complete its GR recovery after the LDP session has been reestablished. Enter a integer from 60 to 3600. The default setting is 120.

Modes

MPLS LDP GR configuration mode

Usage Guidelines

Recovery-time must be chosen accordingly taking into account the time it takes for RTM to recompute the routes and the number of Layer 3 FECs that need to be recovered as part of the LDP GR recovery. This is applicable to GR processing on ingress as well as transit LSRs.

The **no** form of the command resets the default time of 120 seconds.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example sets the LDP GR timer to 240 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# graceful-restart
device(config-router-mpls-ldp-gr)# max-neighbor-recovery-time 240
```

maxas-limit

Imposes a limit on the number of autonomous systems in the AS-PATH attribute.

Syntax

maxas-limit in *num*

no maxas-limit in

Command Default

Disabled.

Parameters

in

Allows an AS-PATH attribute from any neighbor to impose a limit on the number of autonomous systems.

num

Range is from 0 through 300. The default is 300.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

This example sets the limit on the number of BGP4 autonomous systems in the AS-PATH attribute to 100.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# maxas-limit in 100
```

maximum-paths (BGP)

Sets the maximum number of BGP4 and BGP4+ shared paths.

Syntax

maximum-paths *max-path-number* [**ebgp** *max-path-number*] [**ibgp** *max-path-number*] [**use-load-sharing**]

no maximum-paths

Command Default

Disabled.

Parameters

max-path-number

Specifies the maximum number of paths across which the device balances traffic to a given BGP destination. Valid values range is from 1 through 128. The default is 1.

ebgp *max-path-number*

Specifies the maximum number of paths across which the device balances traffic to a given eBGP destination. Valid values range is from 1 through 128. The default is 1.

ibgp *max-path-number*

Specifies the maximum number of paths across which the device balances traffic to a given iBGP destination. Valid values range is from 1 through 128. The default is 1.

use-load-sharing

Uses the maximum IP ECMP path value supported (128) without enabling BGP level ECMP.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use this command to change the maximum number of BGP4 shared paths, either by setting a value or using the maximum IP ECMP path value supported (128) without enabling BGP level ECMP.

If the configured *num* value is less than the possible number of ECMP paths available, BGP routes may not take the same number of ECMP paths. The set of ECMP paths may not be the same for different prefixes.

The no form of the command restores the default.

Examples

This example sets the maximum number of BGP4 shared paths to 128.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# maximum-paths 128
```

This example sets the maximum number of BGP4+ shared paths to 128 without enabling BGP level ECMP.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# maximum-paths use-load-sharing
```

This example sets the maximum number of BGP shared paths to 2 in a nondefault VRF instance in the IPv6 address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# maximum-paths 2
```

maximum-paths (IS-IS)

Specifies the number of paths Intermediate System-to-Intermediate System (IS-IS) can calculate and install in the IPv4 or IPv6 forwarding table.

Syntax

maximum-paths *number*

no maximum-paths *number*

Command Default

The default is 8 paths.

Parameters

value

Specifies the number of paths. Valid values range from 1 through 64 paths. The default is 8.

Modes

IS-IS address-family IPv4 unicast configuration mode

IS-IS address-family IPv6 unicast configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command resets number of paths to the default number of 8.

Examples

The following example specifies that the number of paths IS-IS can calculate and install in the IP forwarding table is 10.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# maximum-paths 10
```

The following example resets the number of paths IS-IS can calculate and install in the IPv6 forwarding table to 8 (the default).

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv6 unicast
device(config-router-isis-ipv6u)# no maximum-paths
```

maximum-paths (OSPF)

Changes the maximum number of OSPF shared paths.

Syntax

maximum-paths *num*

no maximum-paths

Parameters

num

Maximum number of paths across which the device balances traffic to a given OSPF destination. The range is from 1 through 64. The default is 8.

Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The no form of the command restores the default.

Examples

The following example sets the maximum number of shared paths to 22.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# maximum-paths 22
```

maximum-paths ebgp ibgp

Specifies the number of equal-cost multipath eBGP or iBGP routes or paths that are selected.

Syntax

maximum-paths { **ebgp** *num* | **ibgp** *num* }

no maximum-paths

Command Default

This option is disabled.

Parameters

ebgp

Specifies eBGP routes or paths.

ibgp

Specifies iBGP routes or paths.

num

The number of equal-cost multipath routes or paths that are selected. Range is from 1 through 64. 1 disables equal-cost multipath.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the no form of this command to restore the default.

Enhancements to BGP load sharing support the load sharing of BGP4 and BGP4+ routes in IP Equal-Cost Multipath (ECMP), even if the BGP multipath load-sharing feature is not enabled by means of the **use-load-sharing** option for the **maximum-paths** command. You can set separate values for IGMP and ECMP load sharing. Use this command to specify the number of equal-cost multipath eBGP or iBGP routes or paths that are selected.

Examples

This example sets the number of equal-cost multipath eBGP routes or paths that will be selected to 6 in the IPv4 address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# maximum-paths ebgp 6
```

This example sets the number of equal-cost multipath iBGP routes or paths that will be selected to 4 in the IPv6 address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# maximum-paths ibgp 4
```

This example sets the number of equal-cost multipath EBGP routes or paths that will be selected to 3 for the IPv4 address family for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# maximum-paths ebgp 3
```

measured-boot

Measured Boot is a mechanism to ensure that the integrity of the firmware and software running on a SLX hardware platform is maintained. This is ensured by the calculating a hash of the values of each stage in the boot process and comparing these values with the values stored on a remote verification server.

Syntax

measured-boot [*enable* | *disable*]

Modes

Global Configuration Mode

Parameters

enable

Enables the Measured Boot feature on this SLX device.

disable

Disables the Measured Boot feature on this SLX device.

Usage Guidelines

This configuration requires the SLX device to be rebooted.

Examples

The following is an example of enabling the Measured Boot feature on the SLX device.

```
SLX #configure terminal
SLX (config)# measured-boot enable
```

The following is an example of disabling Measured Boot feature on the SLX device.

```
SLX # configure terminal
SLX (config)# measured-boot disable
```

Platform Availability

This command and mode is only available on the Extreme 8720 and Extreme 8520 devices.

measurement-interval

Configures the SLM Measurement interval for Connectivity Fault Management (CFM).

Syntax

measurement-interval *interval*

no measurement-interval

Command Default

The default interval is fifteen minutes.

Parameters

interval

The interval period, in minutes. The range of valid values is from 1 through 1440.

Modes

CFM protocol configuration mode

Y.1731 configuration mode

Usage Guidelines

The **no measurement-interval** command resets the interval to the default value.

Examples

Example of setting the interval when configured for VLAN 30.

```
device# configure terminal
device(config-cfm)# domain name md1 level 4
device(config-cfm-md-md1)# ma-name ma1 id 1 vlan-id 30 pri 7
device(config-cfm-md-ma-ma1)# measurement interval 25
```

Example of configuring the interval for Y.1731 configuration mode.

```
device# configure terminal
device(config)# protocol cfm
device(protocol-cfm)# y1731
device(protocol-cfm-y1731)# test-profile my_test_profile
device(protocol-cfm-y1731-my_test_profile)# measurement-interval 20
device(protocol-cfm-y1731-my_test_profile)# exit
```

med-missing-as-worst

Configures the device to favor a route that has a Multi-Exit Discriminator (MED) over a route that does not have one.

Syntax

med-missing-as-worst

no med-missing-as-worst

Modes

BGP configuration mode

Usage Guidelines

When MEDs are compared, by default the device favors a low MED over a higher one. Because the device assigns a value of 0 to a route path MED if the MED value is missing, the default MED comparison results in the device favoring the route paths that do not have MEDs.

The **no** form of the command restores the default where a device does not favor a route that has a MED over other routes.

Examples

The following example configures the device to favor a route containing a MED.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# med-missing-as-worst
```

member (cluster)

Defines the bridge-domains and vlans shared between cluster nodes and extended on the ICL.

Syntax

member { **bridge-domain** | **vlan** }

Command Default

The cluster has no member bridge-domains or vlans

Parameters

bridge-domain

Configure the bridge-domain on the cluster
all

(Default) Adds all bridge-domains created on the node to the cluster.

add / remove <range>

Adds a specified range of bridge-domains to the cluster.

except

Adds all bridge-domains to the cluster, except the specified bridge-domain.

none

Removes all bridge-domains from the cluster.

vlan

Configure a vlan on the cluster
all

(Default) Adds all vlans created on the node to the cluster.

add / remove <range>

Adds a specified range of vlans to the cluster.

except

Adds all vlans to the cluster, except the specified vlan.

none

Removes all vlans from the cluster.

Modes

Cluster configuration mode

Usage Guidelines

The `all` parameter is the default configuration for both `member bridge-domain` and `member vlan`.

Examples

The following example configures cluster S1-A1 as a member of all vlans, and all bridge-domains except those listed (10, 11, 12).

```
device# config
Entering configuration mode terminal
device(config)# cluster S1-A1
device(config-cluster-S1-A1)# member vlan all
device(config-cluster-S1-A1)# member bridge-domain except 10,11,12
Snowball-MCT1(config-cluster-S1-A1)#
```

member-bridge-domain

Configures member bridge domains for a topology group.

Syntax

member-bridge-domain { **add** | **remove** } *bridge_domain_id*

Command Default

The topology group has no member bridge domains.

Parameters

add

Add a bridge domain to the topology group.

remove

Remove a bridge domain from the topology group.

bridge_domain_id

Bridge domain ID or the bridge domain range; for example: 1, 2, 4-7, 8, 9-22, 55-66. Tha maximun is 253 characters.

Modes

Topology group configuration mode.

Usage Guidelines

You must first add a master VLAN to the topology group.

Examples

The following example adds the member VLANs to the STP topology group.

```
device# configure terminal
device(config)# topology-group 10
device(config-topo-group-10)# master-vlan 15
device(config-topo-group-10)# member-bridge-domain add 5
```

member-vlan (STP)

Adds member VLANs to an STP topology group.

Syntax

member-vlan { **add** | **remove** } *vlan_id*

Command Default

The topology group has no member VLANs.

Parameters

add

Add a VLAN to the topology group.

remove

Remove a VLAN from the topology group.

vlan_id

Adds a member VLAN ID to the STP topology group. This can be a single VLAN or a range of VLANs. For example: 2, 4-7, 8, 9-22, 55-66. The maximum input is 253 characters.

Modes

Topology group configuration mode.

Usage Guidelines

The VLAN(s) must be configured before adding to the topology group.

You must first add a master VLAN to the topology group.

All the VLANs in the member group inherit the STP settings of the master VLAN in the group.

Examples

The following example adds the member VLANs to the STP topology group.

```
device# configure terminal
device(config)# topology-group 10
device(config-topo-group-10)# master-vlan 15
device(config-topo-group-10)# member-vlan add 5
```

mep

Adds local ports as Maintenance End Points (MEPs) to a specific Maintenance Association (MA).

Syntax

mep { *mep-id* [**up** | **down**] | [**vlan** *vlan-id*] | [**ethernet** *slot/ port*] | [**port-channel** *channel*]}

no mep *mep-id*

Command Default

There are no MEP configured.

Parameters

mep-id

Specifies the ID of the MEP.

up

Specifies MEP in the up direction.

down

Specifies MEP in the down direction.

ethernet

Specifies a physical Ethernet interface.

slot

Specifies a valid slot number. For devices that do not support linecards, specify **0**.

port

Specifies a valid port number.

inner-vlan *vlan-id*

Specifies the Inner VLAN.

port-channel *index*

Specifies a port-channel.

vlan *vlan-id*

Specifies a VLAN.

Modes

CFM protocol configuration mode

Usage Guidelines

The **no mep** command deletes the MEP from the MA.

A Maintenance Domain (MD) is part of a network controlled by one operator. The MD levels are carried on all CFM frames to identify different domains. Every MD can be divided into smaller networks having multiple MEPs. Usually an MA is associated with a service instances (for example a VLAN or a VPLS).

VPLS is supported on the Extreme 8720, Extreme 8520, SLX 9250, and SLX 9150 devices only.

MEP is located on the edge of an MA. It defines the endpoint of the MA. Each MEP has unique ID (MEPID) within MA. The connectivity in a MA is defined as connectivity between MEPs. The MEP generates Continuity Check Message and multicasts to all the other MEPs in the same MA to verify connectivity.

Each MEP has a direction, down or up. Down MEP receives CFM PDUs from the LAN and sends CFM PDUs towards the LAN. Up MEP receives CFM PDUs from a bridge relay entity and sends CFM PDUs towards the bridge relay entity on a bridge. End stations support down MEPs only because they have no bridge relay entities.

Examples

This example defines a MEP for VLAN 30 in the down direction.

```
device# configure terminal
device(config)# protocol cfm
device(config-cfm)# domain name md1 level 4
device(config-cfm-md-md1)# ma-name ma1 id 1 vlan-id 30 priority 3
device(config-cfm-md-ma-ma1)# mep 1 down ethernet 0/2
```

message-interval

Configures the frequency with which PIM Join and Prune messages are sent.

Syntax

message-interval *num*

no message-interval *num*

Command Default

The default frequency is every 60 seconds.

Parameters

num

The frequency in seconds. Valid values range from 10 through 65535 seconds.

Modes

Router PIM configuration mode

Usage Guidelines

The **no message-interval** form of the command restores the default frequency of 60 seconds.

Examples

This example configures a frequency of 1 hour for IPv4 PIM.

```
device(config)# router pim
device(config-pim-router)# message-interval 3600
```

This example configures a frequency of 1 hour for IPv6 PIM.

```
device(config)# ipv6 router pim
device(config-ipv6-router-pim-vrf-default-vrf)# message-interval 3600
```

message-interval

Specifies a value for an Ethernet Ring Protection (ERP) message interval.

Syntax

message-interval *time*

no message-interval

Command Default

The default message-interval value is 5000 milliseconds (ms).

Parameters

time

Time in ms. Range is from 100 through 5000, in multiples of 100.

Modes

ERP configuration mode

Usage Guidelines

Ring Automatic Protection Switching (R-APS) messages are sent continuously within an ERP ring.

Use the **no** form of this command to restore the default value.

Examples

The following example configures a message interval of 100 ms.

```
device# configure terminal
device(config)# erp 1
device(config-erp-1)# message-interval 100
```

metric

Assigns a metric to the LSP, which routing protocols can use to determine the relative preference among several LSPs towards a given destination.

Syntax

metric *number*

no metric *number*

Command Default

All LSPs have a metric of 1.

Parameters

number

Specifies the metric value. Enter an integer from 1 to 65535. A lower value is preferred over a higher value.

Modes

MPLS LSP configuration mode

Usage Guidelines

When multiple LSPs have the same destination LSR, and they have the same metric, the traffic load is shared among them.

Use the **no** form of the command to reset the default value.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures LSP to22 with a metric value of 20.

```
device(config)# router mpls
device(config-router-mpls)# lsp to22
device(config-router-mpls-lsp-to22)# no enable
device(config-router-mpls-lsp-to22)# to 10.1.1.2
device(config-router-mpls-lsp-to22)# from 10.1.1.1
device(config-router-mpls-lsp-to22)# metric 20
device(config-router-mpls-lsp-to22)# enable
device(config-router-mpls-lsp-to22)#exit
```

metric-style wide

Enables the wide metric type for new style of TLVs with Intermediate System-to-Intermediate System (IS-IS).

Syntax

metric-style wide [**level-1** | **level-2**]

no metric-style wide

Command Default

The wide metric type is not used.

Parameters

level-1

Specifies the IS-IS routing parameter as Level 1.

level-2

Specifies the IS-IS routing parameter as Level 2.

Modes

IS-IS address-family IPv4 unicast configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

When LDP-IGP synchronization is enabled, the wide metric type must be used.

The **no** form of the command disables the use of the wide metric type.

Examples

The following example enables the wide metric type for Level 1 packets for the IS-IS IPv4 unicast address family.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# metric-style wide level-1
```

metric-type

Configures the default metric type for external routes.

Syntax

metric-type { **type1** | **type2** }

no metric-type { **type1** | **type2** }

Command Default

Type 1

Parameters

type1

The metric of a neighbor is the cost between itself and the device plus the cost of using this device for routing to the rest of the world.

type2

The metric of a neighbor is the total cost from the redistributing device to the rest of the world.

Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The **no** form of the command restores the default setting. You must specify a type parameter when using the **no** form.

Examples

The following example sets the default metric type for external routes to type 2.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# metric-type type2
```

minimum-links

Configures the minimum bandwidth or number of links to be running to allow the port-channel to function.

Syntax

minimum-links *num-of-links*

no minimum-links

Command Default

The number of links is 1.

Parameters

num-of-links

Specifies the number of links. Device support for minimum links is as follows:

Device or series	Minimum-link range
SLX 9150, SLX 9250, Extreme 8520, and Extreme 8720	1–64
SLX 9540, SLX 9640, SLX 9740, and Extreme 8820	1–64

Modes

Port-channel interface configuration mode

Usage Guidelines

Use this command to allow a port-channel to operate at a certain minimum bandwidth all the time. If the bandwidth of the port-channel drops below that minimum number, then the port-channel is declared operationally DOWN even though it has operationally UP members.

Enter **no minimum-links** to restore the default value.

Examples

The following example sets the minimum number of links to 16 on a specific port-channel interface.

```
device# configure terminal
device(config)# interface port-channel 33
```

```
device(config-Port-channel-33)# minimum-links 16
```

mip-policy

Specifies the conditions in which Maintenance Intermediate Points (MIP) are automatically created on ports.

Syntax

mip-policy { **explicit** | **default** }

no mip-policy

Command Default

The MIP policy is set to **default**.

Parameters

explicit

Specifies that explicit MIPs are configured only if a MEP exists on a lower MD Level.

default

Specifies that MIPs are always configured.

Modes

CFM protocol configuration mode .

Usage Guidelines

Use the **no mip-policy** to reset the values to the default.

A Maintenance Intermediate Point (MIP) can be created on a port and VLAN automatically, but only when either the explicit or default policy has been defined for them. For a specific port and VLAN, a MIP is created at the lowest level. Additionally, the level created should be the next higher than the MEP level defined for the port and VLAN.

Use the **explicit** parameter to specify that explicit MIPs are configured only if a MEP exists on a lower Maintenance Domain (MD) level.

Use the **default** parameter to specify that MIPs are always configured.

Examples

Example of the MIP policy command set for explicit when configured for VLAN 30.

```
device# configure terminal
device(config-cfm)#domain name md1 level 4
device(config-cfm-md-md1)#ma-name ma1 id 1 vlan-id 30 pri 7
device(config-cfm-md-ma-ma1)#mip-policy explicit
```

mode (LLDP)

Sets the LLDP mode on the device.

Syntax

mode { **tx** | **rx** }

Command Default

Both transmit and receive modes are enabled.

Parameters

tx

Specifies to enable only the transmit mode.

rx

Specifies to enable only the receive mode.

Modes

Protocol LLDP configuration mode

Examples

To enable only the transmit mode:

```
device(conf-lldp)# mode tx
```

To enable only the receive mode:

```
device(conf-lldp)# mode rx
```

mode gre ip

Enables generic routing encapsulation (GRE) over a tunnel interface and specifies that the tunneling protocol is IPv4.

Syntax

mode gre ip

no mode

Command Default

GRE is disabled.

Modes

Interface tunnel configuration mode

Usage Guidelines

Use the **no mode gre ip** command to disable the GRE IP tunnel encapsulation method for the tunnel interface.

Examples

This example enables GRE IP encapsulation on a tunnel interface.

```
device# configure terminal
device(config)# interface tunnel 5
device(config-intf-tunnel-5)# mode gre ip
```

monitor session

Enables a port mirroring session, which sends copies of packets that enter or exit one port to another physical port or LAG interface, where the packets can be analyzed.

Syntax

monitor session *session_number*

source { **ethernet** *slot* **/** *port* | **port-channel** *index* | **ve** *index* }
destination { **ethernet** *slot* **/** *port* | **port-channel** *index* } **direction** *dir*

no monitor session *session_number*

Parameters

session_number

Specifies a session identification number. Valid values range from 1 through 512.

source

Specifies the interface for which you are defining a mirror.

ethernet

Specifies a physical Ethernet interface.

slot

Specifies a valid slot number. For devices that do not support linecards, specify 0.

port

Specifies a valid port number.

port-channel *index*

Specifies a valid port-channel interface number.

ve *index*

Specifies a valid virtual ethernet interface number.

destination

Specifies the physical-interface or port-channel mirror to use as the destination for mirroring.

ethernet

Specifies a physical Ethernet interface.

slot

Specifies a valid slot number. For devices that do not support linecards, specify 0.

port

Specifies a valid port number.

port-channel *index*

Specifies a port-channel interface.

direction *dir*

Specifies the direction of packets to mirror. Acceptable values are **both** (ingress and egress), **rx** (ingress only), or **tx** (egress only).

Modes

Global configuration mode

Usage Guidelines

All protocols such as LLDP must be disabled on interfaces that you select to be destination interfaces.

Run the **no monitor session** *session_number* command to delete the port mirroring session.

Examples

The following example enables session 22 for monitoring traffic from source Ethernet 0/1 to destination Ethernet 0/2 in the egress direction.

```
device# configure terminal
device(config)# monitor session 22
device(config-session-22)# source ethernet 0/1 destination ethernet 0/2 direction tx
```

The following example enables session 23 for monitoring traffic from source Ethernet 0/1 to destination Ethernet 0/2 in the ingress direction.

```
device# configure terminal
device(config)# monitor session 23
device(config-session-23)# source ethernet 0/1 destination ethernet 0/2 direction rx
```

The following example enables session 24 for monitoring traffic from source Ethernet 0/1 to destination Ethernet 0/2 in both directions.

```
device# configure terminal
device(config)# monitor session 24
device(config-session-24)# source ethernet 0/1 destination ethernet 0/2 direction both
```

The following example shows the configuration of mirroring from a Port Channel to a destination that is a Port Channel. Traffic from both directions is mirrored.

```
SLX# configure terminal
SLX (config)# monitor session 25
SLX (config-session-25)# source port-channel 1 destination port-channel 11 direction both
```

mpls reoptimize

Under ordinary conditions, an LSP path does not change unless the path becomes inoperable. Consequently, the router must be directed to consider configuration changes made to an LSP and to optimize the LSP path based on those changes.

Syntax

mpls reoptimize { **all** | **lsp** *lsp_name* }

Parameters

all

Reoptimizes all LSPs.

lsp*lsp_name*

Reoptimizes the specified LSP.

Modes

Privileged EXEC mode

Usage Guidelines

On re-optimization of an adaptive LSP, LSP accounting statistics might miss the accounting of some of the packets.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example uses the **mpls re-optimize** command to re-optimize LSP *to20*.

```
device# mpls reoptimize lsp to20
```

mpls-interface

Configures MPLS on an interface and accesses MPLS interface sub-configuration mode to configure its parameters.

Syntax

mpls-interface { **ethernet** *slot/port* | **port-channel** *number* | **ve** *number* }

no mpls-interface { **ethernet** *slot/port* | **port-channel** *number* | **ve** *number* }

Parameters

ethernet *slot/port*

Specifies an Ethernet slot and port.

port-channel *number*

Specifies a port-channel interface.

ve *number*

Specifies the VE interface number.

Modes

MPLS configuration mode

Usage Guidelines

Use the **no** form of this command to remove the MPLS interface.

You cannot configure MPLS on a VE interface associated with a protocol based VLAN. The command is rejected, and an error message is displayed.

After you enable MPLS globally on the device, you can enable it on one or more interfaces.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures MPLS on Ethernet interface 0/12.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/12
device(config-router-mpls-if-0/12)# ldp-params
device(config-router-mpls-if-0/12-ldp-params)# exit
device(config-router-mpls-if-ethernet-0/12)# rsvp
```

mtu (interface)

Configures the Layer 2 maximum transmission unit (MTU) size for all Ethernet interfaces and Port-channels.

Syntax

mtu *number*

no mtu

Command Default

The default is 1548 bytes.

Parameters

number

Size of the Layer 2 MTU in bytes. Range is from 1548 through 9216.

Modes

Global configuration mode

Interface configuration mode for an Ethernet or port-channel interface

Usage Guidelines

This command can be executed both globally and on an interface. If it is executed globally, interface configurations take precedence over the global configuration.

Use the **no** form of this command to revert to the default.

Examples

The following example configures the Layer 2 MTU size globally.

```
device# configure terminal
device(config)# mtu 2000
```

The following example configures the Layer 2 MTU size on an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/13
device(conf-if-eth-1/13)# mtu 2000
```

The following example configures the Layer 2 MTU size on a port-channel interface.

```
device# configure terminal
device(config)# interface port-channel 10
```

```
device(config-Port-channel-10)# mtu 2000
```

mtu (PW)

Configures the maximum transmission unit (MTU) for a pseudowire (PW) profile.

Syntax

mtu *mtu-value*

no mtu

Command Default

The MTU value is set to 1500.

Parameters

mtu-value

Specifies the maximum transmission unit (MTU) for the PW profile. Values range from 64 through 15966.

Modes

Pseudowire-profile configuration mode.

Usage Guidelines

The **no** form of the command restores the default configuration.

Examples

The following example shows how to set the MTU value to 2000 for a PW profile named test.

```
device# configure terminal
device(config)# pw-profile test
device(config-pw-profile-test)# mtu 2000
```

mtu-enforce

Configures MTU enforcement check for a pseudowire (PW) profile.

Syntax

mtu-enforce { *false* | *true* }

no mtu-enforce

Command Default

MTU enforcement is disabled.

Parameters

false

Disables the MTU enforcement check.

true

Enables the MTU enforcement check.

Modes

Pseudowire-profile configuration mode.

Usage Guidelines

MTU enforcement is only supported during PW signaling.

The **no** form of the command restores the default value.

Examples

The following example shows how to enable MTU enforcement check for a PW profile named test.

```
device# configure terminal
device(config)# pw-profile test
device(config-pw-profile-test)# mtu-enforce true
```

multipath

Changes load sharing to apply to only iBGP or eBGP paths, or to support load sharing among paths from different neighboring autonomous systems.

Syntax

multipath { **ebgp** | **ibgp** | **multi-as** }

no multipath { **ebgp** | **ibgp** | **multi-as** }

Command Default

This option is disabled.

Parameters

ebgp

Enables load sharing of eBGP paths only.

ibgp

Enables load sharing of iBGP paths only.

multi-as

Enables load sharing of paths from different neighboring autonomous systems.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the no form of this command to restore the default.

By default, when BGP load sharing is enabled, both iBGP and eBGP paths are eligible for load sharing, while paths from different neighboring autonomous systems are not.

Examples

This example changes load sharing to apply to iBGP paths in the IPv4 address family.

```
device# configure terminal
device(config)# router bgp
```

```
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# multipath ibgp
```

This example enables load sharing of paths from different neighboring autonomous systems in the IPv6 address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# multipath multi-as
```

This example changes load sharing to apply to eBGP paths in IPv4 VRF instance "red":

```
device# configure terminal
device(config)# rrouter bgp
device(config-bgp-router)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# multipath ebgp
```

multiplier (LLDP)

Sets the number of consecutive misses of hello messages before LLDP declares the neighbor as dead.

Syntax

multiplier *value*

no multiplier

Command Default

Multiplier default value is 4.

Parameters

value

Specifies a multiplier value to use. Valid values range from 2 through 10.

Modes

Protocol LLDP and profile configuration modes

Usage Guidelines

Enter **no multiplier** to return to the default setting.

The LLDP multipler can also be configured for a specific LLDP profile. When you apply an LLDP profile on an interface using the **lldp profile** command, it overrides the global configuration. If a profile is not present, then the default global profile is used until you create a valid profile.

Examples

To set the number of consecutive misses:

```
device(conf-lldp)# multiplier 2
```

To set the number of consecutive misses for a specific LLDP profile:

```
device(conf-lldp)# profile test1
device(config-profile-test1)# multiplier 5
device(config-profile-test1)#
```

multiplier (UDLD)

Sets timeout multiplier for missed UDLD PDUs.

Syntax

multiplier *value*

no multiplier

Command Default

Multiplier default value is 5.

Parameters

value

Specifies a multiplier value to use. Valid values range from 3 through 10.

Modes

Protocol UDLD configuration mode

Usage Guidelines

When the device at one end is an Extreme Networks IP product, the timeout interval is the product of the "hello" time interval at the other end and the "multiplier" value.

When the UDLD protocol times out waiting for UDLD PDUs, it will block the port.

Enter **no multiplier** to return to the default setting.

Examples

To set the multiplier to 8:

```
device# configure terminal
device(config)# protocol udld
device(config-udld)# multiplier 8
```

multi-topology

Enables IPv6 Intermediate System-to-Intermediate System (IS-IS) MT in an area or a domain so that the MT-enabled device runs IPv6 IS-IS in multi-SPF mode.

Syntax

multi-topology [**transition**]

no multi-topology [**transition**]

Command Default

The transition option is disabled.

Parameters

transition

Enables IPv6 IS-IS MT transition mode in an area or a domain so that a network operating in IPv6 IS-IS single-topology support mode can continue to work while upgrading devices to include IPv6 IS-IS MT support.

Modes

IS-IS address-family IPv6 unicast configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

When transition mode is not enabled, the routers operating in single-topology mode do not establish IPv6 connectivity with the routers operating in MT mode.

The **no multi-topology** form of the command disables IPv6 IS-IS MT.

The **no multi-topology transition** form of the command disables transition mode.

Examples

The following example enables IPv6 IS-IS MT.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv6 unicast
device(config-router-isis-ipv6u)# multi-topology
```

The following example enables IPv6 IS-IS MT with transition support.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv6 unicast
device(config-router-isis-ipv6u)# multi-topology transition
```

mvrp applicant-mode

Configures the MVRP applicant mode on the MVRP-enabled interface as normal-participant to enable the transmission of MVRP data units (MVRPDUs) or non-participant to disable the transmission of MVRPDUs; ensuring that no PDU exchange occurs on the port. The non-participant configuration is recommended on an MVRP-enabled edge port to avoid sending VLAN advertisements to the connected edge device.

Syntax

mvrp applicant-mode { **normal-participant** | **non-participant** }

no mvrp applicant-mode

Command Default

The default setting is normal-participant.

Parameters

normal-participant

Configures the port as a normal participant.

non-participant

Configures the port as a non participant.

Modes

Interface configuration mode

Usage Guidelines

This feature is supported on the SLX 9250, SLX 9540, SLX 9640, SLX 9740, Extreme 8520, and Extreme 8820 devices.

Use the **no** form of this command or the **normal-participant** keyword to reset the default setting of normal-participant.

Before configuring this command, you must configure the interface as switchport and enable MVRP globally on the device and on the interface to allow the MVRP-enabled interface to participate in the protocol.

Examples

The following example configures the edge port as non-participant.

```
device# configure terminal
device(config)# protocol mvrp
device(config-mvrp)# exit
device(config)# interface ethernet 0/15
```

```
device(conf-if-eth-0/15)# switchport
device(conf-if-eth-0/15)# mvrp enable
device(conf-if-eth-0/15)# mvrp applicant-mode non-participant
```

mvrp enable

Enables MVRP on an Ethernet or port-channel interface.

Syntax

mvrp enable

no mvrp enable

Command Default

MVRP is disabled by default on the interfaces.

Modes

Interface configuration mode

Usage Guidelines

This feature is supported on the SLX 9250, SLX 9540, SLX 9640, SLX 9740, Extreme 8720, Extreme 8820 devices.

Use the **no** form of this command to disable MVRP on the interface.

Before configuring this command, you must configure the interface as switchport and globally enable MVRP on the device to allow the MVRP-enabled interface to participate in the protocol.

Examples

The following example enables MVRP on an Ethernet interface.

```
device# configure terminal
device(config)# vlan 10
device(config-vlan-10)# exit
device(config)# protocol mvrp
device(config-mvrp)# exit
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# switchport
device(conf-if-eth-0/1)# switchport mode trunk
device(conf-if-eth-0/1)# switchport trunk allowed vlan add 10
device(conf-if-eth-0/1)# mvrp enable
```

The following example enables MVRP on a port-channel interface.

```
device# configure terminal
device(config)# protocol mvrp
device(config-mvrp)# exit
device(config)# interface ethernet 0/1,2
device(conf-if-eth-0/1,2)# channel-group 10 mode on
device(conf-if-eth-0/1,2)# no shutdown
device(conf-if-eth-0/1,2)# exit
device(config)# interface Port-channel 10
device(config-Port-channel-10)# switchport
```

```
device(config-Port-channel-10)# switchport mode trunk
device(config-Port-channel-10)# mvrp enable
device(config-Port-channel-10)# no shutdown
```

mvrp registration-mode forbidden vlan

Configures the forbidden registration mode for a VLAN or a range of VLANs on an MVRP-enabled Ethernet or port-channel interface.

Syntax

mvrp registration-mode forbidden vlan { **add** | **remove** } *vlanID*

Command Default

By default, the registration mode for an MVRP-enabled interface is set to Normal. For a static VLAN configuration, the registration mode is automatically set to Fixed. To prune the advertisement propagation and deregistration of a dynamic VLAN on an MVRP-enabled interface port, you can register the VLAN as Forbidden.

Parameters

add

Adds the specified VLAN to the forbidden VLAN list on the interface.

remove

Removes the specified VLAN from the forbidden list on the interface and allows advertising of non-forbidden VLANs through the MVRP messages on the interface.

vlanID

Specifies an individual VLAN or a range of VLANs. For example, to add VLANs 25 through 30 to the forbidden list, enter **mvrp registration-mode forbidden vlan add 25-30** .

Modes

Interface configuration mode

Usage Guidelines

This feature is supported on the SLX 9250, SLX 9540, SLX 9640, SLX 9740, Extreme 8720, and Extreme 8820 devices.

The **add** keyword prevents the VLANs specified in the command from being advertised on all other MVRP-enabled ports and also removes the specified VLANs that are dynamically registered from this interface.

Before you configure this command, you must configure the interface as switchport and must enable MVRP both globally and on the interface.

You cannot configure a static VLAN as forbidden.

Examples

The following example adds VLANs 25 through 30 to the forbidden list, and removes VLAN 26 from the forbidden list.

```
device# configure terminal
device(config)# protocol mvrp
device(config-mvrp)# exit
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# switchport
device(conf-if-eth-1/1)# mvrp enable
device(conf-if-eth-1/1)# switchport mode trunk
device(conf-if-eth-1/1)# switchport trunk allowed vlan add 20-24
device(conf-if-eth-1/1)# mvrp registration-mode forbidden vlan add 25-30
device(conf-if-eth-1/1)# mvrp registration-mode forbidden vlan remove 26
```

mvrp timer

Sets the MVRP join, leave, and leave-all timer values on an Ethernet or port-channel interface.

Syntax

mvrp timer join *cs* **leave** *cs* **leave-all** *cs*

no mvrp timer join *cs* **leave** *cs* **leave-all** *cs*

Command Default

The join timer default value is 20 centiseconds (cs).

The leave timer default value is 100 cs.

The leave-all timer default value is 1000 cs.

Parameters

join *cs*

Specifies the join timer in centiseconds. Enter an integer from 20 to 10000000.

leave *cs*

Specifies the leave timer in centiseconds. Enter an integer from 100 to 10000000. The leave timer setting must be greater than or equal to twice the join timer setting plus 30 centiseconds.

leave-all *cs*

Specifies the leave-all timer in centiseconds. Enter an integer from 1000 to 10000000. The leave-all timer setting must be a minimum of three times the value of the leave timer setting.

Modes

Interface configuration mode

Usage Guidelines

MVRP is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of this command resets the timers to the global timer configuration. If the global timers have not been configured, the timers are reset to the default values.

Before configuring this command, you must configure the interface as switchport and globally enable MVRP on the device and on the interface to allow the MVRP-enabled interface to participate in the protocol.

This command requires that you configure the timer values in the specified order and you must configure all values.

When the network radius is large or the expected system load is higher normally, and since the default timer values are aggressive, Extreme recommends that you change the timer values to higher numbers to reduce the MVRP message exchanges and load on the system.

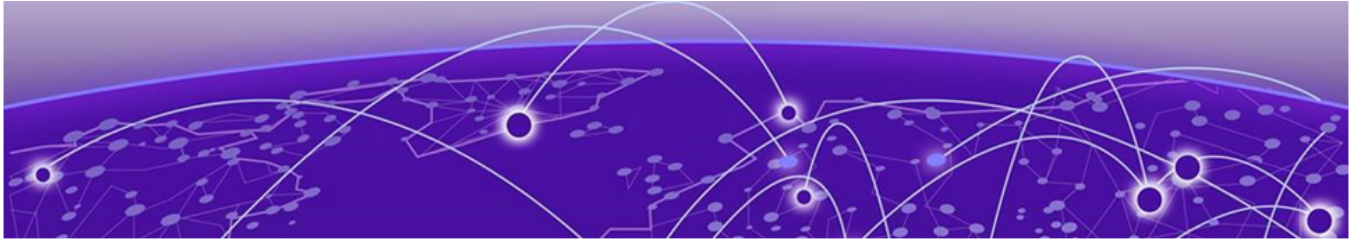
The configured timer settings on the individual MVRP-enabled interfaces override the global timer configuration.

The join timer is not run periodically but is triggered by the MVRP events and the device state changes. However, the leave-all timer is periodic required for garbage collection purposes.

Examples

The following example configures the MVRP timers on an Ethernet interface.

```
device# configure terminal
device(config)# protocol mvrp
device(config-mvrp)# exit
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# switchport
device(conf-if-eth-1/1)# mvrp enable
device(conf-if-eth-1/1)# switchport mode trunk
device(conf-if-eth-1/1)# switchport trunk allowed vlan add 20-24
device(conf-if-eth-1/1)# mvrp timer join 40 leave 200 leave-all 2000
device(conf-if-eth-1/1)#
```



Commands N - Q

name (ERP) on page 1195
name-prefix on page 1196
nbr-timeout on page 1198
neighbor activate on page 1199
neighbor accept-lldp-neighbors on page 1201
neighbor additional-paths on page 1202
neighbor additional-paths advertise on page 1204
neighbor additional-paths disable on page 1206
neighbor advertisement-interval on page 1208
neighbor allowas-in on page 1210
neighbor alternate-as on page 1212
neighbor announce-rpki-state on page 1214
neighbor as-override on page 1216
neighbor bfd on page 1218
neighbor capability as4 on page 1220
neighbor capability orf prefixlist on page 1222
neighbor default-originate on page 1224
neighbor description on page 1226
neighbor ebgp-btsh on page 1228
neighbor ebgp-multihop on page 1230
neighbor enable-peer-as-check on page 1231
neighbor encapsulation on page 1233
neighbor enforce-first-as on page 1234
neighbor filter-list on page 1236
neighbor flowspec redirect on page 1238
neighbor flowspec validation on page 1240
neighbor graceful-restart on page 1242
neighbor graceful-shutdown on page 1244
neighbor local-as on page 1247
neighbor maxas-limit in on page 1249
neighbor maximum-prefix on page 1251
neighbor next-hop-self on page 1254
neighbor next-hop-unchanged on page 1256
neighbor password on page 1258

neighbor peer-dampening on page 1260
neighbor peer-dampening (peer-group) on page 1262
neighbor peer-group on page 1264
neighbor peer-group-name alternate-as-range on page 1266
neighbor prefix-list on page 1267
neighbor remote-as on page 1269
neighbor remove-private-as on page 1271
neighbor route-map on page 1273
neighbor route-reflector-client on page 1275
neighbor rpki validation status disable on page 1277
neighbor send-community on page 1278
neighbor shutdown on page 1280
neighbor soft-reconfiguration inbound on page 1282
neighbor static-network-edge on page 1284
neighbor timers on page 1285
neighbor unsuppress-map on page 1287
neighbor update-source on page 1289
neighbor weight on page 1291
net on page 1293
network on page 1294
next-hop-enable-default on page 1296
next-hop-mpls on page 1297
next-hop-recursion on page 1299
next-hop-recursion (Policy Based Routing) on page 1300
no debug on page 1302
no-core-isolation on page 1304
node on page 1305
non-revertive-mode on page 1306
nonstop-routing (IS-IS) on page 1307
nonstop-routing (OSPF) on page 1308
notification-timer on page 1309
ntp authenticate on page 1310
ntp authentication-key on page 1311
ntp disable on page 1313
ntp peer on page 1314
ntp server on page 1316
ntp trusted-key on page 1318
operational-state on page 1319
optimized replication on page 1320
oscmd on page 1321
overlay access-group on page 1323
overlay access-list type vxlan extended on page 1324

overlay access-list type vxlan standard on page 1325
overlay-gateway on page 1326
overlay-service-policy on page 1328
overlay-transit on page 1330
partial-spf-interval on page 1331
password on page 1333
password-attributes on page 1335
password-attributes expiry-alert-level on page 1339
password-encryption convert-enc-to-level-10 on page 1342
password-policy (TPVM mode) on page 1343
path on page 1345
pdu-rate on page 1347
peer on page 1348
peer (MCT) on page 1351
peer-dampening on page 1352
peer-group ipv6prefix-over-ipv4peer on page 1354
peer-interface on page 1355
peer-keepalive (optional) on page 1356
penalty on page 1358
permit ip host on page 1359
ping on page 1361
pki ocsp on page 1364
police cir on page 1366
policy-map on page 1368
port-channel path-cost on page 1370
preempt-mode on page 1372
prefix-independent-convergence on page 1373
prefix-independent-convergence-static on page 1374
primary-path on page 1375
priority on page 1377
priority-group-table on page 1378
priority-table on page 1380
process-restart on page 1382
profile (LLDP) on page 1385
profile (telemetry) on page 1387
profile counters on page 1389
profile etcam on page 1391
profile lag on page 1393
profile qos on page 1395
profile route on page 1397
profile tcam on page 1400
profile tcam cam-share on page 1402

protocol on page 1404
protocol cfm on page 1405
protocol link-oam on page 1406
protocol lldp on page 1407
protocol loop-detection on page 1408
protocol mvrp on page 1409
protocol spanning-tree on page 1410
protocol udld on page 1412
protocol vrrp on page 1413
protocol vrrp-extended on page 1414
prune-wait on page 1415
pw-profile on page 1416
pw-profile (bridge domain) on page 1418
python on page 1419
qos cos on page 1422
qos cos-mutation on page 1423
qos cos-mutation on page 1424
qos cos-traffic-class on page 1426
qos cpu slot on page 1427
qos dscp-cos on page 1429
qos dscp-mutation on page 1430
qos dscp-traffic-class on page 1431
qos-dscp-mode on page 1432
qos flowcontrol on page 1433
qos map cos-mutation on page 1435
qos map cos-mutation on page 1437
qos map cos-traffic-class on page 1438
qos map dscp-cos on page 1440
qos map dscp-mutation on page 1442
qos map dscp-traffic-class on page 1444
qos map traffic-class-cos on page 1446
qos port-speed-up on page 1448
qos random-detect traffic-class on page 1449
qos red-profile on page 1450
qos remark dscp on page 1452
qos rx-queue cos-threshold on page 1453
qos rx-queue multicast on page 1454
qos rx-queue unicast traffic-class on page 1456
qos service-policy on page 1457
qos traffic-class on page 1458
qos traffic-class-cos on page 1459
qos trust dscp on page 1461

qos-mpls map dscp-exp on page 1462
qos-mpls map exp-dscp on page 1464
qos-mpls map exp-traffic-class on page 1465
qos-mpls map-apply dscp-exp on page 1467
qos-mpls map-apply exp-dscp on page 1468
qos-mpls map-apply exp-traffic-class on page 1469
qos-ttl-mode on page 1470
qos tx-queue scheduler strict-priority on page 1472

name (ERP)

Specifies an optional name for an Ethernet Ring Protection (ERP) instance.

Syntax

name *string*

no name *string*

Command Default

No ERP instance name is configured by default.

Parameters

string

An ASCII string. Range is from 1 through 32 characters. Underscores and dashes are allowed.

Modes

ERP configuration mode

Usage Guidelines

Use the **no** form of this command to remove the ERP instance name.

Examples

The following example specifies the name of an ERP instance.

```
device# configure terminal
device(config)# erp 1
device(config-erp-1)# name mainRing
```

name-prefix

Use the **name-prefix** interface command to specify a name prefix for the dynamic bypass LSPs to be created for the MPLS protected interface.

Syntax

name-prefix *name*

no name-prefix *name*

Command Default

The default name prefix is *dbyp*.

Parameters

name

Specifies the selected character string. The length of the character string is between 1 and 21 characters.

Modes

MPLS router MPLS interface dynamic bypass configuration mode (config-router-mpls-if-ethernet-*slot/port* -dynamic-bypass).

Usage Guidelines

The **no** form of the command removes the name prefix and sets its value to the default string *dbyp*.

When configuring, the dynamic bypass LSPs names must start with this name prefix, appended by interface IP, Merge Point IP (for node protection), and a unique number.

The name prefix configuration is only allowed when there no existing dynamic bypasses corresponding to a dynamic bypass interface. When the user wants to change the name prefix, the user must disable the dynamic bypass on the interface and reconfigure the name prefix, then re-enable the dynamic bypass on the interface.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures the name prefix for MPLS Ethernet interface *0/8* to *MyDbypass*.

```
device>configure
device(config)# router mpls
```

```
device(config-router-mpls)# mpls-interface ethernet 0/8
device(config-rouoter-mpls-if-ethernet-0/8)# dynamic-bypass
device(config-router-mpls-if-ethernet-0/8-dynamic-bypass)# name-prefix MyDbypass
```

nbr-timeout

Configures the length of time a PIM device waits for hello messages before considering a neighbor to be absent.

Syntax

nbr-timeout *num*

no nbr-timeout

Command Default

The default interval is 105 seconds.

Parameters

num

Specifies the timeout value in seconds. Valid values range from 35 through 12600 seconds.

Modes

Router PIM configuration mode

Usage Guidelines

The absence of PIM hello messages from a neighboring device indicates that the neighbor is absent. The interval should not be less than 3.5 times the hello timer value.

The **no nbr-timeout** form of the command reverts the timeout to the default of 105 seconds.

Examples

This example configures a timeout of 600 seconds for IPv4 PIM.

```
device(config)# router pim
device(config-pim-router)# nbr-timeout 600
```

This example configures a timeout of 600 seconds for IPv6 PIM.

```
device(config)# ipv6 router pim
device(config-ipv6-router-pim-vrf-default-vrf)# nbr-timeout 600
```

neighbor activate

Enables the exchange of information with BGP neighbors and peer groups.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **activate**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **activate**

Command Default

Address exchange for IPv4 address family is enabled by default. Address exchange for IPv6 address family must be enabled explicitly.

Parameters

ip-address

Specifies the IPv4 address of the neighbor.

ipv6-address

Specifies the IPv6 address of the neighbor.

peer-group-name

Specifies a peer group.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

BGP address-family L2VPN EVPN configuration mode

Usage Guidelines

The **no** form of the command disables the exchange of an address with a BGP neighbor or peer group.

Examples

The following example establishes a BGP session with a neighbor with the IPv6 address 2001:2018:8192::125.

```
device# configure terminal
device(config)# router bgp
```

```
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 activate
```

The following example establishes a BGP session with a neighbor with the IP address 10.1.1.1 in L2VPN EVPN configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# neighbor 10.1.1.1 activate
```

The following example establishes a BGP session with a neighbor with the IP address 20.0.0.1 and activates IPv6 address family for this neighbor.

```
SLX(config)# router bgp
SLX(config-bgp-router)# neighbor 20.0.0.1 remote-as 200
SLX(config-bgp-router)# address-family ipv6 unicast
SLX(config-bgp-ipv6u)# neighbor 20.0.0.1 activate
```

neighbor accept-lldp-neighbors

Enables automatic neighbor discovery for Border Gateway Protocol (BGP).

Syntax

neighbor *peer-group-name* **accept-lldp-neighbors**

no neighbor *peer-group-name* **accept-lldp-neighbors**

Command Default

By default, automatic neighbor discovery for BGP is disabled.

Parameters

peer-group-name

Specifies the name of a peer group: the properties of this peer group will be applied to BGP neighbors that are automatically discovered by Link Layer Discovery Protocol (LLDP).

Modes

BGP configuration mode

Usage Guidelines

Currently, automatic neighbor discovery is supported for only one peer group identifier.

The **no** form of the command disables the configuration.

Note
The configuration remains enabled when at least one peer group configured with **accept-lldp-neighbors** is present.

Examples

The following example enables automatic neighbor discovery for BGP and applies the properties of a peer group named *lldp-grp* to new automatically-discovered neighbors.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor lldp-grp accept-lldp-neighbors
```

The following example disables automatic neighbor discovery for a peer group named *lldp-grp*.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# no neighbor lldp-grp accept-lldp-neighbors
```

neighbor additional-paths

Enables an additional-paths capability for a specific peer or peer group in a Border Gateway Protocol (BGP) address family.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths** { **receive** [**send**] | **send** }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths receive**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths send**

Command Default

Specific peer devices or peer groups configured under a BGP address family are not capable of receiving or sending additional-paths.

Parameters

ip-address

Address of the neighbor in IPv4 address format.

ipv6-address

Address of the neighbor in IPv6 address format.

peer-group-name

Peer group name of the neighbor.

additional-paths

Enables an additional-paths capability.

receive

Enables the capability to receive additional-paths.

send

Enables the capability to send additional-paths.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Note
An additional-paths capability configured at peer level takes precedence over any additional-paths capability configured at either the peer group or BGP address family level.

Peers exchange and negotiate additional-paths capability during session establishment.

An additional-paths capability can be enabled for a specific peer or peer group as receive only, send only, or both send and receive.

The **no** form of the command disables the additional-paths capability for a specific peer device or peer group.

To remove the configuration when both the **receive** and **send** options have been set, you should enter both the **no neighbor additional-paths** command, specifying the **receive** option to disable the capability to receive additional-paths, and the **no neighbor additional-paths** command, specifying the **send** option to disable the capability to send additional-paths.

Examples

The following example shows how to enable a peer device (10.1.2.3) configured under the IPv4 unicast address family to both receive and send additional-paths.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.1.2.3 additional-paths receive send
```

The following example shows how to disable the capability to receive additional-paths for a specific peer device (10.1.2.3) in the IPv4 unicast address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# no neighbor 10.1.2.3 additional-paths receive
```

The following example shows how to enable a peer device (10.1.2.3) configured under the IPv6 unicast address family to both receive and send additional-paths.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 10.1.2.3 additional-paths receive send
```

neighbor additional-paths advertise

Configures the additional-paths to advertise to a neighbor for a Border Gateway Protocol (BGP) address family.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths advertise** { **all** [**best** *num*] [**group-best**] | **best** *num* | **group-best** }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths advertise all**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths advertise best** *num*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths advertise group-best**

Parameters

ip-address

Address of the neighbor in IPv4 address format.

ipv6-address

Address of the neighbor in IPv6 address format.

peer-group-name

Peer group name of the neighbor.

all

Causes all routes to be advertised as additional-paths to the specified neighbor or peer group. A maximum of 16 routes is allowed.

best *num*

Specifies the number of best paths allowed for advertisement as additional-paths to the specified neighbor or peer group. The number ranges from 2 through 16.

group-best

Causes group-best paths to be advertised as additional-paths to the specified neighbor or peer group. Only routes with a rank less than or equal to 16 are allowed. A route with a rank greater than 16 (even when it is the group best path), is not eligible for selection as an additional path advertised to a neighbor or peer group.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Note
The set of paths configured by using the **neighbor additional-paths advertise** command must be a subset of selected paths; that is, paths previously configured by using the **additional-paths select** command under the particular BGP address-family configuration mode.

The **additional-paths advertise** command options (**all** , **best** , and **group-best**) are not mutually exclusive. When you configure a combination of these options, the combined configuration is applied to the BGP address family.

The **no** form of the command removes the specified configuration. When more than one option is configured, it is recommended that you disable each configured option separately; for example, by using the **no neighbor additional-paths advertise** command specifying the **all** option to disable the **all** configuration, and so on.

Examples

The following example shows how to configure the advertisement of all (a maximum of 16 is allowed) routes for a peer device, 10.123.123.1, under the IPv4 unicast address family.

```
device# configure terminal
device(condig)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-router-ipv4u)# neighbor 10.123.123.1 additional-paths advertise all
```

The following example shows how to restore the default configuration when all options (**all** , **best** , and **group-best**) were previously configured under the IPv4 unicast address family.

```
device# configure terminal
device(condig)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-router-ipv4u)# no neighbor 10.123.123.1 additional-paths advertise all
device(config-bgp-router-ipv4u)# no neighbor 10.123.123.1 additional-paths advertise best
2
device(config-bgp-router-ipv4u)# no neighbor 10.123.123.1 additional-paths advertise
group-best
```

The following example shows how to configure the advertisement of all (a maximum of 16 routes is allowed) routes for a peer device, 10.123.123.1, under the IPv6 unicast address family.

```
 device# configure terminal
device(condig)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-router-ipv6u)# neighbor 10.123.123.1 additional-paths advertise all
```

neighbor additional-paths disable

Disables the inheritance of an additional-paths capability (from the address family or peer group level) for a specific peer or peer group in a Border Gateway Protocol (BGP) address family.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths disable**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **additional-paths disable**

Command Default

By default, an additional-paths capability configured for a specific BGP address family applies to all peer groups and peers configured under the address family, and an additional-paths capability configured for a peer group applies to all peers within the group.

Parameters

ip-address

Address of the neighbor in IPv4 address format.

ipv6-address

Address of the neighbor in IPv6 address format.

peer-group-name

Peer group name of the neighbor.

Modes

BGP configuration mode

Usage Guidelines

When the capability to send and receive additional-paths is configured at the address family or peer group level, the capability applies to all neighbors configured under the address family or within the peer group: you can use the **neighbor additional-paths disable** command to disable this capability inheritance for an individual peer or peer-group.

The **no** form of the command restores the default configuration.

Examples

The following example shows how to disable additional-paths capability inheritance (from the address-family configuration) for an IPv4 address-family peer (10.123.123.1).

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast
device(config-bgp)# neighbor 10.123.123.1 additional-paths disable
```

The following example shows how to restore additional-paths capability inheritance (from the address-family configuration) for an IPv4 peer (10.123.123.1).

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast
device(config-bgp)# no neighbor 10.123.123.1 additional-paths disable
```

The following example shows how to disable additional-paths capability inheritance (from the address- family configuration) for an IPv6 address-family peer with IP address 10.123.123.1.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 10.123.123.1 additional-paths disable
```

neighbor advertisement-interval

Enables changes to the interval over which a specified neighbor or peer group holds route updates before forwarding them.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **advertisement-interval** *seconds*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **advertisement-interval**

Parameters

ip-address

IPv4 address of the neighbor.

ipv6-address

IPv6 address of the neighbor.

peer-group-name

Peer group name configured by the **neighbor** *peer-group-name* command.

seconds

Range is from 0 through 3600. The default is 0.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command restores the default interval.

Examples

The following example changes the BGP4 advertisement interval from the default to 60 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 advertisement-interval 60
```

The following example changes the BGP4+ advertisement interval from the default for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 advertisement-interval 60
```

neighbor allowas-in

Disables the AS_PATH check function for routes learned from a specified neighbor so that BGP does not reject routes that contain the recipient BGP speaker's AS number.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **allowas-in** *number*

no neighbor allowas-in { *ip-address* | *ipv6-address* | *peer-group-name* } **allowas-in**

Command Default

The AS_PATH check function is enabled and any route whose path contains the speaker's AS number is rejected as a loop.

Parameters

ip-address

Specifies the IP address of the neighbor.

ipv6-address

Specifies the IPv6 address of the neighbor.

peer-group-name

Specifies a peer group.

number

Specifies the number of times that the AS path of a received route may contain the recipient BGP speaker's AS number and still be accepted. Valid values are 1 through 10.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

BGP address-family L2VPN EVPN configuration mode

Usage Guidelines

If the AS_PATH check function is disabled after a BGP session has been established, the neighbor session must be cleared for this change to take effect.

The **no** form of the command re-enables the AS_PATH check function.

Examples

The following example specifies that the AS path of a received route may contain the recipient BGP4+ speaker's AS number three times and still be accepted.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 allowas-in 3
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

The following example specifies for VRF instance "red" that the BGP4+ AS path of a received route may contain the recipient BGP speaker's AS number three times and still be accepted.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::124 allowas-in 3
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

The following example specifies that the AS path of a received route may contain the recipient BGP speaker's AS number three times and still be accepted in L2VPN EVPN configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# neighbor 10.1.1.1 allowas-in 3
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

The following example specifies that the AS path of a received IPv6 route from the neighbor 20.0.0.1 may contain the recipient BGP4+ speaker's AS number up to three (3) times and can still be accepted.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 20.0.0.1 allowas-in 3
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

neighbor alternate-as

Adds a range of alternate autonomous system numbers (ASNs) for BGP dynamic neighbors.

Syntax

neighbor *peer-group-name* **alternate-as** { **add** | **remove** } *as-range*

no neighbor *peer-group-name* **alternate-as add**

Command Default

Disabled.

Parameters

add

Adds an AS to the alternate AS range.

remove

Removes an AS from the alternate AS range.

as-range

Specifies an alternate AS value. Enter an integer from 1 through 4294967295.

Modes

BGP configuration mode

Usage Guidelines

This command is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

This command supports only IPv4 BGP.

The **no** form of the command removes configured alternate AS values.

For dynamic neighbors, the remote AS in the peer-group configuration allows the configuration of an alternate AS range, a range under which the EBGP peer can fall under for the listen range that includes the peer group.

When the device receives an OPEN message from a peer, it checks whether this AS number falls under the range configured for the peer group. Then it accepts and makes the session IBGP or BGP peer.

Examples

The following example sets an alternate AS of 100 for listen range neighbors in a peer group called “mypeergroup”.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor mypeergroup remote-as 400
device(config-bgp-router)# neighbor mypeergroup alternate-as add 100
```

The following example sets an alternate AS range of 200 through 300 for listen range neighbors in a peer group called “mypeergroup”.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor mypeergroup remote-as 400
device(config-bgp-router)# neighbor mypeergroup alternate-as add 200-300
```

The following example removes the configured alternate AS number 100 for listen range neighbors in a peer group called “mypeergroup”.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor mypeergroup alternate-as remove 100
```

neighbor announce-rpki-state

This command enables the SLX device to announce the RPKI state to its iBGP neighbors also to receive the RPKI state with prefixes from the configured neighbor. The state is announced to the iBGP neighbor through the extended community attribute. RPKI state is only announced to the iBGP neighbor when **neighbor send-community** is enabled using the *extended*, *all*, or *both* settings for the command.

Syntax

neighbor *<neighbor-address>* **announce-rpki-state**

[no] neighbor *<neighbor-address>* **announce-rpki-state**

Parameters

<neighbor-address>

IPv4 or IPv6 address of the iBGP neighbor based on address family mode.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

By default, RPKI states with prefixes are not shared with the iBGP neighbors. Even if the iBGP neighbor share prefixes with RPKI states, it is not considered. Sharing of RPKI states with iBGP neighbors must be explicitly enabled.

RPKI state will be announced to the iBGP neighbor only when **neighbor send-community** is enabled using the *extended*, *all*, or *both* settings for the command. If this command is not enabled in the appropriate context, a warning message to enable **neighbor send-community** with *extended* parameter.

The [no] format of this command stops the device from sending and receiving the RPKI state with prefixes to iBGP neighbors.

The default state is RPKI state with prefixes are not shared with iBGP neighbors.

Examples

The following example shows the steps to enable sharing of RPKI state and prefix with iBGP neighbor with IPv4 address of 10.10.11.1.

This command enters in to the *router bgp* mode and then enters into the IPv4 unicast address family configuration mode.

```
SLX(config)#router bgp
SLX(config-bgp-router)# address-family IPv4 unicast
```

This command enables the ability to send extended community information to iBGP peers.

```
SLX(config-bgp-ipv4u)# neighbor 10.10.11.1 send-community extended
SLX(config-bgp-ipv4u)#
```

This command enables announcing and receiving RPKI states and prefixes with the configured iBGP peer.

```
SLX(config-bgp-ipv4u)# neighbor 10.10.11.1 announce-rpki-state
```

neighbor as-override

Replaces the autonomous system number (ASN) of the originating device with the ASN of the sending BGP device.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **as-override**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **as-override**

Command Default

This feature is disabled.

Parameters

ip-address

IPv4 address of the neighbor.

ipv6-address

IPv6 address of the neighbor.

peer-group-name

Peer group name configured by the **neighbor** *peer-group-name* command.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to disable this feature.

BGP loop prevention verifies the ASN in the AS path. If the receiving router sees its own ASN in the AS path of the received BGP packet, the packet is dropped. The receiving router assumes that the packet originated from its own AS and has reached the place of origination. This can be a significant problem if the same ASN is used among various sites, preventing sites with identical ASNs from being linked by another ASN. In this case, routing updates are dropped when another site receives them.

Examples

This example replaces the ASN globally.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 as-override
```

This example replaces the BGP4+ ASN for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 as-override
```

neighbor bfd

Enables Bidirectional Forwarding Detection (BFD) sessions for specified Border Gateway Protocol (BGP) neighbors or peer groups.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **bfd** [**holdover-interval** *time* | **interval** *transmit-time* **min-rx** *receive-time* **multiplier** *number*]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **bfd** [**holdover-interval** *time* | **interval** *transmit-time* **min-rx** *receive-time* **multiplier** *number*]

Command Default

BFD sessions are not enabled on specific BGP neighbors or peer groups.

Parameters

ip-address

Specifies the IP address of the neighbor.

ipv6-address

Specifies the IPv6 address of the neighbor.

peer-group-name

Specifies a peer group.

holdover-interval *time*

Specifies the holdover interval, in seconds, for which BFD session down notifications are delayed before notification that a BFD session is down. Valid values range from 1 through 30.

interval *transmit-time*

Specifies the interval, in milliseconds, a device waits to send a control packet to BFD peers. Valid values range from 50 through 30000.

min-rx *receive-time*

Specifies the interval, in milliseconds, a device waits to receive a control packet from BFD peers. Valid values range from 50 through 30000.

multiplier *number*

Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD determines that the connection to that peer is not operational. Valid values range from 3 through 50.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Before using the **holdover-interval**, **interval**, **min-rx**, and **multiplier** parameters, you must first enable BFD using the **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name* } **bfd** command.

For single-hop BFD sessions, BFD considers the interval values that are configured on the interface, but not the nondefault values that are configured with this global command.

The **no** form of the command removes the BFD for BGP configuration for BGP neighbors or peer groups.

Examples

The following example configures BFD for a specified peer group and sets the BFD holdover interval to 18.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor pg1 bfd
device(config-bgp-router)# neighbor pg1 bfd holdover-interval 18
```

The following example configures BFD for a BGP neighbor with the IP address 10.10.1.1 and sets the BFD session timer values.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.10.1.1 bfd
device(config-bgp-router)# neighbor 10.10.1.1 bfd interval 120 min-rx 150 multiplier 8
```

neighbor capability as4

Enables or disables support for 4-byte autonomous system numbers (ASNs) at the neighbor or peer-group level.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **capability as4** [**disable** | **enable**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **capability as4** [**disable** | **enable**]

Command Default

4-byte ASNs are disabled by default.

Parameters

ip-address

IPv4 address of the neighbor.

ipv6-address

IPv6 address of the neighbor .

peer-group-name

Peer group name configured by the **neighbor** *peer-group-name* command.

disable

Disables 4-byte numbering.

enable

Enables 4-byte numbering.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **disable** keyword or the **no** form of this command to remove all neighbor capability for 4-byte ASNs.

4-byte ASNs are first considered at the neighbor, then at the peer group, and finally at the global level.

Examples

This example enables 4-byte ASNs for a specified neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 capability as4 enable
```

neighbor capability orf prefixlist

Advertises outbound route filter (ORF) capabilities to peer routers.

Syntax

neighbor { *ip_address* | *ipv6_address* | *peer-group-name* } **capability orf prefixlist** [**receive** | **send**]

no neighbor { *ip_address* | *ipv6_address* | *peer-group-name* } **capability orf prefixlist** [**receive** | **send**]

Command Default

ORF capabilities are not advertised to a peer device.

Parameters

ip_address

Specifies the IPv4 address of the neighbor.

ipv6_address

Specifies the IPv6 address of the neighbor.

peer-group-name

Specifies a peer group.

receive

Enables the ORF prefix list capability in receive mode.

send

Enables the ORF prefix list capability in send mode.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to disable ORF capabilities.

Examples

This example advertises the ORF send capability to a neighbor with the IP address 10.11.12.13.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 capability orf prefixlist send
```

This example advertises the ORF receive capability to a neighbor with the IPv6 address 2001:2018:8192::125 for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 capability orf prefixlist
receive
```

The following example advertises the ORF Send Capability for IPv6 address family to a neighbor with the IP address 10.11.12.13.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 10.11.12.13 capability orf prefixlist send
```

neighbor default-originate

Configures the device to send the default IPv4 route 0.0.0.0 or the default IPv6 route ::/0 to a neighbor or a peer-group. Route maps can also be applied to the default-originated routes.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **default-originate** [**route-map** *route-map-name*]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **default-originate** [**route-map** *route-map-name*]

Command Default

Disabled.

Parameters

ip-address

IPv4 address of the neighbor.

ipv6-address

IPv6 address of the neighbor.

peer-group-name

Peer group name configured by the **neighbor** *peer-group-name* command.

route-map *route-map-name*

Applies a route map *route-map-name* to a default originated route.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command withdraws the default routes.

Examples

The following example sends the IPv4 default route to the BGP4 neighbor 10.11.12.13.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 default-originate
```

The following example sends IPv6 default route to the BGP4 neighbor 10.11.12.13.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 10.11.12.13 default-originate
```

neighbor description

Specifies a name for a neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **description** *string*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **description**

Parameters

ip-address

IPv4 address of the neighbor.

ipv6-address

IPv6 address of the neighbor.

peer-group-name

Peer group name configured by the **neighbor** *peer-group-name* command.

description *string*

Specifies the name of the neighbor, an alphanumeric string up to 220 characters long.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command removes the name.

Examples

The following example specifies a BGP4 neighbor name.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 description mygoodneighbor
```

The following example specifies a BGP4+ neighbor name for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
```

```
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 default-originate route-map
myroutemap
```

neighbor ebgp-btsh

Enables BGP time to live (TTL) security hack protection (BTSH) for eBGP.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **ebgp-btsh**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **ebgp-btsh**

Command Default

Disabled.

Parameters

ip-address

Specifies the IPv4 address of the neighbor.

ipv6-address

Specifies the IPv6 address of the neighbor.

peer-group-name

Specifies a peer group.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

To maximize the effectiveness of this feature, the **neighbor ebgp-btsh** command should be executed on each participating device. The **neighbor ebgp-btsh** command is supported for both directly connected peering sessions and multihop eBGP peering sessions. For directly connected neighbors, when the **neighbor ebgp-btsh** command is used, the device expects BGP control packets received from the neighbor to have a TTL value of either 254 or 255. For multihop peers, when the **neighbor ebgp-btsh** command is used, the device expects the TTL for BGP control packets received from the neighbor to be greater than or equal to 255 minus the configured number of hops to the neighbor.

The **no** form of the command disables BTSH for eBGP.

Examples

The following example enables GTSM between a device and a neighbor with the IP address 10.10.10.1.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.1.1.1 ebgp-btsh
```

The following example enables GTSM between a device and a neighbor with the IPv6 address 2001:2018:8192::125.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 2001:2018:8192::125 ebgp-btsh
```

neighbor ebgp-multihop

Allows eBGP neighbors that are not on directly connected networks and sets an optional maximum hop count.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **ebgp-multihop** [*max-hop-count*]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **ebgp-multihop**

Parameters

ip-address

IPv4 address of the neighbor

ipv6-address

IPv6 address of the neighbor

peer-group-name

Peer group name configured by the **neighbor** *peer-group-name* command.

max-hop-count

Maximum hop count. Range is from 1 through 255.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Examples

The following example enables eBGP multihop and sets the maximum hop count to 20.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 ebgp-multihop 20
```

The following example enables BGP4+ eBGP multihop for VRF instance "red" and sets the maximum hop count to 40.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 ebgp-multihop 40
```

neighbor enable-peer-as-check

Enables the outbound AS_PATH check function so that a BGP sender speaker does not send routes with an AS path that contains the ASN of the receiving speaker.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **enable-peer-as-check**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **enable-peer-as-check**

Command Default

Disabled.

Parameters

ip-address

Specifies the IPv4 address of the neighbor.

ipv6-address

Specifies the IPv6 address of the neighbor.

peer-group-name

Specifies a peer group.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

BGP address-family L2VPN EVPN configuration mode

Usage Guidelines

When the **neighbor enable-peer-as-check** command is used for a BGP address family, a neighbor reset is required.

The **no** form of the command disables the AS-path check function.

Examples

The following example enables the outbound AS_PATH check function for the L2VPN EVPN unicast address family.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# neighbor 10.1.1.1 enable-peer-as-check
```

The following example enables the outbound AS_PATH check function for the IPv6 unicast address family.

```
SLX# configure terminal
SLX(config)# router bgp
SLX(config-bgp-router)# address-family ipv6 unicast
SLX(config-bgp-ipv6u)# neighbor 10.1.1.1 enable-peer-as-check
```

neighbor encapsulation

Sets the encapsulation type for an IPv4 neighbor, an IPv6 neighbor, or a peer group.

Syntax

neighbor { *IPv4-address* | *IPv6-address* | *peer-group-name* } { **vxlan** }

no neighbor { *IPv4-address* | *IPv6-address* | *peer-group-name* } {**vxlan** }

Command Default

None (SLX 9150 and SLX 9250 devices)

Parameters

IPv4-address

Specifies an IPv4 address.

IPv6-address

Specifies an IPv6 address.

peer-group-name

Specifies a peer group.

vxlan

Specifies VXLAN encapsulation.

Modes

BGP address-family L2VPN EVPN configuration mode

Usage Guidelines

The **no** form of the command restores the default.

Examples

The following example configures VXLAN encapsulation for an IPv4 neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# neighbor 10.1.1.1 encapsulation vxlan
```

neighbor enforce-first-as

Ensures that a device requires the first ASN listed in the AS_SEQUENCE field of an AS path-update message from EBGP neighbors to be the ASN of the neighbor that sent the update.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **enforce-first-as** [**disable** | **enable**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **enforce-first-as** [**disable** | **enable**]

Command Default

Disabled by default.

Parameters

ip-address

IPv4 address of the neighbor.

ipv6-address

IPv6 address of the neighbor.

peer-group-name

Peer group name configured by the **neighbor** *peer-group-name* command.

disable

Disables this feature.

enable

Enables this feature.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to disable this requirement globally for the device.

Examples

This example enables the enforce-first-as feature for a specified neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 enforce-first-as enable
```

This example enables the enforce-first-as feature for a BGP4+ specified neighbor for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 enforce-first-as enable
```

neighbor filter-list

Specifies a filter list to be applied to updates from or to the specified neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **filter-list** *ip-prefix-list-name* { **in** | **out** }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **filter-list** *ip-prefix-list-name* { **in** | **out** }

Command Default

No filter list is applied.

Parameters

ip-address

IPv4 address of the neighbor.

ipv6-address

IPv6 address of the neighbor.

peer-group-name

Peer group name configured by the **neighbor** *peer-group-name* command.

ip-prefix-list-name

Name of the filter list. The name must be between 1 and 63 ASCII characters in length.

in

Specifies that the list is applied on updates received from the neighbor.

out

Specifies that the list is applied on updates sent to the neighbor.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of the command to remove the association of filter-list from peer or peer-group.

Examples

This example specifies that filter list “myfilterlist” be applied to updates to a neighbor with the IP address 10.11.12.13 for the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 filter-list myfilterlist out
```

This example specifies that filter list “2” be applied to updates from a neighbor with the IPv6 address 2001:2018:8192::125 for the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 filter-list 2 in
```

This example specifies that filter list “2” be applied to updates from a neighbor with the IPv6 address 2001:2018:8192::125 for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 filter-list 2 in
```

This example specifies that filter list *2* be applied to updates from a neighbor with the IPv4 address 20.0.0.1 for the VRF instance *red*.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 20.0.0.1 filter-list 2 in
```

neighbor flowspec redirect

Configures the Border Gateway Protocol flow specification (BGP flowspec) redirect nexthop holder and action type at neighbor or peer-group level.

Syntax

neighbor { *ip-address* | *peer-group* } **flowspec redirectholder** { **nrli** | **extended-community** } **type** { **0x0800** | **0x080c** }

no neighbor { *ip-address* | *peer-group* } **flowspec redirecttype** { **0x0800** | **0x080c** } **holder** { **nrli** | **extended-community** }

Command Default

By default, BGP flowspec redirect nexthop holder is set to **nrli** and the action type is set to **0x080c**.

Parameters

ip-address

IP address in IPv4 format.

peer-group

Name of a peer group.

holder

Specifies where the IP address of redirect nexthop is encoded in the BGP update packet.

nrli

Specifies encoding as Network Layer Reachability Information (NRLI) in the BGP update packet.

extended-community

Specifies encoding as extended-community information in the BGP update packet.

type

Specifies the extended-community type for the redirect IP nexthop action.

0x0800

Specifies an extended-community type of **0x0800** .

0x080c

Specifies an extended-community type of **0x080c** .

Modes

BGP address-family IPv4 flowspec configuration mode

Usage Guidelines

Settings configured by using the **neighbor flowspec redirect** command only apply to locally-generated BGP flowspec routes; they are not applied to the advertisement of remote routes.

The **no** form of the command restores the default configuration.

Examples

The following example shows how to specify encoding the nexthop IP address as **nrli** in the BGP update packet and configure the BGP flowspec redirect nexthop action type as **x0800**.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 flowspec
device(config-bgp-ipv4fs)# neighbor 10.61.61.1 flowspec redirect holder nrli next-hop
type 0x0800
```

neighbor flowspec validation

Configures Border Gateway Protocol flow specification (BGP flowspec) route validation at neighbor or peer-group level.

Syntax

neighbor { *ip-address* | *peer-group* } **flowspec validation** [**redirect**]

no neighbor { *ip-address* | *peer-group* } **flowspec validation** [**redirect**]

Command Default

By default, flowspec validation is enabled at neighbor or peer-group level.

Parameters

ip-address

IP address in IPv4 format.

peer-group

Name of a peer group.

redirect

Specifies the validation of only the redirect IP nexthop address.

Modes

BGP address-family IPv4 flowspec configuration mode

Usage Guidelines

Flowspec validation can be configured at neighbor, peer-group or address-family level with the neighbor-level configuration prioritized over peer-group level configuration and the peer-group level configuration prioritized over the address-level configuration.

Use the **neighbor flowspec validation** command to configure flowspec validation at neighbor or peer-group level. To configure flowspec validation at address-family level, refer to the **flowspec validation** command.

By default, flowspec validation is enabled. Use the **no** form of the command to completely disable flowspec validation at neighbor or peer-group level. To only disable redirect IP nexthop validation at neighbor or peer-group level, use the **no** form of the command specifying the **redirect** option.

Only one flowspec validation configuration is allowed at a time. Configuration operates as follows:

- When complete flowspec validation is already disabled at neighbor or peer-group level, issuing the **no neighbor flowspec validation** command specifying the **redirect** option has no impact; complete flowspec validation remains disabled.
- When the **redirect** option is already disabled, issuing the **no neighbor flowspec validation** command without the **redirect** option changes the configuration to complete flowspec validation disabled at neighbor or peer-group level.

Examples

The following example shows how to disable IPv4 flowspec validation. In this example, only redirect IP nexthop validation is disabled for a peer group named peer-group1 in the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 flowspec
device(config-bgp-ipv4fs)# no neighbor peer-group1 flowspec validation redirect
```

neighbor graceful-restart

Enables BGP graceful restart of individual BGP neighbors.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **graceful-restart**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **graceful-restart disable**

Parameters

ip-address

Specifies the IPv4 address of the neighbor.

ipv6-address

Specifies the IPv6 address of the neighbor.

peer-group-name

Specifies a peer group.

graceful-restart

Enables the graceful restart of BGP neighbor.

disable

Disables *graceful-restart* when it is enabled.

Modes

Global level graceful-restart configuration is avilable under inside <term> **address** family configuration mode and neighbour level graceful configuration is avialble under **router bgp** configuration mode.

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

BGP address-family L2VPN EVPN configuration mode

Usage Guidelines

The *disable* parameter of this command must be used. The **graceful restart disable** command must be used to disable graceful restart. The 'no' form of the command will not disable graceful restart.

Examples

The following example configures graceful restart of BGP session with a neighbor with the IPv6 address 2001:2018:8192::125.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 2001:2018:8192::125 graceful-restart
```

The following example removes graceful-restart configuration for a BGP session with a neighbor with the IP address 10.1.1.1 in L2VPN EVPN configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.1.1.1 graceful-restart disable
```

neighbor graceful-shutdown

Configures graceful shutdown of a link to a BGP neighbor or peer group.

Syntax

neighbor [*ipv4-address* | *ipv6-address* | *peer-group-name*] **graceful-shutdown** *seconds* { **community** *value* [**local-preference** *value*] | **local-preference** *value* } [**route-map** *route-map-name*]

no neighbor [*ip-address* | *ipv6-address* | *peer-group-name*] **graceful-shutdown** *seconds* { **community** *value* [**local-preference** *value*] | **local-preference** *value* } [**route-map** *route-map-name*]

Command Default

BGP graceful shutdown is disabled.

Parameters

ipv4-address

Specifies a neighbor in IPv4 address format.

ipv6-address

Specifies a neighbor in IPv6 address format.

peer-group-name

Specifies a neighbor as a peer group name (that is configured by using the **neighbor** *peer-group-name* command).

graceful-shutdown *seconds*

Specifies the number of seconds to elapse before graceful shutdown occurs. The range is from 30 through 600.

community *value*

Specifies the community attribute for BGP graceful shutdown. The range is from 1 through 4294967295.

local-preference *value*

Specifies the local preference attribute for BGP graceful shutdown. The range is from 0 through 4294967295.

route-map *route-map-name*

Specifies the route map to apply for BGP graceful shutdown.

Modes

BGP configuration mode

Usage Guidelines

Note
neighbor send-community configuration enables sending community attribute information to a BGP peer. Before the graceful shutdown community attribute can be sent, the send community must be negotiated by using the **neighbor send-community** command specifying the **both** option.

When a neighbor address is not specified, this command configures graceful shutdown for all neighbors on the device.

This command is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

When a route map is not specified, the default GRACEFUL_SHUTDOWN parameters are applied.

When a route map is specified, only route-map parameters are applied.

Note
Modifications made to the specified route map during the graceful-shutdown period, which is specified using the **graceful-shutdown** parameter, are not effective for graceful shutdown advertisement routes.

The **no** form of the command removes the specified BGP graceful shutdown configuration.

Examples

The following example shows how to configure BGP graceful shutdown for a neighbor (10.11.22.23) and set the shutdown to occur after 580 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.22.23 graceful-shutdown 580
```

The following example shows how to configure BGP graceful shutdown for a peer group named grp-1 and set the shutdown to occur after 620 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor grp-1 graceful-shutdown 620
```

The following example shows how to configure BGP graceful shutdown for a neighbor (10.11.22.23) and apply the attributes of a route map named myroutemap to the shutdown which is set to occur after 600 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.22.23 graceful-shutdown 600 route-map myroutemap
```

The following example shows how to configure BGP graceful shutdown for a neighbor (10.11.22.23) with community attribute 20. The shutdown which is set to occur after 600 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.22.23 graceful-shutdown 600 community 20
```

neighbor local-as

Causes the device to prepend the local autonomous system number (ASN) automatically to routes received from an eBGP peer.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **local-as** *num* [**no-prepend**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **local-as** *num* [**no-prepend**]

Command Default

This feature is disabled.

Parameters

ip-address

IPv4 address of the neighbor.

ipv6-address

IPv6 address of the neighbor.

peer-group-name

Peer group name configured by the **neighbor** *peer-group-name* command.

num

Local ASN. Range is from 1 through 4294967295.

no-prepend

Causes the device to stop prepending the selected ASN.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to remove the local ASN.

Examples

This example ensures that a device prepends the local ASN.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 local-as 100
```

This example stops the device from prepending the selected ASN.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 local-as 100 no-prepend
```

neighbor maxas-limit in

Causes the device to discard routes received in UPDATE messages if those routes exceed a maximum AS path length.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **maxas-limit in** { *num* | **disable** }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **maxas-limit in**

Command Default

This command is disabled by default.

Parameters

ip-address

IPv4 address of the neighbor.

ipv6-address

IPv6 address of the neighbor.

peer-group-name

Peer group name configured by the **neighbor** *peer-group-name* command.

num

Maximum length of the AS path. Range is from 0 through 300. The default is 300.

disable

Prevents a neighbor from inheriting the configuration from the peer group or global configuration and instead uses the default system value.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to remove this configuration.

Examples

This example changes the length of the maximum allowed AS path length from the default.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 maxas-limit in 200
```

This example prevents a neighbor from inheriting the configuration from the peer group or global configuration and instead use the default system value.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 2001:2018:8192::125 maxas-limit in disable
```

neighbor maximum-prefix

Specifies the maximum number of IP network prefixes (routes) that can be learned from a specified neighbor or peer group.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **maximum-prefix** *num* [*threshold*] [**teardown**] [**restart-interval** *restart-interval-in-minutes*]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **maximum-prefix** *num* [*threshold*] [**teardown**] [**restart-interval**]

Command Default

This feature is disabled.

Parameters

ip-address

IPv4 address of the neighbor.

ipv6-address

IPv6 address of the neighbor.

peer-group-name

Peer group name configured by the **neighbor** *peer-group-name* command.

num

Maximum number of IP prefixes that can be learned. Range is from 0 through 2147483647. Default is 0 (unlimited).

threshold

Specifies the percentage of the value specified by *num* (IP prefixes) that causes a syslog message to be generated. Range is from 1 through 100.

teardown

Tears down the neighbor session if the maximum number of IP prefixes is exceeded.

restart-interval *restart-interval-in-minutes*

After a session is torn down, this value controls the duration after which the session is restarted. Range is 1-65535 minutes.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

BGP address-family L2VPN EVPN configuration mode

Usage Guidelines

The **no** form of the command restores the defaults.

The maximum number of prefixes that can be learned from a specific neighbor or from a peer-group is specified in the *maximum-prefix* configuration.

The *teardown* parameter for this command indicates that the neighbor session will be brought down when the number of learned prefixes exceeds the value configured in the *maximum-prefix* configuration.

When a session is brought down due to the above reason, it has to be manually restored using either of the **clear ip bgp neighbor all** or the **clear ip bgp neighbor** commands.

When both the *maximum-prefix* and *teardown* parameters are configured, the neighbour session is automatically torn-down when the *maximum-prefix* value is exceeded. When the *restart-interval* is also configured, this torn-down session is restarted automatically when the duration specified in the *restart-interval-in-minutes* expires.

Examples

The following example sets the maximum number of IPv4 prefixes that will be accepted from the neighbor with the IP address 10.11.12.13 to 100000, and sets the threshold value to 80%.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 maximum-prefix 100000 threshold 80
```

The following example, for VRF instance "red," sets the maximum number of prefixes that will be accepted from the neighbor with the IPv6 address 2001:2018:8192::125 to 100000, and sets the threshold value to 90%.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 maximum-prefix 100000
threshold 90
```

The following example sets the maximum number of prefixes that will be accepted from the neighbor with the IP address 10.1.2.3 to 100000 in L2VPN EVPN configuration mode.

```
device# configure terminal
device(config)# router bgp
```

```
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# neighbor 10.1.2.3 maximum-prefix 100000
```

The following example extends the previous example to configure a threshold value to generate a RASLOG entry. The threshold value is set at 80% of the configured prefixes.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# neighbor 10.1.2.3 maximum-prefix 100000 80
```

The following example sets the maximum number of prefixes that will be accepted from the neighbor with the IP address 10.1.2.3 to 100000 in L2VPN EVPN configuration mode. It also configures a threshold for generating a RASLOG entry. The example command then configures a restart interval to restart the session after 7 minutes when the interface is shut down due to maximum prefixes being exceeded.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# neighbor 10.1.2.3 maximum-prefix 100000 80 restart-interval 7
```

The following example sets the maximum number of IPv6 prefixes that will be accepted from the neighbor with the IP address 10.11.12.13 to 10000, and sets the threshold value to 80%.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 10.11.12.13 maximum-prefix 10000 threshold 80
```

neighbor next-hop-self

Causes the device to list itself as the next hop in updates that are sent to the specified neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **next-hop-self** [**always**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **next-hop-self** [**always**]

Parameters

ip-address

Specifies the IPv4 address of the neighbor.

ipv6-address

Specifies the IPv6 address of the neighbor.

peer-group-name

Specifies the peer group name configured by the **neighbor** *peer-group-name* command.

always

Enables this feature for route reflector (RR) routes.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command disables this feature.

Examples

The following example causes all updates destined for the neighbor with the IP address 10.11.12.13 to advertise this device as the next hop.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 next-hop-self
```

The following example, for the VRF instance "red," causes all updates destined for the neighbor with the IPv6 address 2001:2018:8192::125 to advertise this device as the next hop.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 10.11.12.13 next-hop-self
```

neighbor next-hop-unchanged

Enables BGP to send updates to eBGP peers with the next-hop attribute unchanged.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **next-hop-unchanged**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **next-hop-unchanged**

Command Default

This functionality is not enabled.

Parameters

ip-address

Specifies an IPv4 address.

ipv6-address

Specifies an IPv6 address.

peer-group-name

Specifies a peer group.

Modes

BGP address-family L2VPN EVPN configuration mode

Usage Guidelines

By default, BGP speakers change the next hop while sending the updates to eBGP neighbors. Use this command to override this behavior. When this command is used, the next hop attribute remains unchanged while updates are sent to eBGP peers, and the BGP speaker is forced to retain the next hop address in the BGP updates received from neighbors.

The **no** form of the command disables the sending of updates to eBGP peers with the next-hop attribute unchanged.

Examples

The following example disables the sending of updates to eBGP peers with the next-hop attribute unchanged.

```
device# configure terminal
device(config)# router bgp
```

```
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# no neighbor 10.11.12.13 next-hop-unchanged
```

neighbor password

Specifies an MD5 password for securing sessions between the device and a neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **password** *string*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **password**

Command Default

No password is set.

Parameters

ip-address

Specifies the IPv4 address of the neighbor.

ipv6-address

Specifies the IPv6 address of the neighbor.

peer-group-name

Specifies the peer group name configured by the **neighbor** *peer-group-name* command.

password *string*

Password of up to 63 characters in length that can contain any alphanumeric character. MD5 passwords cannot have ASCII character 32 ('SPACE') as a part of the password string.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command removes a configured MD5 password.

Examples

The following example specifies a password for securing sessions with a specified neighbor.

```
device# configure terminal
```

```
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 password s0M3P@55W0Rd
```

The following BGP4+ example, for VRF instance "red," specifies a password for securing sessions with a specified neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv4u-vrf)# neighbor 2001:2018:8192::125 password s0M3P@55W0Rd
```

neighbor peer-dampening

Enables peer-dampening for a single neighbor.

Syntax

neighbor { *x.x.x.x* | *A:B::C:D* } **peer-dampening** [**delay-hold** *0-65535* | **penalty** *1-65535* | **max-penalty** *1-65535* | **stability-interval** *0-65535*]

no neighbor { *x.x.x.x* | *A:B::C:D* } **peer-dampening** [**delay-hold** | **penalty** | **max-penalty** | **stability-interval**]

Parameters

{ *x.x.x.x* | *A:B::C:D* }

The IP address of the neighbor device in IPv4 or IPv6 format.

delay-hold *0-65535*

The amount of time, in seconds, that a session remains in the *idle-state* after the first peer flap event is received. During this time, all route advertisements from this peer are ignored. The default value is zero (0) seconds.

penalty *1-65535*

The amount of time, in seconds, which gets added to *idle-hold* timer every time a peer flap event is received. The default value is 300 seconds.

max-penalty *1-65535*

The maximum amount of time, in seconds, that a session remains in the *idle-*state after it has experienced repeated instability. The default value is 3600 seconds.

stability-interval *0-65535*

The interval of time, in seconds, the session must be error-free in order to consider it to be stable. The default value is 1800 seconds.

Modes

Router BGP

Usage Guidelines

- BGP peer dampening can be global or on individual neighbor/peer-group.
- All routes from a dampened peer will be removed from the routing table
- When route dampening is also configured, peer dampening will take precedence over route dampening.
- Dampening cannot be applied to dynamic peers.

- Dampening cannot be applied to administratively down neighbors.
- When downgrading to a firmware that does not support *peer-dampening*, an error will be displayed. You must remove this configuration to successfully complete the downgrade.

Examples

The following example shows how to enable Peer Dampening feature for a single neighbor.

```
SLX (config)# router bgp
SLX (config-bgp-router)# neighbor 10.9.9.10 peer-dampening delay-hold 10 penalty 300 max-
penalty 3600 stability-interval 1800
SLX (config-bgp-router)#
```

neighbor peer-dampening (peer-group)

Enables BGP Peer Dampening for a peer group.

Syntax

neighbor *peer-group* **peer-dampening** [**delay-hold** *0-65535* | **penalty** *1-65535* | **max-penalty** *1-65535* | **stability-interval** *0-65535*]

no neighbor peer-dampening (peer-group) [**delay-hold** | **penalty** | **max-penalty** | **stability-interval**]

Parameters

peer-group

The name of the peer-group to which this configuration must be applied to.

delay-hold *0-65535*

The amount of time, in seconds, that a session remains in the *idle-state* after the first peer flap event is received. During this time, all route advertisements from this peer are ignored. The default value is zero (0) seconds.

penalty *1-65535*

The amount of time, in seconds, which gets added to *idle-hold* timer every time a peer flap event is received. The default value is 300 seconds.

max-penalty *1-65535*

The maximum amount of time, in seconds, that a session remains in the *idle-*state after it has experienced repeated instability. The default value is 3600 seconds.

stability-interval *0-65535*

The interval of time, in seconds, the session must be error-free in order to consider it to be stable. The default value is 1800 seconds.

Modes

Router BGP

Usage Guidelines

- BGP peer dampening can be global or on individual neighbor/peer-group.
- All routes from a dampened peer will be removed from the routing table
- When route dampening is also configured, peer dampening will take precedence over route dampening.
- Dampening cannot be applied to dynamic peers.

- Dampening cannot be applied to administratively down neighbors.
- When downgrading to a firmware that does not support *peer-dampening*, an error will be displayed. You must remove this configuration to successfully complete the downgrade.

Examples

The following example shows how to enable Peer Dampening for a peer-group.

```
SLX (config)# router bgp
SLX (config-bgp-router)# neighbor 50.0.0.1 peer-group pg-level-1
SLX (config-bgp-router)# neighbor pg-level-1 peer-dampening delay-hold 10 penalty 300 max-
penalty 3600 stability-interval 1800
SLX (config-bgp-router)#
```

neighbor peer-group

Configures a BGP neighbor to be a member of a peer group.

Syntax

neighbor { *ip-address* | *ipv6-address* } **peer-group** *string*

no neighbor { *ip-address* | *ipv6-address* } **peer-group** *string*

Parameters

ip-address

Specifies the IPv4 address of the neighbor.

ipv6-address

Specifies the IPv6 address of the neighbor.

peer-group *string*

Specifies the name of a BGP peer group. The name can be up to 63 characters in length and can be composed of any alphanumeric character.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command removes a neighbor from the peer group.

When a peer group is created, a warning is displayed to activate peer group for IPv6 address family.

When an IPv6 neighbor is added to a peer group, and the peer group is not activated for IPv6 address-family, a warning will be displayed.

Examples

The following example assigns a specified neighbor to a peer group called *mypeergroup1*.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 peer-group mypeergroup1
  %Warning: Please activate Peer-group for IPv6 address-family
```

The following BGP4+ example, for VRF instance "red", assigns a specified neighbor to a peer group called *mypeergroup1*.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv4u)# neighbor 2001:2018:8192::125 peer-group mypeergroup1
  %Warning: Please activate Peer-group for IPv6 address-family in default-vrf
```

neighbor peer-group-name alternate-as-range

Adds a neighbor from an autonomous system (AS) to the IPv4 multiprotocol BGP neighbor table of the local router.

Syntax

neighbor peer-group-name alternate-as-range {**add** | **remove** *as-range* } [*as-range*]

no neighbor peer-group-name alternate-as-range

Command Default

By default, AS neighbors are not added to the BGP neighbor table

Parameters

add | **remove**

Specifies whether to add or remove the indicated AS number or range.

as-range

Specifies the AS number or range of AS numbers to add to the BGP neighbor table. Separate multiple entries with a comma. Separate contiguous ranges with a hyphen. For example: 100, 200-300.

Modes

BGP configuration mode

Usage Guidelines

Use the **no** form of the command to reset the default functionality.

Examples

This example adds an AS number and a range of AS numbers.

```
device# configure terminal
device(cofig)# neighbor peer-group-name alternate-as-range add 100,200-300
```

This example removes an AS number.

```
device# configure terminal
device(cofig)# neighbor peer-group-name alternate-as-range remove 100
```

This example resets the default functionality.

```
device# configure terminal
device(cofig)# no neighbor peer-group-name alternate-as-range
```

neighbor prefix-list

Filters outgoing and incoming route updates to or from a particular BGP neighbor according to the length of its IP address and mask.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **prefix-list** *string* { **in** | **out** }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **prefix-list** *string* { **in** | **out** }

Command Default

This feature is disabled by default.

The *no* form of this command removes prefix list association from the BGP neighbor or peer-group.

Parameters

ip-address

IPv4 address of the neighbor

ipv6-address

IPv6 address of the neighbor

peer-group-name

Peer group name configured by the **neighbor** *peer-group-name* command.

string

Name of the prefix list. Range is from 1 through 63 ASCII characters.

in

Applies the filter in incoming routes.

out

Applies the filter in outgoing routes.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of the command to restore the defaults.

Examples

This example applies the prefix list "myprefixlist" to incoming advertisements to neighbor 10.11.12.13 for the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 prefix-list myprefixlist in
```

This example applies the prefix list "myprefixlist" to outgoing advertisements to neighbor 2001:2018:8192::125 for the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 prefix-list myprefixlist out
```

This example applies the prefix list "myprefixlist" to outgoing advertisements to neighbor 2001:2018:8192::125 for VRF instance "red," .

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 prefix-list myprefixlist out
```

This example applies the prefix list *myipv6prefixlist* to incoming advertisements to the neighbor 10.11.12.13 for the default VRF of address family IPv6 unicast mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 10.11.12.13 prefix-list myipv6prefixlist in
```

neighbor remote-as

Specifies the autonomous system (AS) in which a remote neighbor resides.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **remote-as** *num*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **remote-as**

Command Default

No AS is specified.

Parameters

ip-address

IPv4 address of the neighbor

ipv6-address

IPv6 address of the neighbor

peer-group-name

Peer group name configured by the **neighbor** *peer-group-name* command.

num

Remote AS number (ASN). Range is from 1 through 4294967295.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command removes the neighbor from the AS.

Examples

The following example specifies AS 100 for a neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 remote-as 100
```

The following BGP4+ example, for VRF instance "red," specifies AS 100 for a neighbor.

```
device# configure terminal
```

```
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 remote-as 100
```

neighbor remove-private-as

Configures a device to remove private autonomous system numbers (ASNs) from UPDATE messages that the device sends to a neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **remove-private-as**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **remove-private-as**

Parameters

ip-address

IPv4 address of the neighbor

ipv6-address

IPv6 address of the neighbor

peer-group-name

Peer group name configured by the **neighbor** *peer-group-name* command.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The device will remove ASNs 64512 through 65535 (the well-known IPv4 BGP private ASNs) and ASNs 4200000000 through 4294967294 (the well-known IPv6 BGP private ASNs) from the AS-path attribute in UPDATE messages that the device sends to a neighbor.

The **no** form of the command restores the default so that private ASNs are not removed from UPDATE messages sent to a neighbor by a device.

Examples

The following example removes private ASNs globally.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 remove-private-as
```

The following example removes private ASNs for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 10.11.12.13 remove-private-as
```

neighbor route-map

Filters the outgoing and incoming route updates to or from a particular BGP neighbor according to a set of attributes defined in a route map.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **route-map** { **in** *string* | **out** *string* }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **route-map** { **in** *string* | **out** *string* }

Command Default

This feature is disabled.

Parameters

ip-address

IPv4 address of the neighbor

ipv6-address

IPv6 address of the neighbor

peer-group-name

Peer group name configured by the **neighbor** *peer-group-name* command.

in

Applies the filter on incoming routes.

string

Name of the route map. Length is between 1-63 ASCII characters.

out

Applies the filter on outgoing routes.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

BGP address-family L2VPN EVPN configuration mode

Usage Guidelines

The **no** form of the command restores the defaults.

Examples

The following example applies a route map named "myroutemap" to an outgoing route from 10.11.12.13.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 route-map out myroutemap
```

The following example applies a route map named "myroutemap" to an incoming route from 2001:2018:8192::125.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 2001:2018:8192::125 route-map in myroutemap
```

The following example applies a route map named "myroutemap" to an outgoing route from 10.11.12.13 in L2VPN EVPN configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# neighbor 10.11.12.13 route-map out myroutemap
```

The following example applies a route map named *myroutemap* to an incoming route from 10.11.12.13 in address family IPv6 mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv46u)# neighbor 10.11.12.13 route-map in myroutemap
```

neighbor route-reflector-client

Configures a neighbor as a route-reflector client.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **route-reflector-client**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **route-reflector-client**

Parameters

ip-address

Specifies the IPv4 address of the neighbor

ipv6-address

IPv6 address of the neighbor

peer-group-name

Specifies the peer group name configured by the **neighbor** *peer-group-name* command.

Modes

BGP configuration mode

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv4 unicast vrf configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use this command on a host device to configure a neighbor to be a route-reflector client. The host device from which the configuration is made becomes a route-reflector server.

The *no* form of this command removes route reflection capability for the BGP session.

Examples

The following example configures an IPv4 neighbor as a route-reflector client.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 route-reflector-client
```

The following example configures an IPv6 neighbor as a route-reflector client.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 2000::1 route-reflector-client
```

The following example configures an IPv6 neighbor to be a route-reflector client for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# neighbor 2001:2018:8192::125 route-reflector-client
```

The following example configures an IPv4 neighbor as a route-reflector client in address family IPv6 mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 10.11.12.13 route-reflector-client
```

neighbor rpki validation status disable

This command disables the RPKI validation for the configured neighbor. The default behavior is to allow the RPKI validation for the prefixes received from its neighbor.

Syntax

neighbor *ip address* **rpki validation state disable**

[no] neighbor *ip address* **rpki validation state disable**

Parameters

ip address

The IP address of the neighbor iBGP peer.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

When this configuration is set, any prefix received from the configured iBGP neighbor is not validated against the cached RPKI information.

The *no* format of this command enables the default behavior. The default behavior is to validate prefixes received from the configured iBGP neighbor.

Examples

This example disables validation of prefixes received from the iBGP peer with the IPv4 address of 10.10.11.1.

```
SLX(config)#router bgp
SLX(config-bgp-router)# address-family ipv4 unicast
SLX(config-bgp-ipv4u)# neighbor 10.10.11.1 rpki validation state disable
SLX(config-bgp-ipv4u)#
```

This example resets the configuration for validating of prefixes received from the iBGP peer with the IPv4 address of 10.10.11.1. Once this configuration is set, all prefixes from the iBGP neighbor will be validated according to the configured route map rules.

```
SLX(config)#router bgp
SLX(config-bgp-router)# address-family ipv4 unicast
SLX(config-bgp-ipv4u)# no neighbor 10.10.11.1 rpki validation state disable
SLX(config-bgp-ipv4u)#
```

neighbor send-community

Enables sending the community attribute in updates to the specified BGP neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **send-community** [**all** | **both** | **extended** | **large** | **standard**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **send-community** [**all** | **both** | **extended** | **large** | **standard**]

Command Default

The device does not send community attributes.

Parameters

ip-address

IPv4 address of the neighbor

ipv6-address

IPv6 address of the neighbor

peer-group-name

Peer group name configured by the **neighbor** *peer-group-name* command.

all

Sends all community attributes: extended, large, and standard. BGP address-family L2VPN EVPN configuration mode does not support this keyword.

both

Sends both standard and extended attributes.

extended

Sends extended attributes.

large

Sends BGP large community attributes. BGP address-family L2VPN EVPN configuration mode does not support this keyword.

standard

Sends standard attributes.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

BGP address-family L2VPN EVPN configuration mode

BGP address-family VPNv4 unicast configuration mode

BGP address-family VPNv6 unicast configuration mode

Usage Guidelines

If the **send-community** attribute is enabled after a BGP session has been established, the neighbor session must be cleared for this change to take effect.

The **no** form of the command restores the defaults.

Examples

The following example sends standard community attributes to a neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 send-community standard
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

The following example sends extended community attributes to a neighbor for VRF instance "red".

```
device# configure terminal
ddevice(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 send-community extended
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

The following example sends standard and extended community attributes to a neighbor in L2VPN EVPN configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# neighbor 10.1.1.1 send-community both
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

The following example sends standard community attributes to a neighbor in the address IPv6 unicast mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 10.11.12.13 send-community standard
%Warning: Please clear the neighbor session for the parameter change to take effect!
```

neighbor shutdown

Causes a device to shut down the session administratively with its BGP neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **shutdown**
[**generate-rib-out**]

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **shutdown**
[**generate-rib-out**]

Parameters

ip-address

IPv4 address of the neighbor

ipv6-address

IPv6 address of the neighbor

peer-group-name

Peer group name configured by the **neighbor** *peer-group-name* command.

generate-rib-out

When a peer is put into the shutdown state, Routing Information Base (RIB) outbound routes are not produced for that peer. Use this option to produce those routes.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Shutting down a session lets you configure the neighbor and save the configuration without the need to establish a session with that neighbor.

Examples

The following example causes a device to shut down the session administratively with its neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 shutdown
```

The following example causes a device to shut down the session administratively with its neighbor and generate RIB outbound routes for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 shutdown generate-rib-out
```

neighbor soft-reconfiguration inbound

Stores all the route updates received from a BGP neighbor.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **soft-reconfiguration inbound**

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **soft-reconfiguration inbound**

Parameters

ip-address

Specifies the IPv4 address of the neighbor

ipv6-address

Specifies the IPv6 address of the neighbor

peer-group-name

Specifies the peer group name.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Soft reconfiguration stores all the route updates received from a neighbor. If you request a soft reset of inbound routes, the software compares the policies against the stored route updates, instead of requesting the neighbor's BGP4 or BGP4+ route table or resetting the session with the neighbor.

Examples

The following example globally stores route updates from a BGP4 neighbor.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 soft-configuration inbound
```

The following example stores route updates from a BGP4+ neighbor for VRF instance "red".

```
device# configure terminal
```

```
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 soft-configuration inbound
```

neighbor static-network-edge

Overrides the default BGP4 behavior and advertises the network to a neighbor or peer group only when the corresponding route is installed as a forward route in the routing table.

Syntax

neighbor { *ip-address* | *peer-group-name* } **static-network-edge**

no neighbor { *ip-address* | *peer-group-name* } **static-network-edge**

Parameters

ip-address

Specifies the IPv4 address of the neighbor

peer-group-name

Specifies the peer group name configured by the **neighbor** *peer-group-name* command.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

Usage Guidelines

A BGP static network is always advertised to neighbors or a peer group, and if the corresponding route is not present in the routing table, BGP installs the null0 route. This command overrides the default behavior. This command is not supported for BGP4+.

Examples

The following example globally overrides the default BGP4 behavior.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 static-network-edge
```

The following example overrides the default BGP4 behavior for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast vrf red
device(config-bgp-ipv4u-vrf)# neighbor 10.11.12.13 static-network-edge
```

neighbor timers

Specifies how frequently a device sends KEEPALIVE messages to its BGP neighbors, as well as how long the device waits for KEEPALIVE or UPDATE messages before concluding that a neighbor is dead.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **timers keep-alive** *keepalive_interval* **hold-time** *holdtime_interval*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **timers keep-alive** *keepalive_interval* **hold-time** *holdtime_interval*

Parameters

ip-address

IPv4 address of the neighbor

ipv6-address

IPv6 address of the neighbor

peer-group-name

Peer group name configured by the **neighbor** *peer-group-name* command.

keep-alive *keepalive_interval*

Frequency (in seconds) with which a device sends keepalive messages to a peer. Range is from 0 through 65535 seconds. The default is 60.

hold-time *holdtime_interval*

Interval in seconds that a device waits to receive a keepalive message from a peer before declaring that peer dead. Range is from 0 through 65535 seconds. The default is 180.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command restores the defaults.

Examples

The following example sets the keepalive timer for a device to 120 seconds and the hold-timer to 360 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 timers keep-alive 120 hold-time 360
```

The following example sets the keepalive timer to 120 seconds and the hold-timer to 360 seconds for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 10.11.12.13 timers keep-alive 120 hold-time 360
```

neighbor unsuppress-map

Removes route suppression from BGP neighbor routes when those routes have been suppressed as a result of aggregation. All routes matching route-map rules are unsuppressed.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **unsuppress-map** *string*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **unsuppress-map** *string*

Command Default

This feature is disabled.

Parameters

ip-address

IPv4 address of the neighbor.

ipv6-address

IPv6 address of the neighbor

peer-group-name

Peer group name configured by the **neighbor** *peer-group-name* command.

string

Name of the route map. Range is from 1 through 63 ASCII characters.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of the command to restore the defaults.

Examples

The following BGP4 example removes route suppression for the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 unsuppress-map myroutemap
```

The following BGP4+ example removes route suppression for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 unsuppress-map myroutemap
```

The following BGP4+ example removes route suppression for address family IPv6 unicast of default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 10.11.12.13 unsuppress-map myroutemap
```

neighbor update-source

Configures the BGP device to communicate with a neighbor through a specified interface.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **update-source** { *ip-address-u-s* | *ipv6-address-u-s* | **ethernet** *slot* **/** *port* | **loopback** *num*| **ve-interface** *vlan_id* }

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **update-source** { *ip-address-u-s* | *ipv6-address-u-s* | **ethernet** *slot* **/** *port* | **loopback** *num*| **ve-interface** *vlan_id* }

Command Default

Disabled.

Parameters

ip-address

IPv4 address of the neighbor

ipv6-address

IPv6 address of the neighbor

peer-group-name

Peer group name configured by the **neighbor** *peer-group-name* command.

ip-address-u-s

IP address of the update source.

ipv6-address-u-s

IPv6 address of the update source.

ethernet

Specifies an ethernet interface.

slot

Specifies a valid slot number. For devices that do not support line cards, specify **0**.

port

Specifies a valid port number.

loopback *num*

Specifies a loopback interface.

ve-interface *vlan_id*

Specifies a virtual Ethernet VLAN interface.

Modes

BGP configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of the command to restore the defaults.

Examples

The following example configures the device to communicate with a neighbor through the specified IPv4 address and Ethernet interface 3/2.

```
device#configure terminal
device#(config)# router bgp
device(config-bgp-router)# neighbor 10.11.12.13 update-source ethernet 3/2
```

The following example configures the device to communicate with a neighbor through the specified IPv6 address.

```
SLX (config)# router bgp
SLX (config-bgp-router)# neighbor pg1 update-source 11:11::2
SLX (config-bgp-router)#
```

neighbor weight

Specifies a weight that the device will add to routes that are received from the specified BGP neighbor. BGP gives preference to routes with higher weights.

Syntax

neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **weight** *num*

no neighbor { *ip-address* | *ipv6-address* | *peer-group-name* } **weight**

Command Default

The default for *num* is 0.

Parameters

ip-address

IPv4 address of the neighbor.

ipv6-address

IPv6 address of the neighbor

peer-group-name

Name of the peer group.

num

Value from 1 through 65535.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of the command to restore the defaults.

BGP prefers larger weights over smaller weights.

Examples

This example changes the weight from the default.

```
device# configure terminal
device(config)# router bgp
```

```
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# neighbor 10.11.12.13 weight 100
```

This example changes the weight from the default for VRF instance "red".

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# neighbor 2001:2018:8192::125 weight 100
```

This example changes the weight from the default for IPv6 address family for neighbor 10.11.12.13.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# neighbor 10.11.12.13 weight 100
```

net

Configures an Intermediate System-to-Intermediate System (IS-IS) network entity title (NET) for the routing process.

Syntax

net *NSAP address*

no net *NSAP address*

Command Default

900 seconds (15 minutes).

Parameters

NSAP address

Specifies a Network Service Access Point (NSAP) address; composed of both an area ID and a system ID.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The *area-id* parameter specifies the area and has the format xx or xx.xxxx. For example, 49 and 49.2211 are valid area IDs.

The *system-id* parameter specifies the device's unique IS-IS router ID and has the format xxxx.xxxx.xxxx. You can specify any value for the system ID. A common practice is to use the base MAC address of the device as the system ID. The base MAC address is also the MAC address of port 1.

You must use the same system ID in all the NETs on the device.

The **no** form of the command removes the configured NET.

Examples

The following example configures a NET that has the area ID 49.2211, the system ID 0000.00bb.cccc (the base MAC address), and the SEL value 00.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# net 49.2211.0000.00bb.cccc.00
```

network

Configures the device to advertise a BGP network.

Syntax

network *network/mask* [**backdoor** | **route-map** *map-name* | **weight** *num*]

no network *network/mask* [**backdoor** | **route-map** *map-name* | **weight** *num*]

Command Default

No network is advertised.

Parameters

network/mask

Network and mask in CIDR notation.

backdoor

Changes administrative distance of the route to this network from the eBGP administrative distance (the default is 20) to the local BGP weight (the default is 200), tagging the route as a backdoor route.

route-map *map-name*

Specifies a route map with which to set or change BGP attributes for the network to be advertised. Range is from 1 through 63 ASCII characters.

weight*num*

Specifies a weight to be added to routes to this network. Range is 0 through 65535. The default is 0.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the no form of the command to restore the defaults.

Examples

This example imports the IP prefix 10.1.1.1/32 into the BGP4 database and specifies a route map called “myroutemap”.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# network 10.1.1.1/32 route-map myroutemap
```

This example imports the IPv6 prefix 2001:db8::/32 into the BGP4+ database and sets a weight of 300.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# network 2001:db8::/32 weight 300
```

next-hop-enable-default

Configures the device to use the BGP default route as the next hop.

Syntax

next-hop-enable-default

no next-hop-enable-default

Command Default

This feature is disabled.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

The **no** form of the command restores the default.

Examples

The following BGP4 example configures the device to use the default route as the next hop for the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# next-hop-enable-default
```

The following BGP4+ example configures the device to use the default route as the next hop for the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# next-hop-enable-default
```

next-hop-mpls

Configures BGP shortcuts using next-hop MPLS to force BGP to use an MPLS tunnel as the preferred route to a destination network when an MPLS LSP tunnel is available.

Syntax

next-hop-mpls [**compare-lsp-metric** | **follow-igp**]

no next-hop-mpls [**compare-lsp-metric** | **follow-igp**]

Command Default

BGP uses the default BGP decision process and native IP forwarding to build BGP EMCP routes. Only IP routing tables are used to resolve routes for the routing table.

Parameters

compare-lsp-metric

Enables BGP to compare the configured LSP metrics as the IGP cost for the next hop.

follow-igp

Ignores the MPLS metric cost in the BGP decision process and uses the IGP cost. BGP checks when an MPLS LSP is present, and totally ignores the LSP metric.

Modes

BGP address-family IPv4 unicast configuration mode

Usage Guidelines

When the **next-hop-mpls** command is enabled without either option, BGP sets the LSP metrics to one.

Enabling or disabling an option takes effect immediately. BGP automatically recalculates the existing BGP routes.

The **compare-lsp-metric** and **follow-igp** options are mutually exclusive.

When the **compare-lsp-metric** option is configured and you change the LSP metric, the routing table is updated.

Use the **no** form of the command to disable global next-hop MPLS.

When you use the **no** form of the command with the **compare-lsp-metric** or **follow-igp** option, all LSP metrics become equal cost. However, global next-hop MPLS remains enabled.

For the **follow-igp** option, consider the following:

- When you are running IGP throughout the network, and the IGP metric is trusted in the entire domain, you may want to rely on this IGP metric to make a best path and forwarding decision, regardless of whether the forwarding happens in native IP or MPLS encapsulation.
- The MPLS metric is manually configured in each LSP. There is no dynamic way to tie MPLS metric with an IGP metric. When using MPLS LSP as a BGP route outgoing interface, you loses the ability to tie the forwarding decision with a unified IGP metric.
- When combined with the BGP **install-igp-cost** command, you can change the route cost from BGP MED to IGP cost and is used when BGP routes are added to the RTM.
- When combined with a BGP outbound policy for route **set metric-type internal** command, you can set Layer-3 VPN and IP over MPLS routes using IGP metric to send out as the BGP MED value.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example enables BGP shortcuts through next-hop MPLS and BGP to set the next hop IGP cost to one instead of the actual LSP metric.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# next-hop-mpls
```

The following example enables BGP shortcuts through next-hop MPLS and BGP to use the configured LSP metrics as the IGP cost for the next hop.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# next-hop-mpls compare-lsp-metric
```

The following example enables BGP shortcuts through next-hop MPLS and BGP to ignore the LSP metrics and to use the IGP cost for the next hop.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# next-hop-mpls follow-igp
```

next-hop-recursion

Enables BGP recursive next-hop lookups.

Syntax

next-hop-recursion

no next-hop-recursion

Command Default

This feature is disabled.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

If the BGP next hop is not the immediate next hop, a recursive route lookup in the IP routing information base (RIB) is needed. With recursion, a second routing lookup is required to resolve the exit path for destination traffic. Use this command to enable recursive next-hop lookups.

Examples

This example enables recursive next-hop lookups for BGP4.

```
device# configure terminal
device(config)# address-family ipv4 unicast
device(config-bgp-ipv4u)# next-hop-recursion
```

This example enables recursive next-hop lookups for BGP4+.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# next-hop-recursion
```

next-hop-recursion (Policy Based Routing)

Enables recursive next-hop lookups in route maps. Available for both IPv4 and IPv6 next hop entries in the PBR route maps.

Syntax

next-hop-recursion

no next-hop-recursion

Command Default

This feature is disabled by default.

Modes

Route Map configuration mode.

Usage Guidelines

Use the **no** form of this command to restore the default.

If the next hop is not the immediate next hop, a recursive route lookup in the routing information base (RIB) is needed. With recursion, a second routing lookup is required to resolve the exit path for destination traffic. Use this command to enable recursive next-hop lookups for PBR.

Examples

This example enables recursive next-hop lookups for PBR where the configured next hop is IPv4.

```
SLX# configure terminal
SLX (config)# route-map r999 permit 10
SLX (config-route-map-r999/permit/10)# match ip address acl test1
SLX (config-route-map-r999/permit/10)# set ip next-hop 10.10.10.11
SLX (config-route-map-r999/permit/10)# next-hop-recursion
SLX (config-route-map-r999/permit/10)# exit
SLX (config)# exit
SLX# show running-config route-map
route-map r999 permit 10
   match ip address acl test1
   next-hop-recursion
   set ip next-hop 10.10.10.11
!
```

This example enables recursive next-hop lookups for PBR where the configured next hop is IPv6.

```
SLX# configure terminal
SLX (config)# route-map r999 permit 10
SLX (config-route-map-r999/permit/10)# match ipv6 address acl test1
SLX (config-route-map-r999/permit/10)# set ipv6 next-hop 2001:db8:0:0:0:ff00:42:1111
```

```
SLX (config-route-map-r999/permit/10)# next-hop-recursion
SLX (config-route-map-r999/permit/10)# exit
SLX (config)# exit
SLX# show running-config route-map
route-map r999 permit 10
    match ipv6 address acl test1
    next-hop-recursion
    set ipv6 next-hop 2001:db8:0:0:0:ff00:42:1111
    !
```

no debug

Disables the debug process for the selected module or all modules.

Syntax

no debug { **all** | **arp** | **bfd** | **dhcp** | **dot1x** | **endpoint-tracking** | **icmp** | **ip** | **ipv6** | **lacp** | **link-oam** | **lldp** | **mpls** | **sflow** | **spanning-tree** | **udld** | **vrrp**}

Parameters

all

Disables the debug on all modules for which it is enabled.

arp

Disables the Address Resolution Protocol packet debug.

bfd

Disables the Bidirectional Forwarding Detection debug.

dhcp

Disables the Dynamic Host Configuration Protocol packet debug.

dot1x

Disables the IEEE 802.1x port-based access control debug.

endpoint-tracking

Disables the endpoint tracking debug.

icmp

Disables the Internet Control Message Protocol packet debug.

ip

Disables the IPv4 packet debug.

ipv6

Disables the IPv6 packet debug.

lacp

Disables the Link Aggregation Control Protocol debug.

link-oam

Disables the link OAM debug.

lldp

Disables the Link Layer Discovery Protocol debug.

mpls

Disables the Multiprotocol Label Switching debug.

sflow

Disables sFlow (sampled flow) debug.

spanning-tree

Disables the Spanning-Tree Protocol debug.

udld

Disables the Unidirectional Link Detection debug.

vrrp

Disables the VRRP debug.

Modes

Privileged EXEC mode

Examples

This example disables the debug for VRRP.

```
no debug vrrp
```

This example disables debug on all modules for which it is enabled.

```
no debug all
```

no-core-isolation

By default, the core isolation feature is enabled. When all the core interfaces between the Leaf and Spine nodes go down, the ESI interface will be made down. If the core isolation feature is disabled using this command, the ESI interface will not be made down, and then all the core interfaces between the Leaf and the Spine nodes go down.

Syntax

no-core-isolation

Command Default

Parameter descriptions - no-core-isolation – It disables core isolation functionality.

Modes

EVPN mode.

Usage Guidelines

By default, the core isolation feature is enabled. When all the core interfaces between the Leaf and Spine nodes go down, the ESI interface will be made down. If the core isolation feature is disabled using this command, the ESI interface will not be made down, and then all the core interfaces between the Leaf and the Spine nodes go down.

Examples

The following example enables the no-core-isolation and disables the core isolation functionality.

```
SLX(config)# evpn default
SLX(config-evpn-default)# no-core-isolation
```

node

Penalizes all links originating from the node IP address.

Syntax

node *ip_addr*

no node *ip_addr*

Command Default

The command is disabled by default.

Parameters

ip_addr

All links that originate from the specified IP address are penilized.

Modes

MPLS CSPF-group configuration mode.

Usage Guidelines

The **no** form of the command disables the configuration.

MPLS iis supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The example below configures a fate sharing group and specifies node 10.1.1.1 as the penalizing IP address.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# cspf-group computation-mode add-penalty
device(config-router-mpls-policy)# exit
device(config-router-mpls)# cspf-group group3
device(config-router-mpls-cspf-group-group3)# penalty 100
device(config-router-mpls-cspf-group-group3)# from 10.1.1.1
device(config-router-mpls-cspf-group-group3)# link 10.1.1.1 10.1.1.2
device(config-router-mpls-cspf-group-group3)# subnet 10.1.2.0/24
device(config-router-mpls-cspf-group-group3)# node 10.1.1.1
```

non-revertive-mode

Sets non-revertive mode for Ethernet Ring Protection (ERP).

Syntax

non-revertive-mode

no non-revertive-mode

Command Default

Non-revertive mode is not set by default.

Modes

ERP configuration mode

Usage Guidelines

After the Ethernet Ring enters a protected state, if you do not want the topology to return to the original state (even after the failure has cleared) you can use the **non-revertive-mode** command. Run this command on the RPL owner only, and then run the **enable** command.

This command is allowed only on the RPL-owner node. An error message is issued if it is executed on another node.

Use the **no** form of this command to return the default.

Examples

The following example configures non-revertive mode and enables the configuration.

```
device# configure terminal
device(config)# erp 1
device(config-erp-1)# non-revertive-mode
device(config-erp-1)# enable
```

nonstop-routing (IS-IS)

Enables nonstop routing (NSR) for Intermediate System-to-Intermediate System (IS-IS).

Syntax

nonstop-routing

no nonstop-routing

Command Default

Enabled

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command disables nonstop routing.

Examples

The following example enables NSR for IS-IS on a device.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# nonstop-routing
```

The following example disables NSR for IS-IS on a device.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no nonstop-routing
```

nonstop-routing (OSPF)

Enables nonstop routing (NSR) for OSPF.

Syntax

nonstop-routing

no nonstop-routing

Command Default

Enabled.

Modes

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The **no** form of the command disables non-stop routing.

Examples

The following example re-enables NSR on a device.

```
device# configuration terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# nonstop-routing
```

notification-timer

Sets the length of the EOL notification timer for LDP-IGP synchronization.

Syntax

notification-timer *milliseconds*

no notification-timer *milliseconds*

Command Default

The default value is 60000 milliseconds.

Parameters

milliseconds

Specifies the length of the EOL notification timer in milliseconds. Enter an integer from 100 to 120000.

Modes

MPLS LDP end-of-lib (eol) configuration mode

Usage Guidelines

Use the **no** form of the command to reset the default value.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures the EOL notification timer to 80000 milliseconds.

```
device(config)# router mpls
device(config-mpls)# ldp
device(config-mpls-ldp)# end-of-lib
device(config-mpls-ldp-eol)# notification-timer 80000

device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# eol
device(config-router-mpls-ldp-eol)# notification-timer 80000
```

ntp authenticate

This command enables or disables the NTP authentication at global level. If the authentication is enabled, the NTP packets from servers, peers, clients not having MAC is dropped. Only those servers/peers configured with key authentication is considered for time synchronization. Client requests only with authentication is served, whose key-IDs match with one of the trusted key-IDs.

Syntax

ntp authenticate

no ntp authenticate

Command Default

By default the authentication is disabled.

Modes

Global configuration mode

Usage Guidelines

The no form of **ntp authenticate** disables the NTP authentication.

Examples

```
device(config)# ntp authenticate
```

ntp authentication-key

Creates an authentication key to associate with the NTP server, thereby enabling NTP authentication.

Syntax

ntp authentication-key *key-id* {**md5** | **sha1** }*key-string*

no ntp authentication-key *key-id*

Command Default

By default the authentication keys are not configured.

Parameters

key-id

Specifies an ID for an authentication key. The range is from 1 through 65534.

md5

The MD5 encryption.

sha1

The SHA1 encryption.

key-string

Specifies a key string. The string can be a maximum of 15 ASCII characters.

Modes

Global configuration mode

Usage Guidelines

This command adds an NTP authentication key to a list of authentication keys in the database. The key is shared by the client (device) and an external NTP server.

The maximum number of configurable NTP authentication keys is five. You cannot configure a duplicate key ID with a different key string. Use the **no ntp authentication-key** *key-id* command to remove the specified authentication key.

Authentication key must be created before associating the key with any server. Refer to the **ntp server** command for information on how to create this association.

Before downgrading the firmware to a version that does not support the encryption-level option, the encryption-level should be set to 0.

Examples

To create an authentication key with an ID of 33, an MD5 string called *check*, and an encryption level of 0 :

```
device# configure
device(config)# ntp authentication-key 33 md5 check encryption-level 0
```

ntp disable

Disables the NTP server/client mode. Disabling the NTP server/client mode does not remove the configuration.

Syntax

ntp disable { **ntp disable**} [**serve**]

no ntp disable*serve*

Command Default

By default, the NTP is enabled.

Parameters

serve

If this keyword is specified, then NTP will not serve the time to downstream devices. This keyword disables the NTP server mode functionalities.If this keyword is not specified, then both NTP client mode and NTP server mode functionalities will be disabled.

Modes

Global configuration mode

Examples

Use no to disable NTP server and client mode.

```
Disable NTP server and client mode:
 device(config)# ntp disable
Disable NTP client mode:
 device(config)# ntp disable serve
```

ntp peer

Configures the NTP peers and specifies the peers to synchronize the system clock. A maximum of 8 NTP peers can be configured.

Syntax

ntp peer {*ip_address* } [**key** *key_id*] [**maxpoll** *interval*] [**minpoll** *interval*] [**use-vrf***vrf_name*] [**version** *3* | *4*]

no ntp peer{*ip_address* }

Command Default

No default peers are configured.

Parameters

ip_address

Specifies the IPv4 or IPv6 address of the NTP peer.

key *key_id*

Specifies the symmetric key ID. By default, no symmetric key is configured. The range is 1 to 65,534.

maxpoll *interval*

Specifies the longest polling interval. The range is 4 to 17. Default is 10. The interval argument is power of 2, for example: 3=8s, 4=16s, 5=32s, 6=64s, 7=128s, 8=256s, 9=512s.

minpoll *interval*

Specifies the shortest polling interval. The range is 4 to 17. The default is 6. The interval argument is power of 2, for example: 3=8s, 4=16s, 5=32s, 6=64s, 7=128s, 8=256s, 9=512s.

use-vrf*vrf_name*

Specifies the VRF name to synchronize the time with server. The default is **mgmt-vrf**.

version *3* | *4*

Specifies the NTP version supported by the peer. The default is 4.

Modes

Global configuration mode

Usage Guidelines

This command is not effective if the NTP is enabled in client-only mode. If the peer is already mobilized as symmetric passive, then configuring statically will not be effective.

The **no** form of the command removes the peer configuration and applied options.

Examples

Configures the NTP peers and specify the peers to synchronize the system clock.

```
device(config)# ntp peer 1.2.3.4
device(config-peer-1.2.3.4/mgmt-vrf)# key 1 maxpoll 9 minpoll 7 version 3
```

The following error message is displayed when the minimum poll value is greater than maximum poll value: `Minimum poll interval cannot be greater than maximum poll interval`.

ntp server

Specifies or adds an NTP server IP address and optionally associates an authentication key to the server.

Syntax

ntp server {*ip_address* } [**source-interface-type** {**ethernet** *source-interface-number* | **loopback** *source-interface-number* | **management** *source-interface-number*| **ve** *source-interface-number* }][**key** *key_id*] [**maxpoll** *interval*] [**minpoll** *interval*] [**use-vrf** *vrf_name*] [**version** *3* | *4*]

no ntp server {*ip_address* }

Command Default

No default peer is configured.

Parameters

ip_address

Specifies the IPv4 or IPv6 address of the NTP peer.

source-interface-type

Specifies the type of interface.

ethernet

Specifies an Ethernet interface as the source type.

loopback

Specifies a loopback interface as the source type.

management

Specifies a management interface as the source type.

ve

Specifies a VE as the source type.

source-interface-number

Specifies the interface number. Valid values range from 1 through 4096.

key *key_id*

Specifies the symmetric key ID. By default, no symmetric key is configured. The range is 1 to 65,534.

maxpoll *interval*

Specifies the longest polling interval. The range is 4 to 17. Default is 10. The interval argument is power of 2, for example: 3=8s, 4=16s, 5=32s, 6=64s, 7=128s, 8=256s, 9=512s.

minpoll *interval*

Specifies the shortest polling interval. The range is 4 to 17. The default is 6. The interval argument is power of 2, for example: 3=8s, 4=16s, 5=32s, 6=64s, 7=128s, 8=256s, 9=512s.

use-vrf*vrf_name*

Specifies the VRF name to synchronize the time with server. The default is **mgmt-vrf**.

version *3* | *4*

Specifies the NTP version supported by the peer. The default is 4.

Modes

Global configuration mode

Usage Guidelines

Use this command to add an NTP server IPv4 or IPv6 address to a list of server IP addresses, or to associate an existing authentication key with an NTP server IP address.

The maximum number of NTP servers allowed is five.

Network Time Protocol (NTP) commands must be configured on each individual switch.

Use the **no ntp server** *ip-address* command to remove the specified NTP server IP address. Removing the current active NTP server resets the NTPstatus to "LOCL" until a new, active server is selected.

Use the **no ntp server** *ip-address* **key** *key-id* command to remove the key from the specified NTP IP address.

By default, all management services are enabled on the management VRF ("mgmt-vrf") and the default VRF ("default-vrf").

Examples

This example associates a configured key ID of 15 to an NTP server on the management VRF.

```
device(config)# ntp peer 1.2.3.4
device(config-server-1.2.3.4/mgmt-vrf)# key 15
```

ntp trusted-key

This command configures additional subset of trusted key-IDs which can be used for NTP and client authentication. The keys configured for server/peer is implicitly considered as part of trusted keys.

Syntax

ntp trusted-key [*key-id-1 key-id-2key-id-n*]

no ntp trusted-key

Command Default

By default the trusted key-IDs are not configured.

Parameters

key-id-1key-id-2key-id-n

List of authentication keys.

Modes

Global configuration mode

Usage Guidelines

A key must be configured as an authentication key before you can use it as a trusted key.

The **no** form of the command clears a configured key-ID from the trusted key list.

Examples

This command configures an additional subset of trusted key-IDs.

```
device(config)# ntp trusted-key 1 5 15
 device(config)# no ntp trusted-key 15
```

operational-state

Enables or disables support for OpenConfig Telemetry Support for SLX.

Syntax

operational-state syncup enable { *all* | *interface* | *bgp* | *platform* }

Parameters

all

Indicates that OpenConfig Telemetry support must be enabled on all supported modules.

interface

Indicates that OpenConfig Telemetry Support is only to be enabled for the *Interface* module.

bgp

Indicates that OpenConfig Telemetry Support is only to be enabled for the *BGP* module.

platform

Indicates that OpenConfig Telemetry Support is only to be enabled for the *Platform* module.

Modes

Configuration Mode

Usage Guidelines

Examples

The following command lists the options available for the command.

```
SLX (config)# operational-state syncup enable ?
Possible completions:
    All         Enable oper db syncup for all modules
    Bgp         Enable oper db syncup for bgp
    Interface   Enable oper db syncup for interface
    Platform    Enable platform specific oper db syncup

SLX (config)#
```

The following example enables OpenConfig Telemetry Support for the BGP module.

```
SLX (config)# operational-state syncup enable bgp
SLX (config)#
```

optimized replication

Enables optimized replication.

Syntax

optimized replication

no optimized replication

Modes

Global configuration mode

Usage Guidelines

no optimized-replication removes the entire mode and disables all underlay groups.

The default mdt group needs to be configured first and removed last in the optimized-replication mode.

When all vlans are removed from a group and the group config is removed. The same rule applies to BDs as well.

The **no underlay-mdt-group GROUP vlan add VLAN-RANGE** command can be used to remove a config if there is an exact match with the current config line or the remove option is used to remove vlans or BDs from a group.

Examples

```
overlay-gateway 10
type layer2-extension
optimized-replication
underlay-mdt-default-group 239.0.0.100 ! default MDT for all VNIs
underlay-mdt-group 239.0.0.1 vlan add 10-12,20 ! shared MDT; but not the default
underlay-mdt-group 239.0.0.3 vlan add 30 ! MDT dedicated to vlan 30
underlay-mdt-group 239.0.0.4 vlan add 40
underlay-mdt-group 239.0.0.5 bridge-domain add 50,60-70
```

oscmd

Runs commands or scripts supported by the Linux OS directly from the SLX-OS CLI.

Syntax

oscmd { *Linux-command* | *script-name* }

Parameters

Linux-command

Specifies the Linux command that you want to run.

script-name

Specifies the script that you want to run.

Modes

Privileged EXEC mode

Usage Guidelines

This command is only available for users with admin-level permissions.

All scripts run under **oscmd** must have execute permission.

After writing and testing a user-defined script file, you can copy it to the SLX-OS device. Imported scripts are stored in the `/var/config/vcs/scripts` directory.

You can also create scripts from the Linux shell using the "vi" editor. The newly-created scripts must exist in the `/fabos/users/admin` directory.

Although as an SLX-OS admin you have permissions to run the following commands from the Linux shell, you do not have permissions to run them—from the SLX-OS CLI—appended to the **oscmd** command.

- **bash**
- **script**
- **vi**
- **vim**

Examples

In the following example, the Linux **ps -ef** command lists the process status from the CLI.

```
device#  oscmd ps -ef
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 Jul24 ?        00:00:04 /sbin/init
root         2     0  0 Jul24 ?        00:00:00 [kthreadd]
```

```
root         3     2  0 Jul24 ?        00:00:00 [migration/0]
root         4     2  0 Jul24 ?        00:00:03 [ksoftirqd/0]
root         5     2  0 Jul24 ?        00:00:00 [migration/1]
root         6     2  0 Jul24 ?        00:00:03 [ksoftirqd/1]
root         7     2  0 Jul24 ?        00:00:00 [migration/2]
root         8     2  0 Jul24 ?        00:00:02 [ksoftirqd/2]
root         9     2  0 Jul24 ?        00:00:00 [migration/3]
root        10     2  0 Jul24 ?        00:00:02 [ksoftirqd/3]
root        11     2  0 Jul24 ?        00:00:00 [migration/4]
root        12     2  0 Jul24 ?        00:00:02 [ksoftirqd/4]
root        13     2  0 Jul24 ?        00:00:00 [migration/5]
root        14     2  0 Jul24 ?        00:00:03 [ksoftirqd/5]
root        27     2  0 Jul24 ?        00:00:00 [cpuset]
root        28     2  0 Jul24 ?        00:00:01 [khelper]
root        31     2  0 Jul24 ?        00:00:00 [netns]
root        34     2  0 Jul24 ?        00:00:00 [async/mgr]
root       270     2  0 Jul24 ?        00:00:00 [sync_supers]
root       272     2  0 Jul24 ?        00:00:00 [bdi-default]

...

root      8kblockd/6]182     1  0 Jul24 ?        00:00:00 /usr/sbin/inetd
root      8237     1  0 Jul24 ?        00:00:00 /usr/sbin/sshd
admin    27536 27535  0 04:19 pts/4    00:00:00 ps -ef
```

In the following example, "my_script" is the name of a user-defined script that is downloaded by using the **copy** command or exists in the `/fabos/users/admin` directory; and is executable under the Linux OS .

```
device# oscmd my_script
```

overlay access-group

Applies an overlay ACL to an overlay-transit node.

Syntax

overlay access-group *overlay-acl-name* **in**

no overlay access-group *overlay-acl-name* **in**

Parameters

overlay-acl-name

Specifies the name of the overlay ACL.

in

Applies the ACL to incoming traffic.

Modes

Overlay-transit mode

Usage Guidelines

Overlay ACLs are not supported for SLX 9150 or SLX 9250 devices.

You can apply only one overlay ACL to an overlay-transit node.

To remove an overlay ACL from an overlay-transit node, use the **no** form of this command.

Examples

The following example applies an overlay ACL to an overlay-transit node.

```
device# configure terminal
device(config)# overlay-transit tr_name
device(config-overlay-transit-tr_name)# overlay access-group ov_trans_acl_01 in
```

The following example removes an overlay ACL from an overlay-transit node.

```
device(config-overlay-transit-vxlan1)# no overlay access-group ov_trans_acl_01 in
```

overlay access-list type vxlan extended

Creates an overlay VXLAN extended ACL for deep inspection.

Syntax

overlay access-list type vxlan extended *acl-name*

no overlay access-list type vxlan extended *acl-name*

Command Default

No overlay VXLAN extended ACL is defined.

Parameters

acl-name

Specifies the overlay ACL name.

Modes

Global configuration mode

Usage Guidelines

Overlay ACLs are not supported for SLX 9150 or SLX 9250 devices.

Extended ACLs enable you to configure VXLAN tunnel endpoints (VTEP source and destination IP), VNI and VNI IP range, inner source and destination IP and networks, and inner source and destination ports.

To delete an overlay VXLAN extended ACL, use the **no** form of this command .

Examples

The following example creates an overlay VXLAN extended ACL and then defines a permit rule.

```
device# configure terminal
device(config)# overlay access-list type vxlan extended ovr_vxl_ext
device(conf-overlayacl-ext-vxlan)# seq 10 permit dst-vtep-ip any src-vtep-ip 20.1.1.100
vni 50 native tag none dst-ip 100.1.1.1 src-ip any dst-port 5555 src-port 6666 count
mirror ethernet 1/4
```

overlay access-list type vxlan standard

Creates an overlay VXLAN standard ACL.

Syntax

overlay access-list type vxlan standard *acl-name*

no overlay access-list type vxlan standard *acl-name*

Command Default

No overlay VXLAN standard ACL is defined.

Parameters

acl-name

Specifies the overlay ACL name.

Modes

Global configuration mode

Usage Guidelines

Overlay ACLs are not supported for SLX 9150 or SLX 9250 devices.

Enables configuring only the VXLAN tunnel endpoint (VTEP) IP address and VXLAN Network Identifier (VNI) to match.

To delete an overlay VXLAN standard ACL, use the **no** form of this command .

Examples

The following example creates an overlay VXLAN standard ACL and then defines a permit rule.

```
device# configure terminal
device(config)# overlay access-list type vxlan standard ovr_vxl_std_01
device(conf-overlayacl-std-vxlan)# seq 10 permit dst-vtep-ip 10.1.1.100 src-vtep-ip
10.1.1.100 vni 5 count sflow
```

overlay-gateway

Creates a VXLAN overlay gateway instance and enables VXLAN overlay gateway configuration mode.

Syntax

overlay-gateway *name*

no overlay-gateway *name*

Parameters

name

Specifies a name for the VXLAN overlay gateway. Only one gateway instance can be configured. The name is an alphanumeric, 32-character-maximum string that can also contain hyphens and underscores.

Modes

Global configuration mode

Usage Guidelines

Use this command to create a VXLAN overlay gateway instance with the given name. An overlay network is a virtual network that is built on top of existing network Layer 2 and Layer 3 technologies. Setting up a gateway consists of the following:

- Configuring the source IP address
- Configuring the VLAN or bridge domain
- Mapping a bridge domain to a VNI
- Configuring MAC addresses to export to the VXLAN domain
- Enabling statistics collection for VLAN domains
- Enabling SPAN

One you create the gateway instance, you enter VXLAN overlay gateway configuration mode, where you can configure other properties for this gateway. The key commands available in this mode are summarized below:

Table 15: Key commands available in VXLAN overlay gateway configuration mode

Command	Description
activate	Activates a VXLAN overlay gateway instance.
ip interface loopback	Sets the loopback port number for the overlay gateway instance.
map bridge-domain	In a VXLAN overlay gateway configuration that uses the Layer 2 extension, maps a bridge domain with VXLAN Network Identifiers (VNIs).
map vlan	In a VXLAN overlay gateway configuration that uses Layer 2 extension, associates VLANs with VXLAN Network Identifiers (VNIs).
sflow	Enables sFlow monitoring of the tunnel endpoints for a VXLAN overlay gateway.
site	Configures a remote Layer 2 extension site in a VXLAN overlay gateway context.
type layer2-extension	Specifies that a VXLAN overlay gateway uses Layer 2 extension.

Only one VXLAN overlay gateway instance can be configured.

Use the **no overlay-gateway** command to delete the VXLAN overlay gateway instance from the cluster. All tunnels for the gateway are also deleted. There are no other **no** forms of this command.

By default, a VXLAN overlay gateway instance is inactive. To activate an instance, first configure its other properties (such as which devices it attaches to), and then enter the **activate** command.

Examples

The following example creates a VXLAN overlay gateway instance named gateway1 and accesses VXLAN overlay gateway configuration mode.

```
device# configure terminal
device(config)# overlay-gateway gateway1
device(config-overlay-gw-gateway1)#
```

overlay-service-policy

Binds an overlay policy map to an overlay gateway or overlay transit instance.

Syntax

overlay-service-policy in *policy-mapname*

no overlay-service-policy in *policy-mapname*

Command Default

No overlay policy map is bound.

Parameters

in

Specifies that the policy be applied on ingress traffic (required).

policy-mapname

Name of an overlay policer policy map.

Modes

Overlay gateway instance configuration mode

Overlay transit instance configuration mode

Usage Guidelines

This command is not supported for SLX 9150 or SLX 9250 devices.

Only ingress policies are supported.

Overlay transit instances are applicable to spine nodes only in an IP Fabric.

Use the **no** form of the command to unbind the policy.

Examples

The following example binds a policy map to an overlay gateway instance.

```
device# configure terminal
device(config)# overlay-gateway gw1
device(conf-overlay-gw-gw1)# overlay-service-policy in servicepolicy1
```

The following example binds a policy map to an overlay transit instance on a spine node.

```
device# configure terminal
device(config)# overlay-transit transit1
device(conf-overlay-transit-transit1)# overlay-service-policy in servicepolicy1
```

The following example unbinds the policy map from the above instance.

```
device# configure terminal
device(config)# overlay-transit myOTinstance
device(conf-overlay-transit-transit1)# no overlay-service-policy in servicepolicy1
```

overlay-transit

Configures an overlay transit.

Syntax

overlay-transit *overlay-transit-name*

no overlay-transit *overlay-transit-name*

Parameters

overlay-transit-name

Specifies the overlay transit name.

Modes

Global configuration mode

Usage Guidelines

This command is not supported for SLX 9150 or SLX 9250 devices.

Use the **no** form of this command to delete the overlay transit configuration.

Examples

The following example configures an overlay transit.

```
device# configure terminal
device(config)# overlay-transit vlx_transit
```

The following example deletes an overlay transit configuration.

```
device(config)# no overlay-transit vlx_transit
```

partial-spf-interval

Changes the partial shortest path first (PSPF) interval.

Syntax

partial-spf-interval *max-wait initial-wait second-wait*

no partial-spf-interval

Parameters

max-wait

Specifies the maximum interval in seconds between SPF recalculations. The range is from 0 through 120 seconds. The default is 5 seconds.

initial-wait

Specifies the initial SPF calculation delay in milliseconds after an LSP change. The range is from 0 through 120000 milliseconds. The default for this variable is value of the *max-wait* time.

second-wait

Indicates the hold time between the first and second SPF calculation in milliseconds. The range is from 1 through 120000 milliseconds. The default is 5000 milliseconds (5 seconds). The default for this variable is value of the *max-wait* time.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command restores the defaults.

Examples

The following example specifies that the maximum interval between SPF recalculations is 15 seconds, the initial SPF calculation delay is 10000 milliseconds, and the hold time between the first and second SPF calculation is 15000 milliseconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# partial-spf-interval 15 10000 15000
```

The following example restores the default values.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no partial-spf-interval
```

password

Command to change the password for the current user ID. This command is available under each BMC User ID configuration mode.

Syntax

password *<user-password>*

Parameters

user-password

The password to be configured for this user account.

Modes

BMC User ID mode

Usage Guidelines

The user password must meet the following criteria:

- Both lower and upper case alphabets are allowed.
- Numbers are allowed.
- The following special characters are allowed:

  [@ # $ % ^ * ( ) _ + \ - = { } [ ] | : ; " < > ? / ~ ` . ,] *
- The following special characters are NOT allowed:

  & ! '

Examples

This example configures the password for the BMC User ID 1.

```
SLX # configure terminal
SLX (config)# bmc
SLX (config-bmc)# user-id 1
SLX (config-bmc-user-1)# password ?
Description: Password for BMC user
Possible completions:
  <string>
  SLX (config-bmc-user-1)# password testing123
  SLX (config-bmc-user-1)#
  SLX (config-bmc-user-1)# do show running-config bmc
bmc
 user-id 1
  password $9$VaXhc9WCy+1IwRU2ZaS2vQ==
 !
 user-id 2
  password $9$VaXhc9WCy+1IwRU2ZaS2vQ==
 !
 user-id 3
```

```
  !
!
```

password-attributes

Configures global password attributes.

Syntax

password-attributes { [**max-logins** *maxlogins*][**max-retry** *maxretry*] [**min-length** *minlen*] [**max-logins** *maxlogin*][**history** *number*] [**repeat** *minnum*] [**sequence** *number*] [**login-notify-duration** *hours*] [**admin-lockout** | **character-restriction** { [**lower** *numlower*] [**numeric** *numdigits*] [**special-char** *numsplchars*] [**upper** *numupper*] [**force-default-password-change**][**max-password-age** *number-of-days*] }

no password-attributes { [**max-logins** *maxlogins*][**max-retry** *maxretry*] [**min-length** *minlen*] [**max-logins** *maxlogin*][**history** *number*] [**repeat** *minnum*] [**sequence** *number*] [**login-notify-duration** *hours*] [**admin-lockout** | **character-restriction** { [**lower** *numlower*] [**numeric** *numdigits*] [**special-char** *numsplchars*] [**upper** *numupper*] }] [**force-default-password-change**][**max-password-age** *number-of-days*] }

Command Default

The default for *min-length* is 8. All other defaults are 0.

Parameters

admin-lockout

Enables lockout for admin role accounts.

character-restriction

Configures the restriction on various types of characters.
lower *numlower*

Specifies the minimum number of lowercase alphabetic characters that must occur in the password. Values range from 0 through 32 characters. The default value is 0.

numeric *numdigits*

Specifies the minimum number of numeric characters that must occur in the password. Values range from 0 through 32 characters. The default is 0.

special-char *numsplchars*

Specifies the number of punctuation characters that must occur in the password. All printable, non-alphanumeric punctuation characters, except colon (:) are allowed. Values range from 0 through 32 characters. The default value is 0.

upper *numupper*

Specifies the minimum number of uppercase alphabetic characters that must occur in the password. Values range from 0 through 32 characters. The default value is 0.

max-logins *maxlogins*

Specifies the maximum number of log-in sessions for a user. Values range from 0 through 10. The default value is 0.

max-retry *maxretry*

Specifies the number of failed password log-ins permitted before a user is locked out. Values range from 0 through 16. The default value is 0.

min-length *minlen*

Specifies the minimum length of the password. Valid values range from 8 through 32 characters. The default is 8 characters.

max-logins *maxlogin*

Specifies the maximum number of log-in sessions allowed per local user. Valid values range from 0 through 10. The default is 0, representing an infinite number of log-ins.

history *number*

Specifies the number of old passwords against which a newly configured password is checked. The new password is discarded if it matches an old password. Valid values range from 0 through 10. The default is 0.

repeat *minimum*

Specifies the minimum number of consecutive repetitive characters in a newly configured password. The new password is discarded if it has consecutive repetitive characters (for example, aaa, xxx,1111). Configure 1 for disabling. The default is 1.

sequence *number*

Specifies the minimum number of consecutive sequential characters both in forward and reverse direction (for example, abc, cba) in a newly configured password. The new password is discarded if it has consecutive sequential characters (for example, abc, xyz, fedc). Configure 1 for disabling. The default is 1.

login-notify-duration *hours*

Specifies the duration in hours for which admin is notified of the number of last successful attempts. Use value 0 to disable the notification. Valid values range from is from 0 through 120. The default is 0.

force-default-password-change

Force the user to change password at first login. This is applicable to all default accounts on the system.

max-password-age *number-of-days*

Specifies the number of days after which the user is forced to change the password. The default value is zero (0) indicating that the password does not expire and need not be changed.

Modes

Global configuration mode

Usage Guidelines

To reset password attributes to their default values, run the **no** form of this command.

If you use PuTTY to open a telnet session and then close the session by closing the PuTTY window, the **max-logins** feature does not count the session as closed because the client does not send an application layer closure message to be processed by the PAM module. Therefore, if **max-logins** is enabled when you use PuTTY to open a telnet session, use the **exit** command to close the session.

The **max-logins** feature does not apply to REST log-ins and RESTCONF log-ins.

Examples

The following example configures global password attributes and verifies the configuration.

```
device#configure terminal
device(config)# password-attributes max-retry 4
device(config)# password-attributes character-restriction lower 2
device(config)# password-attributes character-restriction upper 1 numeric 1 special-char
1
device(config)# exit
device# show running-config password-attributes

password-attributes max-retry 4
password-attributes character-restriction upper 1
password-attributes character-restriction lower 2
password-attributes character-restriction numeric 1
password-attributes character-restriction special-char 1
```

The following example resets the character restriction attributes and verifies the configuration.

```
device#configure terminal
device(config)# no password-attributes character-restriction lower
device(config)# no password-attributes character-restriction upper
device(config)# exit
device# show running-config password-attributes

password-attributes max-retry 4
password-attributes character-restriction numeric 1
password-attributes character-restriction special-char 1
```

The following example clears all global password attributes.

```
device#configure terminal
device(config)# no password-attributes
device(config)# exit
device# show running-config password-attributes

% No entries found.
```

The following example sets the maximum number of retries to 3 and enables lockout policy for admin role accounts.

```
device#configure terminal
device(config)# password-attributes max-retry 3 admin-lockout
```

The following example shows the configuration to force a user to change their login password the first time they login in.

```
Enable forcing default password change:
SLX(config)# password-attributes force-default-password-change

Display password-attribute configuration:
SLX# show running-config password-attributes
password-attributes force-default-password-change
SLX#
```

The following example displays how the user can set the maximum number of days for the user account password. After the maximum no. of days have reached, the user should change the password. The default value is 0 which means, the password expiration is disabled.

```
Configure Maximum password age parameter:
SLX(config)# password-attributes max-password-age 4

Remove Maximum password age configuration:
SLX(config)# no password-attributes max-password-age

Display Maximum password age configuration:
SLX# show running-config password-attributes
password-attributes max-password-age 4
SLX#
```

password-attributes expiry-alert-level

Configures the various alert levels when a SLX-OS user account's password is set to expire.

Syntax

password-attributes expiry-alert-level { [**info** *number-of-days*] | [**minor** *number-of-days*] | [**major** *number-of-days*] | [**critical** *number-of-days*] }

[no] password-attributes expiry-alert-level { [**info** *number-of-days*] | [**minor** *number-of-days*] | [**major** *number-of-days*] | [**critical** *number-of-days*] }

Parameters

info *number-of-days*

The configuration for the first level of notification for password expiry. This is the first level of warning for password expiry. When configured, this is the earliest notification that is generated for password expiry. This alarm is generated once.

minor *number-of-days*

The configuration for the second level of notification for password expiry. This alarm is generated once.

major *number-of-days*

The configuration for the third level of notification for password expiry. This is the penultimate level notification for password expiry. This alarm is generated once.

critical *number-of-days*

The configuration for the final level of notification for password expiry. This alarm is generated once.

Command Default

There are no default configurations for these alert levels.

Modes

Global Configuration Mode

Usage Guidelines

Password expiry alerts will be only be generated if the **max-password-age** value is configured first.

This configuration is common for all user accounts.

Allowed range is 1-90 days.

On the day the password expires, an *ERROR* RASLOG is generated with the message *Event: user password expiring, Password of user account <user-account-name> is expiring today.*

The number of alert days must be configured in the decreasing order of days as follows:

info > minor > major > critical

The command will fail with the error message **%Error: Number of days for expiry-alert-level must be in the order of info > minor > major > critical** when the alert levels are not configured in the above order.

Appropriate RASLOGs will be generated once for each configured alarm level.

All alert types need not be configured. User can choose to configure one or more of these alerts. User can also choose not to configure any alerts. However, when all alerts are not configured, only one RASLOG of the type *ERROR* with the message *Event: user password expiring, Password of user account <user-account-name> is expiring today.* is generated on the day the password will expire.

This configuration is common for all user accounts. When the number of days configured for a specific alert level is reached, one alert will be generated. The alert will not be repeated.

The *no* form of this command removes the configuration. It will turn off the alert for the provided alert level(s) or all the alert levels when no parameter is provided.

Examples

The following example configures all the password expiry alarm levels.

```
SLX # configure terminal
SLX (config)# password-attributes expiry-alert-level info 30 minor 20 major 10 critical 2
SLX (config)#
SLX (config)# do show running-config password-attributes
password-attributes min-length 9
password-attributes max-logins 2
password-attributes max-retry 2
password-attributes max-lockout-duration 1
password-attributes history 1
password-attributes repeat 2
password-attributes sequence 2
password-attributes force-default-password-change
password-attributes max-password-age 10
password-attributes character-restriction upper 1
password-attributes character-restriction lower 1
password-attributes character-restriction numeric 1
password-attributes character-restriction special-char 1
password-attributes admin-lockout
password-attributes login-notify-duration 1
password-attributes expiry-alert-level info 30 minor 20 major 10 critical 2
SLX (config)#
```

The following example changes the *info* alarm's number of days to 25 days.

```
SLX# configure terminal
SLX (config)# password-attributes expiry-alert-level info 25
SLX (config)#
SLX (config)# do show running-config password-attributes
password-attributes min-length 9
password-attributes max-logins 2
password-attributes max-retry 2
password-attributes max-lockout-duration 1
password-attributes history 1
password-attributes repeat 2
password-attributes sequence 2
password-attributes force-default-password-change
password-attributes max-password-age 10
password-attributes character-restriction upper 1
password-attributes character-restriction lower 1
password-attributes character-restriction numeric 1
password-attributes character-restriction special-char 1
password-attributes admin-lockout
password-attributes login-notify-duration 1
password-attributes expiry-alert-level info 25 minor 20 major 10 critical 2
SLX (config)#
```

The following example removes the configuration for password expiry alert of the level *info*.

```
SLX# configure terminal
SLX (config)# no password-attributes expiry-alert-level info
SLX (config)#
SLX (config)# do show running-config password-attributes
password-attributes min-length 9
password-attributes max-logins 2
password-attributes max-retry 2
password-attributes max-lockout-duration 1
password-attributes history 1
password-attributes repeat 2
password-attributes sequence 2
password-attributes force-default-password-change
password-attributes max-password-age 10
password-attributes character-restriction upper 1
password-attributes character-restriction lower 1
password-attributes character-restriction numeric 1
password-attributes character-restriction special-char 1
password-attributes admin-lockout
password-attributes login-notify-duration 1
password-attributes expiry-alert-level minor 20 major 10 critical 2
SLX (config)#
```

password-encryption convert-enc-to-level-10

Changes existing AES-256 encrypted passwords and MD5 passwords to SHA-512 .

Syntax

password-encryption convert-enc-to-level-10

Command Default

By default, passwords from previous releases have the encryption with which they were configured.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to convert all existing passwords to make them more secure in SLX-OS 20.1.1 or later. Any clear-text (enc-level 0) passwords are retained in the configuration database and not converted to SHA-512.

This command is available only to administrative users.

If you downgrade to a release earlier than SLX-OS 20.1.1, all MD5 passwords that were converted to SHA-512 will not be available.

Examples

The following example shows the warning and the prompt before passwords are converted.

```
device# password-encryption convert-enc-to-level-10
%WARN: This operation will convert all existing user passwords to SHA-512 format.
However, the enc level 0 (clear-text) passwords, if any, will be retained as is
in the configuration database. These configurations will be lost if the system is
downgraded to lower releases than SLX 20.1.1.
Do you want to continue? [y/n]y
All passwords are converted successfully.
```

The following example shows the warning when a configuration rollback is in progress.

```
device# password-encryption convert-enc-to-level-10
%WARN:This operation will convert all existing user passwords to SHA-512 format.
However, the enc level 0 (clear-text) passwords, if any, will be retained as is
in the configuration database. These configurations will be lost if the system is
downgraded to lower releases than SLX 20.1.1.
Do you want to continue? [Y/N]y
%%ERROR: Password conversion is not allowed when configuration rollback session
is in progress; Please try again later.
```

password-policy (TPVM mode)

Command to configure the password length and other password strength restrictions for the TPVM password. This command is available under TPVM configuration mode.

Syntax

password-policy { **character-restriction** | **min-len** }

password-policy min-len *<minimum-password-length>*

password-policy character-restriction [**lower** *<number-of-lower-case-alphabets>* | **numeric** *<number-of-numeric-characters>* | **special-char** *<number-of-special-characters>* | **upper** *<number-of-upper-case-alphabets>*]

no password-policy min-len

no password-policy character-restriction [**lower** | **numeric** | **special-char** | **upper**]

Parameters

min-len *minimum-password-length*

Sets the minimum password length for the TPVM account. The password can be between 8 and 40 characters long. The default minimum password length is 8 characters.

character-restriction lower *number-of-lower-case-alphabets*

Sets the minimum number of lower case alphabets that need to be present in the password. The range is 0 to 40 characters.

character-restriction numeric *number-of-numeric-characters*

Sets the minimum number of numeric characters that need to be present in the password. The range is 0 to 40 numbers.

character-restriction special-char *number-of-special-characters*

Sets the minimum number of special characters that need to be present in the password. The range is 0 to 40 special characters.

character-restriction upper *number-of-upper-case-alphabets*

Sets the minimum number of upper case alphabets that need to be present in the password. The range is 0 to 40 upper case characters.

Modes

TPVM mode

Usage Guidelines

- The TPVM password must be between 8 and 40 characters long. This length is controlled by the *min-len* configuration.
- Both lower and upper case alphabets are allowed.
- Numbers are allowed.
- The following special characters are allowed:

  [@ # $ % ^ * ( ) _ + - = { } [ ] | : ; " < > ? / ~ ` . ,] *
- The following special characters are NOT allowed:

  & ! ' \

Examples

This example shows how to configure the TPVM password strength with length 12, minimum of 3 lowercase, 3 lower case, 2 numbers, 1 special characters.

```
SLX # configure terminal
SLX (config)# tpvm
SLX (config-tpvm-TPVM)# password-policy min-len 12
SLX (config-tpvm-TPVM)# password-policy character-restriction lower 3
SLX (config-tpvm-TPVM)# password-policy character-restriction upper 3
SLX (config-tpvm-TPVM)# password-policy character-restriction numeric 2
SLX (config-tpvm-TPVM)# password-policy character-restriction special-char 1
```

This example shows how to remove a restriction imposed on the TPVM password strength. Here the minimum restriction of 1 special character is being removed

```
SLX # configure terminal
SLX (config)# tpvm
SLX (config-tpvm-TPVM)# no password-policy character-restriction special-char
```

path

A path is a list of router hops that specifies a route across an MPLS domain. Once the user creates a path, the user can create signaled LSPs that see the path.

Syntax

path *path_name* [**hop** *ip_addr*] | [[**insert** *ip_addr*] [[**loose** | **strict**] *ip_addr*]

no path { *path_name* } [**hop** *ip_addr*] | [[**insert** *ip_addr*] [[**loose** | **strict**] *ip_addr*]

Command Default

No paths are modified by default.

Parameters

path_name

Specifies the selected path name.

hop *ip_addr*

Configures the specified the strict or loose hop.

insert *ip_addr*

Specifies the inserted path strict or loose hop.

loose *ip_addr*

There can be other routers in between.

strict *ip_addr*

The router must be directly connected to the preceding node.

Modes

MPLS path mode (config-router-mpls-path-*name*).

Usage Guidelines

The no form of the command removes the specified path.

A path is always configured at the ingress LER and assumes that the ingress LER is the beginning of the path. A path can contain any number of nodes, which correspond to MPLS-enabled routers in the network.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only..

Examples

The following example configures a path called sf_to_sj that has four nodes.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# path sf_to_sj
device(config-router-mpls-path-sf_to_sj)# hop 2.3.4.5 strict
device(config-router-mpls-path-sf_to_sj)# hop 1.2.3.4 strict
device(config-router-mpls-path-sf_to_sj)# exit
```

pdu-rate

Configures pdu-rate value, which is the number of OAMPDUs per second.

Syntax

pdu-rate *rate*

Command Default

The default value is 1.

Parameters

rate

Specifies the pdu rate per second.

Modes

Link OAM configuration mode

Usage Guidelines

The range is from 1 through 10. Configure the timeout interval at least three times the pdu interval to avoid Link OAM protocol flaps against loss of one or two PDUs for any latency issues.

Examples

```
(config-link-oam)# pdu-rate 10
```

peer

Configures a peer IP address in a bridge domain. A corresponding pseudowire (PW) interface is created when the peer IP address is configured.

Syntax

peer *ip-address* [**control-word**] [**cos** *num*] [**flow-label**] [**load-balance**] [**lsp** *lsp-name1*, *lsp-name2*, . . . *lsp-name32*]

no peer [*ip-address* [**lsp** *lsp-name1*, *lsp-name2*, . . . *lsp-name32*]]

Command Default

No PW interfaces are configured.

Parameters

ip-address

A PW IP address for a remote peer.

control-word

Enables control word for routing of pseudowire (PW) traffic to the peer.

cos *num*

Specifies a Class of Service (CoS) value for selecting a label-switched path to reach the peer. The value ranges is from 0 through 7.

flow-label

Enables flow label to support PW load balancing.

load-balance

Specifies load balancing. As many as16 alternate paths are used for load balancing.

lsp *lsp-name1*, *lsp-name2*, . . . *lsp-name32*

Specifies the name of a label-switched path. As many as 32 label-switched path names can be configured.

Modes

Bridge-domain configuration mode.

Usage Guidelines

The virtual connection identifier (VC ID) must be configured by using the **vc-id** command prior to configuring the peer IP address to create a PW interface.

The **no** form of the command deletes the peer IP address configuration and the PW interface that corresponds to the specified peer IP address.

The following are examples of configuration combinations that are allowed:

- **peer** *ip-address* **control-word**
- **peer** *ip-address* **cos** *num*
- **peer** *ip-address* **flow-label**
- **peer** *ip-address* **load-balance**
- **peer** *ip-address* **control-word flow-label**
- **peer** *ip-address* **control-word cos** *num* **flow-label**
- **peer** *ip-address* **control-word cos** *num* **flow-label load-balance**
- **peer** *ip-address* **control-word cos** *num* **flow-label**
- **peer** *ip-address* **control-word flow-label load-balance**
- **peer** *ip-address* **cos** *num* **load-balance**
- **peer** *ip-address* **cos** *num* **flow-label**
- **peer** *ip-address* **load-balance cos**
- **peer** *ip-address* **load-balance lsp** *lsp-name1, lsp-name2,...lsp-name32*
- **no peer** *ip-address*
- **no peer** *ip-address* **lsp** *lsp-name1, lsp-name2, . . . lsp-name32*

Note
When a peer is already configured, you cannot add a CoS or load balancing configuration. To configure a CoS value or load-balancing, the peer must be removed by using the **no peer** command and reconfigured by specifying the required **cos** or **load-balance** options.

To remove the CoS or load-balance configuration, the peer configuration must be removed by using the **no peer** command.

Examples

The following example shows how to configure a peer IP address (10.12.12.12) for bridge domain 1 with the **load-balance** option.

```
device# configure terminal
device(config)# bridge-domain 1
device(config-bridge-domain-1)# peer 10.12.12.12 load-balance
```

The following example shows how to configure a peer IP address (10.12.12.12) for bridge domain 1 specifying two label-switched paths (lsp1 and lsp2).

```
device# configure terminal
device(config)# bridge-domain 1
device(config-bridge-domain-1)# peer 10.12.12.12 lsp lsp1 lsp2
```

The following example shows how to configure a peer IP address (10.1.1.1) for bridge domain 1 specifying load balancing and four label-switched paths (lsp1, lsp2, lsp3 and lsp4).

```
device# configure terminal
device(config)# bridge-domain 1
device(config-bridge-domain-1)# peer 10.1.1.1 load-balance lsp lsp1 lsp2 lsp3 lsp4
```

The following example shows the error message that is displayed when you try to configure the **load-balance** option for an existing peer. The peer configuration must be removed and reconfigured to specify the **load-balance** option, as shown in the example.

```
device# configure terminal
device(config)# bridge-domain 1
device(config-bridge-domain-1)# peer 15.15.15.15
device(config-bridge-domain-1)# peer 15.15.15.15 load-balance
Error: can not configure load-balance on existing peer.
device(config-bridge-domain-1)#no peer 15.15.15.15
device(config-bridge-domain-1)# peer 15.15.15.15 load-balance
```

peer (MCT)

Configures the IP address for the MCT cluster peer.

Syntax

peer *ip-address*

no peer [*ip-address*]

Parameters

ip-address

Specifies the IP address for the cluster peer. The address is either the peer loopback address or nexthop IP address.

Modes

Cluster configuration mode.

Usage Guidelines

Configure a corresponding neighbor for the peer. If the peer is already configured as a neighbor, when you deploy and undeploy the cluster, the neighbor resets to renegotiate its capability.

If the peer already exists for other address family, clear the IP peer session.

The **no** form of the command deletes the peer IP address configuration.

Examples

The following example shows the configuring of the cluster peer IP address.

```
device(config)# cluster MCT1
device(config-cluster-MCT1)# peer 10.10.10.12
```

peer-dampening

Enables dampening of unstable BGP Peers globally for all neighbors (IPv4, IPv6 across all VRFs). Dampening can be enabled on all neighbors or on an individual neighbour/a peer-group. Dampening cannot be applied on dynamic peers.

Syntax

peer-dampening [**delay-hold** *0-65535* | **penalty** *1-65535* | **max-penalty** *1-65535* | **stability-interval** *0-65535*]

no peer-dampening [**delay-hold** | **penalty** | **max-penalty** | **stability-interval**]

Parameters

delay-hold *0-65535*

The amount of time, in seconds, that a session remains in the *idle-state* after the first peer flap event is received. During this time, all route advertisements from this peer are ignored. The default value is zero (0) seconds.

penalty *1-65535*

The amount of time, in seconds, which gets added to *idle-hold* timer every time a peer flap event is received. The default value is 300 seconds.

max-penalty *1-65535*

The maximum amount of time, in seconds, that a session remains in the *idle-*state after it has experienced repeated instability. The default value is 3600 seconds.

stability-interval *0-65535*

The interval of time, in seconds, the session must be error-free in order to consider it to be stable. The default value is 1800 seconds.

Modes

Router BGP

Usage Guidelines

- BGP peer dampening can be global or on individual neighbor/peer-group.
- All routes from a dampened peer will be removed from the routing table
- When route dampening is also configured, peer dampening will take precedence over route dampening.
- Dampening cannot be applied to dynamic peers.
- Dampening cannot be applied to administratively down neighbors.
- When downgrading to a firmware that does not support *peer-dampening*, an error will be displayed. You must remove this configuration to successfully complete the downgrade.

Examples

The following example shows how to enable peer dampening globally.

```
SLX (config)#router bgp
SLX (config-bgp-router)# peer-dampening delay-hold 10 penalty 300 max-penalty 3600
stability-interval 1800
SLX (config-bgp-router)#
```

The following example shows how to disable Peer Dampening globally for all peers.

```
SLX (config)# router bgp
SLX (config-bgp-router)# no peer-dampening
SLX (config-bgp-router)#
```

peer-group ipv6prefix-over-ipv4peer

Enables exchanging of IPv6 routes over IPv4 BGP peer sessions. This configuration applies only to BGP neighbors that are members of a peer-group.

Syntax

peer-group ipv6prefix-over-ipv4peer

[no] peer-group ipv6prefix-over-ipv4peer

Parameters

None

Modes

BGP Configuration Mode

Usage Guidelines

The *no* form of this command disables exchanging IPv6 addresses over IPv4 BGP peer sessions.

Note

When the *IPv6 address family* is already activated under a peer-group and the command **peer-group ipv6prefix-over-ipv4peer** is executed, the Neighbor NLRI Negotiation capabilities are modified from *IPv4 unicast routes* to *IPv4 and IPv6 unicast routes*. This will result in the existing BGP IPv4 connections - that are mapped to a peer-group and have IPv6 address family enabled - being reset.

This reset also happens when *IPv6 address family* is already activated under a peer-group, and CLI **peer-group ipv6prefix-over-ipv4peer** is being disabled.

Examples

The following example enables exchanging IPv6 addresses over IPv4 BGP peer sessions.

```
SLX (config)# router bgp
SLX (config-router-bgp)# peer-group ipv6prefix-over-ipv4peer
SLX (config-router-bgp)#
```

peer-interface

Configures the Ethernet interface or port-channel to reach the MCT cluster peer.

Syntax

peer-interface Ethernet *slot/port* | **port-channel** *number*

no peer-interface

Parameters

Ethernet *slot/port*

Specifies the Ethernet interface for the cluster peer.

port-channel *number*

Specifies the port-channel for the cluster peer.

Modes

Cluster configuration mode.

Usage Guidelines

The **no** form of the command deletes the peer interface configuration.

You must configure the peer interface before deploying the cluster configuration.

You cannot change the peer interface when the cluster is deployed.

Examples

The following example shows the configuring of the cluster peer interface.

```
device(config)# cluster MCT1
device(config-cluster-MCT1)# peer-interface port-channel 20
```

peer-keepalive (optional)

Configures the keepalive session for the MCT cluster peer.

Syntax

peer-keepalive { **auto** } [**destination** *IP address* |**role** *primary/secondary*]

no peer-keepalive { **auto** } [**destination** *IP address* |**role** *primary/secondary*]

Command Default

The default is `auto`.

Parameters

auto

Destination and source IP will be automatically discovered and should not be configured.

destination *ip-address* `source-interface` *interface*

Manually configures the destination and source interface. Overrides the auto discovery default.

role *primary/secondary*

Configures the role of the node if the ICL goes down, but MCT peer remains up.

Modes

Cluster configuration mode.

Usage Guidelines

`no peer-keepalive` disables keep-alive session.

The default keepalilve session uses the management VRF and runs between the management IP addresses of the MCT nodes.

The primary node is responsible for forwarding all traffic when ICL goes down.

The Secondary node brings down all client interfaces and tunnels and isolates all client traffic.

By default, the node with lower IP is selected as primary and higher IP is selected as secondary. This behavior can be changed by configuring the `role`.

Examples

The following example automatically configures the peer-keepalive default destination IP, source interface, and primary/secondary roles.

```
device(config)# cluster MCT1
device(config-cluster-MCT1)# peer-keepalive
device(config-peer-keepalive)# auto
device(config-peer-keepalive)#
```

penalty

Sets the penalty value for a CSPF fate-sharing group.

Syntax

penalty { *penalty_value* }

no penalty

Command Default

The command is disabled by default.

Parameters

penalty_value

Specifies the penalty value that is assigned to objects of the same fate-sharing group. The range is from 1 through 65535. The default value is one (1). Objects of the same fate-sharing group share the same penalty value. For example, all objects in group 3 share the same penalty value of 100.

Modes

MPLS CSPF group mode.

Usage Guidelines

The **no** form of the command disables the command..

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures the penalty value to 100.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# cspf-group group3
device(config-router-mpls-cspf-group-group3)# penalty 100
```

permit ip host

Creates a rule in an Address Resolution Protocol (ARP) ACL that permits ARP messages from a host specified by both IP and MAC addresses.

Syntax

permit ip host *sender-ip* **mac host** *sender-mac-address*

no permit ip host *sender-ip* **mac host** *sender-mac-address*

Command Default

No permit rules are defined.

Parameters

sender-ip

Specifies the sender IP address.

mac host *sender-mac-address*

Specifies the sender MAC address, in hexadecimal format.

Modes

ARP ACL configuration mode

Usage Guidelines

On untrusted interfaces of DAI-enabled VLANs, incoming ARP packets from permitted IP/MAC addresses are accepted only if all of the following steps were performed:

- Create the ACL, using the **arp access-list** command.
- In the ACL, create one or more rules, using the **permit ip host** command. Each rule specifies an IP/MAC address-pair.
- Apply the ACL to one or more VLANs, using the **ip arp inspection filter** command.
- Enable DAI on such VLANs, using the **ip arp inspection** command.

This command is also used to implement ARP Guard. ARP Guard is supported only on devices based on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command removes the permit rule from the ACL.

Examples

The following example defines a **permit ip host** rule in an ARP ACL, applies the ACL to a VLAN, and enables DAI on that VLAN.

```
device# configure terminal
device(config)# arp access-list arp_acl_1
device(config-arp-acl)# permit ip host 1.1.1.1 mac host 0020.2222.2222
device(config-arp-acl)# permit ip host 1.1.1.2 mac host 0020.2222.2223
device(config-arp-acl)# exit

device(config)# vlan 200
device(config-vlan-200)# ip arp inspection filter arp_acl_1
device(conf-vlan-200)# ip arp inspection
```

The following example creates a **permit ip host** rule within the **arp access-list** command.

```
device# configure terminal
device(config)# arp access-list host2 permit ip host 1.1.1.1 mac host 0000.0011.0022
```

The following example creates an ARP ACL, creates **permit ip host** rules within, and applies it to an interface. This is the first stage of ARP Guard implementation.

```
device# configure terminal
device(config)# arp access-list arp_acl_2
device(config-arp-acl)# permit ip host 1.1.1.1 mac host 0020.2222.2222
device(config-arp-acl)# permit ip host 1.1.1.2 mac host 0020.2222.2223
device(config-arp-acl)# exit

device(config)# interface ethernet 1/2
device(conf-if-eth-1/2)# switchport
device(conf-if-eth-1/2)# ip arp inspection filter arp_acl_2
```

Note
At this point, ARP Guard is not yet enabled. For more information, see the "ARP Guard" section of the *Extreme SLX-OS Layer 3 Routing Configuration Guide*.

ping

Verifies network connectivity between a source and a destination on a TCP/IP network.

Syntax

ping *dest-ipv4-addr* [**ipv6** *dest-ipv6-addr*] [*host-name*] [**count** [*number*] [**interface** { **Ethernet***slot/port*| **management** | **ve** *vlan_id* }]] [**timeout** *seconds*] [**datagram-size** *bytes*] [**quiet**] [**numeric**] [**vrf** { **mgmt-vrf** | **default-vrf** |*vrf-name* } }

Command Default

The default for count is 5. The default for timeout is 1. The default for datagram-size is 56.

Parameters

dest-ipv4-addr

Specifies the IPv4 address of the destination device.

ipv6 *dest-ipv6-addr*

Specifies the IPv6 address of the destination device.

host-name

Specifies the destination host name. The default value is 1.

count *number*

Specifies the number of transmissions (pings). The range is from 1 through 7200.

interface Ethernet

Represents a valid, physical Ethernet interface.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

interface management

Specifies the management interface.

interface ve *vlan_id*

Specifies the interface is a virtual Ethernet, and specifies the VLAN ID of the interface.

timeout *seconds*

Specifies the time (in seconds) to wait for a response. The range is from 1 through 60. The default value is 1.

Note
This option applies only to IPv4.

datagram-size *bytes*

Specifies the datagram size (also known as the maximum transmission unit, or MTU) in bytes. The range is from 36 through 9100. The default value is 56.

quiet

Prints only the first and last line of the command output.

numeric

Does not look up host names.

vrf

Pings the specified VRF instance.

mgmt-vrf

Specifies the management VRF.

default-vrf

Specifies the default-vrf.

vrf-name

Specifies a VRF name.

Modes

Privileged EXEC mode

Usage Guidelines

This command sends a specified number of pings with configured parameters to the specified destination device.

Examples

This example pings an IPv4 destination address.

```
device# ping 172.16.4.80
Type Control-c to abort
PING 172.16.4.80 (172.16.4.80): 56 data bytes
64 bytes from 172.16.4.80: icmp_seq=0 ttl=120 time=101.466 ms
64 bytes from 172.16.4.80: icmp_seq=1 ttl=120 time=122.914 ms
64 bytes from 172.16.4.80: icmp_seq=2 ttl=120 time=145.637 ms
64 bytes from 172.16.4.80: icmp_seq=3 ttl=120 time=170.032 ms
64 bytes from 172.16.4.80: icmp_seq=4 ttl=120 time=103.036 ms
--- 172.16.4.80 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 101.466/128.617/170.032/26.188 ms
```

This example pings an IPv4 destination address in quiet mode.

```
device# ping 172.16.4.80 quiet
Type Control-c to abort
PING 172.16.4.80 (172.16.4.80): 56 data bytes
--- 172.16.4.80 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 100.605/146.372/192.552/32.505 ms
```

This example pings an IPv6 destination address in numeric mode with a datagram size.

```
device# ping ipv6 fec0:60:69bc:92:218:8bff:fe40:1470 count 3 datagram-size 48
numeric timeout 3
Type Control-c to abort
PING fec0:60:69bc:92:218:8bff:fe40:1470 (fec0:60:69bc:92:218:8bff:fe40:1470): 48
data bytes
56 bytes from fec0:60:69bc:92:218:8bff:fe40:1470: icmp_seq=0 ttl=64 time=6.356 ms
56 bytes from fec0:60:69bc:92:218:8bff:fe40:1470: icmp_seq=1 ttl=64 time=0.170 ms
56 bytes from fec0:60:69bc:92:218:8bff:fe40:1470: icmp_seq=2 ttl=64 time=0.171 ms
--- fec0:60:69bc:92:218:8bff:fe40:1470 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.170/2.232/6.356/2.916 ms
```

pki ocsp

Configures OCSP (Online Certificate Status Protocol) on a VRF with a source interface.

Syntax

pki ocsp [**source-interface** { **ethernet** *eth-id* | **loopback** *loopback-id* | **management** *mgmt-addr* | **ve** *ve-id* }]

no pki ocsp [**source-interface** { **ethernet** *eth-id* | **loopback** *loopback-id* | **management** *mgmt-addr* | **ve** *ve-id* }]

Command Default

By default, OCSP is not configured.

Parameters

source-interface

Indicates the type of interface to use as the source interface or address.

ethernet *eth-id*

Specifies the Ethernet interface to use as the source interface, in slot/port format (0/1).

loopback *loopback-id*

Specifies the Loopback interface to use as the source interface.

management *mgmt-addr*

Specifies the management address (active MM or chassis IP) to use as the source address.

ve *ve-id*

Specifies the VE interface to use as the source interface.

Modes

Global configuration mode

Usage Guidelines

Customers on different networks have their OCSP responder connected to the SLX device by the management IP or the in-band IP (Ethernet port). Customers prefer that all network packets originating from a specific device be traceable to a known IP address on the device from which they originate. You can use this command to configure the source interface, where a network packet from the device is sent to a server that listens for these packets.

Use the **no** form of the command to delete the OCSP configuration.

When a source interface is not specified, the default source is the IP address of the interface from which the packet egresses.

If, at run time, the source interface is not up or the IP address for the source interface was not configured, the command behaves as though the source interface was not configured.

Examples

This example configures an Ethernet interface as the source address.

```
device# configure terminal
device(config)# pki ocsp 10.1.1.100
device(config-pki-ocsp-10.1.1.100/mgmt-vrf)# source-interface ethernet 0/1
```

police cir

Configures the committed information rate, committed burst size, exceeded information rate, and the exceeded burst size for the class map.

Syntax

police cir *cir-bps* [**cbs** *bytes*] [**eir** *bps* [**ebs** *bytes*]]

no police cir [**cbs**] [**eir** [**ebs**]]

Parameters

cir-bps

Specifies the committed information rate in bits per second. Enter an integer from 0 to 300000000000.

cbs *bytes*

Specifies the committed burst size in bytes. Enter an integer from 1250 to 37500000000.

eir *bps*

Specifies the exceeded information rate in bits per second. Enter an integer from 0 to 300000000000.

ebs *bytes*

Specifies the exceeded burst size in bytes. Enter an integer from 1250 to 37500000000.

Modes

Policy-map class configuration mode

Usage Guidelines

Use the **no** version of this command to remove the parameter from the class map.

You can enter CIR and EIR values from 0 to 300000000000, but the operational values are from 22000 to 300000000000.

Only the **police cir** command is mandatory for configuring a class map.

If the optional parameters for a class map are not set, they are treated as disabled. To delete all parameters for a class-map, use the **no police** command.

If CBS and EBS values are not configured, then these values are derived from the CIR and EIR values, respectively. The burst size calculation is as follows: Burst size (CBS or EBS) = 1.2*information rate (CIR/EIR)/8.

If the configured CBS value is less than 2*(default MTU) value, then 2*(default MTU) is programmed as the CBS in the hardware. For example, if you configure CBS at 2000

bytes and the default MTU on an interface is 1548 bytes, when a policy map is applied on this interface, the CBS programmed in the hardware is 2*MTU (3096 bytes). If you update the MTU value, the CBS value is not be updated.

If the optional EIR or EBS value is not configured, it is disabled and Always Violated traffic is dropped.

To disable the learning of MAC addresses for stream matching of the ACL-based rate limiting entries, the CIR and EIR values must be 0.

The MAC address entries in the MAC-address table which are already learned will not be flushed when you configure the CIR or EIR value as 0. You must explicitly clear the entries in MAC-address table by using the **clear mac-address-table dynamic** command.

Examples

The following example sets the committed information rate (cir), committed burst size (cbs), exceeded information rate (eir), and the exceeded burst size (ebs).

```
device# configure terminal
device(config)# policy-map policy_2
device(config-policymap)# class default
device(config-policymap-class)# police cir 3000000 cbs 375000000 eir 300000000 ebs
37500000
```

policy-map

Configures a policy map containing a class map so that you can apply policer and QoS attributes to a particular interface.

Syntax

policy-map *policy-mapname*

no policy-map *policy-mapname*

Command Default

No policy map is created.

Parameters

policy-mapname

Name of police policy map

Modes

Global configuration mode

Usage Guidelines

When you launch the **policy-map** command, the system is placed in `config-policymap mode` for the configured map. At this point, you can add a class map containing policing parameters to the policy map. (Refer to the description of the **class** command.)

This command creates a policer policy map to apply policer and QoS attributes to a particular interface. Each policy map can contain up to 32 class maps. The class map can be associated with specific policing and QoS parameters.

Maximum number of policy map creations are 128

Associate the policy map to the interface for inbound or outbound direction with the **service-policy** command.

Enter **no policy-map** *policy-mapname* while in global configuration mode to remove the policy map.

Examples

Create a policy map and place system into config-policymap mode so that you can add a class map.

```
device# configure terminal
```

```
device(config)# policy-map policymap1
device(config-policymap)#
```

Remove the policy map while in global configuration mode.

```
device# configure terminal
device(config)# no policy-map policymap1
```

port-channel path-cost

Sets the port channel path cost behavior.

Syntax

port-channel path-cost [**custom** | **standard**]

Command Default

Path cost is standard.

Parameters

custom

Specifies to use the custom behavior, which sets the path cost changes according to the port-channel's bandwidth.

standard

Specifies to use the standard behavior, which sets that the path cost does not change according to port-channel's bandwidth.

Modes

Spanning tree configuration mode

Examples

To set the behavior for the path cost to custom:

```
device# configure terminal
device(config)# protocol spanning-tree stp
device(conf-stp)# port-channel path-cost custom

device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# port-channel path-cost custom

device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# port-channel path-cost custom

device# configure terminal
device(config)# protocol spanning-tree pvst
device(conf-pvst)# port-channel path-cost custom

device# configure terminal
device(config)# protocol spanning-tree rpvst
device(conf-rpvst)# port-channel path-cost custom
```

To set the behavior for the path cost to standard:

```
device# configure terminal
```

```
device(config)# protocol spanning-tree stp
device(conf-stp)# port-channel path-cost standard

device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# port-channel path-cost standard

device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# port-channel path-cost standard

device# configure terminal
device(config)# protocol spanning-tree pvst
device(conf-pvst)# port-channel path-cost standard

device# configure terminal
device(config)# protocol spanning-tree rpvst
device(conf-rpvst)# port-channel path-cost standard
```

preempt-mode

Enables or disables preempt mode for a VRRP or VRRP Extended (VRRP-E) router session.

Syntax

preempt-mode

no preempt-mode

Command Default

Enabled for VRRP; Disabled for VRRP-E.

Modes

Virtual-router-group configuration mode

Virtual-router-extended-group configuration mode

Usage Guidelines

This command is for VRRP and VRRP-E.

For VRRP-E, the interface must be a virtual interface (Ve).

When set, the highest-priority backup router will always be the master if the owner is not available. If not set, a higher priority backup will not preempt a lower-priority master.

Enter **no preempt-mode** to turn off preempt mode.

Examples

To turn on preempt mode for a virtual-router-group 1 session:

```
device# configure terminal
device(config)# ipv6 protocol vrrp-extended
device(config)# interface ve 10
device(config-if-Ve-10)# ipv6 vrrp-extended-group 1
device(config-vrrp-extended-group-1)# preempt-mode
```

prefix-independent-convergence

Configures BGP Prefix-Independent Convergence (PIC), providing a BGP next-hop and additional paths to the routing information base manager (RIBM) and forwarding information base (FIB) if applicable.

Syntax

prefix-independent-convergence

no prefix-independent-convergence

Command Default

This feature is disabled by default.

Modes

Global configuration mode

Usage Guidelines

Use the **show running-config** command to confirm the configuration. Backup paths are not displayed in the output.

Use the **no** form of this command to disable BGP PIC.

After enabling and disabling BGP PIC, use the **clear ip bgp neighbor** command to clear the configuration.

Examples

The following example configures BGP PIC.

```
device# configure terminal
device(config)# prefix-independent-convergence
```

prefix-independent-convergence-static

This command reduces the convergence time for the static routes when a failover from the primary static nexthop to the backup static nexthop happens.

Syntax

prefix-independent-convergence-static

[no] prefix-independent-convergence-static

Command Default

Static Prefix Independent Convergence (Static PIC) is not enabled by default.

Modes

Global configuration mode

Usage Guidelines

When static PIC is enabled, both primary and backup next-hop static routes are downloaded to the device. When static PIC is not enabled, only the primary next-hop static route is downloaded.

You must run the **clear ip route all vrf <vrf-name>** or the IPv6 version of the command when changing static PIC configuration.

Examples

This example configures static PIC.

```
SLX(config)# prefix-independent-convergence-static

%Warning: Please run "clear ip[v6] route all vrf <vrf name>" for all static routes
configured in VRFs
```

This examples removes the configuration of static PIC.

```
SLX (config)# no prefix-independent-convergence-static
```

primary-path

Configures an explicit path for the bypass LSP or dynamic bypass LSP.

Syntax

primary-path { *path_name* }

no primary-path { *path_name* }

Command Default

By default, there is no configuration of the primary path.

Parameters

path_name

Specifies the name of the configured path in the MPS router.

Modes

MPLS router bypass LSP configuration mode (config-router-mpls-bypass-lsp-*bypass_name*).

MPLS router MPLS interface dynamic bypass configuration mode (config-router-mpls-if-ethernet-*slot/port*-dynamic-bypass)

Usage Guidelines

The path must be already defined in MPLS router.

The user can configure an explicit path for dynamic bypass LSPs that are created for a protected interface.

The **no** form of this command removes the path from the bypass LSP and considers the primary path as not configured.

MPLS is supported on Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example defines *dbyp-path* as the primary path.

```
device>configure
device(config)# router mpls
device(config-router-mpls)# bypass-lsp dbyp-path
device(config-router-mpls-bypass-lsp-dbyp-path)#
```

The following example defines *dbyp-path* as the primary path for dynamic bypass MPLS ethernet interface *0/8*.

```
device>configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/8
device(config-router-mpls-if-ethernet-0/8)# dynamic-bypass
device(config-router-mpls-if-ethernet-0/8-dynamic-bypass)# primary-path dbyp-path
```

priority

Sets the priority of a physical router in a VRRP router group.

Syntax

priority *range*

Command Default

The default priority is 100.

Parameters

range

The priority of a physical router in a virtual router group. Higher numbers have priority over lower numbers. Valid values range from 1 to 254.

Modes

Virtual-router-group configuration mode

Virtual-router-extended-group configuration mode

Usage Guidelines

You can perform this command for VRRP or VRRP-E.

When set, the highest priority backup router will always be the master. (For VRRP, however, the owner is always the master if it is available.) If not set, a higher priority backup will not preempt a lower priority backup that is acting as master.

For an owner router in VRRP, the priority automatically becomes 255 if the virtual IP address of the virtual router and the real IP address of the owner are the same.

Examples

To set the priority to 110 for the VRRP virtual group 1:

```
device# configure terminal
device(config)# protocol vrrp
device(config)# interface ve 10
device(config-if-Ve-10)# vrrp-group 1
device(config-vrrp-group-1)# priority 110
```

To set the priority to 110 for the VRRP-E virtual group 1:

```
device# configure terminal
device(config)# ipv6 protocol vrrp-extended
device(config)# interface ve 10
device(config-if-Ve-10)# ipv6 vrrp-extended-group 1
device(config-vrrp-extended-group-1)# priority 110
```

priority-group-table

Defines the Priority Group ID (PGID) and the scheduling policy associated with it. Each PGID can be assigned one of 16 values. The valid values are [0-7] and [15.0-15.7]. The value range 0-7 indicate DWRR priority and the range 15.0-15.7 indicate Strict Priority values. This configuration and the **priority-table** configuration sets how traffic is handled when congestion occurs. For DWRR traffic, packets are dropped when PFC is not enabled for that flow.

Syntax

priority-group-table *<Priority Group>* **weight** *<weight in percent>* **pfc** [**on** | **off**]

priority-group-table *<Priority Group>* **pfc** [**on** | **off**]

[no] priority-group-table *<Priority Group>*

Parameters

<Priority Group>

Configures the Priority Group. Valid values are 0-7 and 15.0-15.7.

A value in the range 0-7 indicate DWRR priority and unless the *PFC* is set for the entry, packets are liable to be dropped if congestion occurs.

A value in the range 15.0-15.7 indicates strict priority traffic. Traffic in this range is never dropped. Within this range, packets marked with 15.0 has a higher priority than packets marked with 15.1, packets marked with 15.1 has higher priority than those marked with 15.2, and so on. Packets marked as 15.7 has the lowest priority within the Strict Priority group.

weight *<weight in percent>*

For DWRR traffic only. DWRR traffic is in the range 0-7. Sets a value in percentage. For example, set 10 for 10%, 20 for 20%. Ensure that the sum of all DWRR weights in this table must be equal to 100%. If the sum does not equal 100%, then an error is thrown.

pfc [**on** | **off**]

For DWRR traffic only. Configures Priority Flow Control (PFC) for this entry. PFC is enabled when set to *on*. It is recommended that no more than one (1) priority group be enabled for PFC.

PFC cannot be configured for Strict Priority Groups (15.0-15.7).

Modes

CEE Map Mode

Usage Guidelines

PFC can only be enabled for DWRR traffic. It is recommended that only one priority group be configured as PFC enabled. You must create separate entries for each of the priority groups. There can be maximum sixteen (16) entries in the Priority Group Table.

The *no* form of this command removes a priority-group-table configuration entry from the CEE map.

Examples

Configures the Priority Group Table values.

```
device# configure terminal
device(config)# cee-map default
device(config-cee-map-default)# priority-group-table 15.0 pfc off
device(config-cee-map-default)# priority-group-table 15.1 pfc off
device(config-cee-map-default)# priority-group-table 15.2 pfc off
device(config-cee-map-default)# priority-group-table 15.3 pfc off
device(config-cee-map-default)# priority-group-table 15.4 pfc off
device(config-cee-map-default)# priority-group-table 15.5 pfc off
device(config-cee-map-default)# priority-group-table 15.6 pfc off
device(config-cee-map-default)# priority-group-table 15.7 pfc off

device(config-cee-map-default)# priority-group-table 1 weight 40 pfc on
device(config-cee-map-default)# priority-group-table 2 weight 60 pfc off

device(config-cee-map-default)#
```

This example displays the configuration made in the previous example.

```
device# config term
device(config)# do show cee maps default

CEE Map 'default'
Precedence: 1
Priority Group Table
1: Weight 40, PFC Enabled, BW% 40
2: Weight 60, PFC Disabled, BW% 60
15.0: PFC Disabled
15.1: PFC Disabled
15.2: PFC Disabled
15.3: PFC Disabled
15.4: PFC Disabled
15.5: PFC Disabled
15.6: PFC Disabled
15.7: PFC Disabled
Priority Table
CoS: 0 1 2 3 4 5 6 7
---------------------------------------
PGID: 2 2 2 1 2 2 2 15.0
Enabled on the following interfaces:
Ethernet 0/1
```

priority-table

Maps the Priority Group Table entries to priority groups.

Syntax

priority-table *<Priority Group ID>*

[no] priority-table

Parameters

<Priority Group ID>

Configures the CoS to Priority Group Table mapping. Ensure that you map the CoS to those priority groups for which bandwidth is allocated.

Modes

CEE Map Mode

Usage Guidelines

Ensure that you map the CoS to those priority groups for which bandwidth is allocated. The CoS 7 is always reserved for the Strict Priority traffic and is assigned the Priority Group 15.0.

The *no* form of this command removes the CoS to Priority Group Table mapping.

Examples

This example maps the CoS to priority groups.

```
device# config term
device(config)# cee-map default
device(config-cee-map-default)# priority-table 2 2 2 1 2 2 2 15.0
```

This example displays the configuration made in the previous example.

```
device# config term
device(config)# do show cee maps default

CEE Map 'default'
Precedence: 1

Priority Group Table
1: Weight 40, PFC Enabled, BW% 40
2: Weight 60, PFC Disabled, BW% 60
15.0: PFC Disabled
15.1: PFC Disabled
15.2: PFC Disabled
15.3: PFC Disabled
15.4: PFC Disabled
15.5: PFC Disabled
15.6: PFC Disabled
```

```
15.7: PFC Disabled
Priority Table
CoS: 0 1 2 3 4 5 6 7
---------------------------------------
PGID: 2 2 2 1 2 2 2 15.0
Enabled on the following interfaces:
Ethernet 0/1
```

process-restart

Enables the process restart (PR) capability (for fault recovery) for BGP, IS-IS, MPLS, OSPFv2, and OSPFv3.

Syntax

process-restart { **bgp** | **isis** | **mpls** | **ospfv2** | **ospfv3**}

no process-restart { **bgp** | **isis** | **mpls** | **ospfv2** | **ospfv3**}

Command Default

The process restart capability for BGP, IS-IS, OSPFv2, and OSPFv3 is disabled. The process restart capability for MPLS is enabled.

Parameters

bgp

Specifies the BGP protocol.

isis

Specifies the IS-IS protocol.

mpls

Specifies the MPLS protocol.

ospfv2

Specifies the OSPFv2 protocol.

ospfv3

Specifies the OSPFv3 protocol.

Modes

HA configuration mode (config-ha)

Usage Guidelines

Note
The process restart capability should not be enabled when BGP EVPN is configured. For more information, see the *Extreme SLX-OS Layer 3 Routing Configuration Guide*.

The process restart capability for BGP, IS-IS, MPLS, OSPFv2 and OSPFv3 is a fault containment mechanism that ensures that process-level failures do not cause system-level failures.

All of these processes are COLD restartable processes, meaning when there is a fault inside one of these processes, and it crashes, the system does not undergo a failover.

Instead, the process is restarted on the same ACTIVE MM. All the other modules and processes that interact with this particular process are made aware of the process restart, and they adjust accordingly.

All MPLS-based services, such as IPoMPLS, VLL, and VPLS, are disrupted for the duration of MPLS process restart. After the MPLS process is restarted, the control protocols (LDP and RSVP) re-signal the tunnels and cross-connects and all the dependent MPLS applications to resume service. For routing protocols such as BGP, IS-IS and OSPF, all the existing adjacencies are brought down, and are reestablished after the process comes up again. Some traffic loss can be expected until the adjacency comes up again.

If more than one process restart happens within a minute, the entire board reboots, resulting in device reload.

The benefits of the process restart feature can be seen in the following cases:

- The unplanned outage of the routing protocol process can be handled without impacting the whole system or other dependent services.
- The system returns to a stable state quicker than if nonstop routing (NSR) or graceful restart (GR) is configured on the device.

The following table lists the precedence of process restart over GR or NSR.

Table 16: Precedence of process restart over GR or NSR by protocol

Protocol	Precedence
BGP	Process restart over GR
IS-IS	Process restart over NSR
MPLS	Not applicable
OSPFv2	Process restart over GR or NSR
OSPFv3	Process restart over GR or NSR

Examples

The following example disables the process-restart capability for MPLS.

```
device# configure terminal
device(config)# ha
device(config-ha)# no process-restart mpls
```

The following example enables the process-restart capability for BGP.

```
device# configure terminal
device(config)# ha
device(config-ha)# process-restart bgp
```

The following example enables the process-restart capability for IS-IS.

```
device# configure terminal
device(config)# ha
device(config-ha)# process-restart isis
```

The following example enables the process-restart capability for OSPFv2.

```
device# configure terminal
device(config)# ha
device(config-ha)# process-restart ospfv2
```

The following example disables the process-restart capability for OSPFv3.

```
device# configure terminal
device(config)# ha
device(config-ha)# no process-restart ospfv3
```

profile (LLDP)

Creates an LLDP profile.

Syntax

profile *name*

no profile *name*

Parameters

name

Assigns a name to the profile. The name must be between 1 and 63 ASCII characters in length.

name

Assigns a name to the profile. The name must be between 1 and 32 ASCII characters in length.

Modes

Protocol LLDP configuration mode

Usage Guidelines

When you apply an LLDP profile on an interface using the **lldp profile** command, it overrides the global configuration. If a profile is not present, then the default global profile is used until you create a valid profile. Up to 64 profiles can be created.

Enter **no profile** *name* to remove the named profile.

Examples

The following example creates a profile named test.

```
device# configure terminal
device(config)# protocol lldp
device(conf-lldp)# profile test
```

The following example creates a profile named test1.

```
device(config)# protocol lldp
device(conf-lldp)# profile ?
Possible completions:
<Profile Name (Max Size - 32)>
device(conf-lldp)# profile test1
device(config-profile-test1)#
```

The following example deletes a profile named test:

```
device# configure terminal
device(config)# protocol lldp
device(conf-lldp)# no profile test
```

profile (telemetry)

Designates telemetry profiles for telemetry collectors.

Syntax

profile enhanced-queue-discard-pkts-profile
default_enhanced_queue_discard_pkts_statistics

no profile enhanced-queue-discard-pkts-profile
default_enhanced_queue_discard_pkts_statistics

profile enhanced-queue-max-queue-depth-profile
default_enhanced_queue_max_queue_depth_statistics

no profile enhanced-queue-max-queue-depth-profile
default_enhanced_queue_max_queue_depth_statistics

profile interface-profile default_interface_statistics

no profile interface-profile default_interface_statistics

profile mpls-traffic-bypass-profile
default_mpls_traffic_bypass_statistics

no profile mpls-traffic-bypass-profile
default_mpls_traffic_bypass_statistics

profile mpls-traffic-fec-profile default_mpls_traffic_fec_statistics

no profile mpls-traffic-fec-profile default_mpls_traffic_fec_statistics

profile mpls-traffic-lsp-profile default_mpls_traffic_lsp_statistics

no profile mpls-traffic-lsp-profile default_mpls_traffic_lsp_statistics

profile queue-profile default_queue_statistics

no profile queue-profile default_queue_statistics

profile system-profile default_system_utilization_statistics

no profile system-profile default_system_utilization_statistics

Command Default

No profile is designated.

Parameters

enhanced-queue-discard-pkts-profile
default_enhanced_queue_discard_pkts_statistics

(Supported only on SLX 9540 and SLX 9640 devices) Specifies profile **default_enhanced_queue_discard_pkts_statistics** of the **enhanced-queue-**

discard-pkts profile type. This profile tracks packets discarded in the 32 queues with the most discards.

enhanced-queue-max-queue-depth-profile default_enhanced_queue_max_queue_depth_statistics

(Supported only on SLX 9540 and SLX 9640 devices) Specifies profile **default_enhanced_queue_max_queue_depth_statistics** of the **enhanced-queue-max-queue-depth** profile type. This profile tracks maximum queue size in the 32 queues with the largest queue size.

interface-profile default_interface_statistics

Specifies profile **default_interface_statistics** of the **interface** profile type.

mpls-traffic-bypass-profile default_mpls_traffic_bypass_statistics

(Supported only on SLX 9540 and SLX 9640 devices) Specifies profile **default_mpls_traffic_bypass_statistics** of the **mpls-traffic-bypass** profile type.

mpls-traffic-fec-profile default_mpls_traffic_fec_statistics

(Supported only on SLX 9540 and SLX 9640 devices) Specifies profile **default_mpls_traffic_fec_statistics** of the **mpls-traffic-fec** profile type.

mpls-traffic-lsp-profile default_mpls_traffic_lsp_statistics

(Supported only on SLX 9540 and SLX 9640 devices) Specifies profile **default_mpls_traffic_lsp_statistics** of the **mpls-traffic-lsp** profile type.

queue-profile default_queue_statistics

(Supported only on SLX 9540 and SLX 9640 devices) Specifies profile **default_queue_statistics** of the **queue** profile type. This profile captures the overall queue statistics for the device.

system-profile default_system_utilization_statistics

Specifies profile **default_system_utilization_statistics** of the **system-utilization** profile type.

Modes

Telemetry-collector configuration mode

Usage Guidelines

The **no** version of this command removes the profile details from the collector.

Examples

Typical command execution example.

```
device# configure terminal
device(config)# telemetry collector collector_1
device(config-telemetry-collector-collector_1)# profile system-profile
default_system_utilization_statistics
```

profile counters

Optimizes hardware counters.

Syntax

profile counters { **counter-profile-1** | **counter-profile-2** | **counter-profile-3** | **counter-profile-4** | **counter-profile-5** | **counter-profile-6** | **default** }

Command Default

The **default** counter profile is enabled and statistics are collected for ingress and egress L4 traffic.

Parameters

counter-profile-1

Specifies resources optimized for Ingress ACL, OF, and Egress ACL, with forward and drop counting for Layer 4 ingress traffic.

counter-profile-2

Specifies resources optimized for OF, MPLS, VPLS, VLL, and MCT, with hit counting for Layer 4 ingress traffic.

counter-profile-3

Specifies resources optimized for MPLS, VPLS, VLL, MCT, with hit counting for Layer 4 ingress traffic.

counter-profile-4

L4-optimized, forward or drop counting for all ingress L4.

Specifies resources optimized for Layer 4 traffic, with forward and drop counting for all Layer 4 ingress traffic.

counter-profile-5

Specifies resources optimized for egress rate limit, with support for counting up to 32,000 VOQs.

counter-profile-6

Specifies resource optimized for reporting egress VE traffic statistics. This is only supported on SLX 9540 and SLX 9640 devices where the corresponding counter engines are setup for counting egress VE statistics.

default

Ingress and egress L4.

Modes

Hardware configuration mode

Usage Guidelines

This command is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

For the new setting to take effect, you need to run the **copy running-config startup-config** to reload the device. Run this command during a maintenance window so that the profile changes are activated without interrupting normal network services.

Use the **profile counters default** form of the command to restore the default setting.

The option *counter-profile-6* is only available for SLX 9540 and SLX 9640 devices where the corresponding counter engines are setup for counting egress VE statistics.

Examples

The following example optimizes bridge domain hit counting for Layer 4 ingress traffic.

```
device# configure terminal
device(config)# hardware
device(config-hardware)# profile counters counter-profile-2
**Warning: To activate the new profile config, please run 'copy running-config
startup-config' followed by reload system.
```

The following example configures the device for collecting egress VE traffic statistics.

```
device# configure terminal
device(config)# hardware
device(config-harware)# profile counters counter-profile-6
**Warning: To activate the new profile config, please run 'copy running-config
startup-config' followed by reload system.
```

profile etcam

Specifies external TCAM (ETCAM) profiles to support border profiles for Internet peering.

Syntax

profile etcam { **default** | **ipv4-v6-route** | **ipv6-route** }

Command Default

The default ETCAM profile is enabled.

Parameters

default

Specifies the default ETCAM profile: IPv4 unicast routes in the external lookup device (ELK). The internal longest prefix match (LPM) is used to program IPv6 unicast routes.

ipv4-v6-route

Specifies the profile that programs IPv4 and v6 unicast routes on external TCAM.

ipv6-route

Specifies the profile that programs IPv6 unicast routes in the external TCAM. The internal LPM is used to program IPv4 unicast routes.

Modes

Hardware configuration mode

Usage Guidelines

This command is supported only on the SLX 9640.

For the new setting to take effect, you need to run the **copy running-config startup-config** to reload the device. Run this command during a maintenance window so that the profile changes are activated without interrupting normal network services.

This command does not have a **no** form. Specify **default** to revert to the default settings.

Examples

The following example specifies that IPv4 and IPv6 routes are programmed in the ELK.

```
device# configure terminal
device(config)# hardware
device(config-hardware)# profile etcam ipv4-v6-route
```

```
**Warning: To activate the new profile config, please run 'copy running-config
startup-config' followed by reload system.
```

profile lag

Configures a LAG profile for hardware support.

Syntax

profile lag { **default | lag-profile-1** }

Command Default

The default LAG profile is enabled.

Parameters

default

Specifies the default LAG profile. As described in the Usage Guidelines, the maximum numbers of port-channel IDs and links per port-channel vary with device and TCAM profile.

lag-profile-1

Specifies lag-profile-1 as the LAG profile. As described in the Usage Guidelines, the maximum numbers of port-channel IDs and links per port-channel vary with device and TCAM profile.

Modes

Hardware configuration mode

Usage Guidelines

This command is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

To view the current LAG profile, enter the **show hardware profile current** command.

For the new setting to take effect, you need to run the **copy running-config startup-config** to reload the device. Run this command during a maintenance window so that the profile changes are activated without interrupting normal network services.

This command does not support a **no** form. Use the **profile lag default** form of the command to restore the default LAG profile.

Port channel scale and support for SLX 9740/Extreme 8820

Table 17: Port-channel scale for SLX 9740/Extreme 8820 devices.

Device	LAG Profile	Supported port-channel IDs	Maximum links per port-channel
SLX 9740-40/ Extreme 8820-40	default	1-256; Only 77 port-channels can be created at one time.	64
SLX 9740-80/ Extreme 8820-80	default	1-256; Only 153 port-channels can be created at one time.	64

Note

- For the 1U SLX 9740-40/Extreme 8820-40, the number of LAGs will be 77, where:
  - 76 are the front end ports (all breakouts)
  - 1 (insight port)
- For the 2U SLX 9740-80/Extreme 8820-80, the number of LAGs will be 153. where:
  - 152 are the front end ports (all breakouts)
  - 1 (insight port)

Maximum numbers of port-channel IDs and links per port-channel vary with device and LAG profile, as follows.

Table 18: Port-channel scale for SLX 9540 and SLX 9640 devices

Supported port-channel IDs	Maximum links per port-channel
1–256; Only 64 port-channels can be created at any one time.	64
1–256; Only 64 port-channels can be created at any one time.	32

Examples

The following example specifies lag-profile-1.

```
device# configure terminal
device(config)# hardware
device(config-hardware)# profile lag lag-profile-1
**Warning: To activate the new profile config, please run 'copy running-config
startup-config' followed by reload system.
```

profile qos

Sets the QoS profile for hardware.

Syntax

profile qos { *lossless* | *lossy* }

Command Default

No explicit configuration of lossy or lossless profile is configured on the interface.

Parameters

lossless

Sets lossless buffer pool support on the hardware interface.

lossy

Sets lossy buffer pool support on the hardware interface.

Modes

Hardware configuration mode

Usage Guidelines

Use this command on ExtremeSwitching SLX 9150 and ExtremeSwitching SLX 9250 to enable allocating 25% of the packet buffer to the lossless pool during initialization.

The ExtremeSwitching SLX 9150 and ExtremeSwitching SLX 9250 switches have limited on-board memory. Allocating a portion of this memory for lossless pool when not required is a waste of this limited resource. This command enable you to select when to use the lossless pool.

Changing this configuration requires a reboot to take effect.

Examples

To set the hardware QoS mode to lossless mode.

```
device# configure terminal
device(config)# hardware
device(config-hardware)# profile qos lossless
```

To set the hardware Qos mode to lossy mode.

```
device# configure terminal
device(config)# hardware
```

```
device(config-hardware)# profile qos lossy
```

profile route

Specifies the hardware route profile and maximum load-sharing path.

Syntax

profile route { **default** | **enable** | **max-l2** | **max-l3-host** | **max-route** | **maximum-paths** | **route-enhance** }

profile route default

profile route enable { **ipv6-max-prefix-64** | **urpf** }

[no] profile route enable { **ipv6-max-prefix-64** | **urpf** }

profile route max-l2

profile route max-l3-hosts

profile route max-routes

profile route maximum-paths { *8* | *16* | *32* | *64* | *128* }

profile route route-enhance { *hw_opt* | *multi_vrf* | *v4_fib_comp* | *v6_fib_comp* }

Command Default

The default route profile is enabled.

Parameters

default

Specifies the default route profile. (Not supported on SLX 9640.)

enable { **ipv6-max-prefix-64** | **urpf** }

- *ipv6-max-prefix-64* - Use this option to enable/disable 64-bit prefix only mode for IPv6 routes. When enabled, IPv6 routes with prefix lengths of > 64 bits will not be accepted. (Only supported on SLX 9150 and SLX 9250.)
- *urpf* - Use this option to enable/disable *urpf* (Unicast Reverse Path Forwarding) support on the device. When this is enabled, it reduces the maximum route/host capacity on the SLX device by half. This configuration knob only enables/disables the hardware capability on the SLX device. `rpf-mode` configuration CLI needs to be configured on the L3 interface level for the *uRPF* function. (Only supported on SLX 9150 and SLX 9250.)

Note
Interface level *uprf* configuration will not have any impact without this profile being enabled.

max-l2

Sets a profile that maximizes the addition of L2-MACs over L3 Unicast Hosts or L3 Unicast Routes.

max-l3-host

Sets a profile that maximizes the addition of L3 Unicast Hosts over L3 Unicast Routes or L2-MACs.

max-routes

Sets a profile that maximizes the addition of L3 Unicast Routes over L3 Unicast Hosts or L2-MACs.

maximum-paths { *8* | *16* | *32* | *64* | *128* }

Configures the maximum number of load sharing paths for ECMP. Select from one of the available choices.

route-enhance

(supported only on SLX 9540) Specifies various route enhancement.

hw_opt

Specifies route enhancement for hardware optimization. Disabled by default.

multi_vrf

Specifies route enhancement for multiple VRF support (route scaling) on a non-default VRF.

v4_fib_comp

Specifies route enhancement for IPv4 FIB compression.

v6_fib_comp

Specifies route enhancement for IPv6 FIB compression.

{ **off** | **on** }

(supported only on SLX 9540) Disables or enables the specified **route-enhance** options. By default, all options are disabled.

Modes

Hardware configuration mode

Usage Guidelines

To display the default and current number of routes supported for your device, run the **show hardware profile** command.

Use the **profile route default** form of the command to restore the default setting.

Use the **no profile route enable** form of the command to disable the route forwarding features.

Note
SLX 9540 and SLX 9640 support 64 maximum paths.

Important
SLX 9640 supports only *maximum-paths* option under router profile.

Examples

The following example sets 64 as the maximum paths for ECMP.

```
device(config-hardware)# profile route maximum-paths 64
**Warning: To activate the new profile config, run
'copy running-config startup-config' followed by 'reload system'.
**Warning: User should remove unsupported configurations.
```

The following command enables preferring L2 MACs over L3 Unicast Routes or L3 Unicast Host.

```
device(config)# profile route max-l2
device(config)#
```

The following example sets 128 as the maximum paths for ECMP.

```
SLX(config-hardware)# profile route maximum-paths 128
%Warning: To activate the new profile config, please run 'reload system'.
SLX(config-hardware)#
```

profile tcam

Optimizes hardware resources, by specifying a ternary content-addressable memory (TCAM) profile.

Syntax

profile tcam { **app-telemetry** | **border-routing** | **default** | **layer2-ratelimit** | **multicast-profile** | **vxlan-visibility** }

Command Default

The default TCAM profile is enabled.

Parameters

app-telemetry

Optimizes resources for application telemetry. MCT is supported.

border-routing

Optimizes resources for border routing and BGP Flowspec features.

default

Optimizes resources with basic support for all applications. MCT is supported.

layer2-ratelimit

Optimizes resources for Layer 2 ACL egress rate-limiting and related applications.

multicast-profile

Optimizes resources for Layer 2 and Layer 3 IPv6 multicast.

vxlan-visibility

Optimizes resources for VXLAN transit visibility and GRE.

Modes

Hardware configuration mode

Usage Guidelines

This feature is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

This command does not support a **no** form. Use the **profile tcam default** form of the command to restore the default setting.

For the new setting to take effect, you need to run the **copy running-config startup-config** to reload the device. Run this command during a maintenance window so that the profile changes are activated without interrupting normal network services.

On the SLX 9740 and Extreme 8820 devices, only the `default` and `ipv6-optimised` configuration options are supported. When trying to configure the other options, the message `Not supported in the platform` is displayed.

Examples

The following example optimizes TCAM resources for Layer 2 applications and VPLS support.

```
device# configure terminal
device(config)# hardware
device(config-hardware)# profile tcam layer2-ratelimit
```

profile tcam cam-share

Enables TCAM sharing for security or policy-based routing (PBR) ACLs that are applied to multiple interfaces.

Syntax

profile tcam cam-share [**l2-ingress-acl**] [**l3-v4-ingress-acl**] [**l3-v4-pbr**] [**l3-v6-ingress-acl**] [**l3-v6-pbr**]

no profile tcam cam-share

Command Default

By default, TCAM sharing is disabled.

Parameters

l2-ingress-acl

Enables TCAM sharing for Layer 2 security ACLs applied to ingress traffic.

l3-v4-ingress-acl

Enables TCAM sharing for IPv4 security ACLs applied to ingress traffic.

l3-v4-pbr

Enables TCAM sharing for IPv4 ACLs included in route maps for PBR.

l3-v6-ingress-acl

Enables TCAM sharing for IPv6 security ACLs applied to ingress traffic.

l3-v6-pbr

Enables TCAM sharing for IPv6 ACLs included in route maps for PBR.

Modes

Hardware configuration mode

Usage Guidelines

TCAM sharing is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only sharing all ports with the same ASIC.

TCAM sharing for security ACLs works as follows: TCAM resources are shared if a specific ACL is applied to multiple ports.

TCAM sharing for PBR ACLs works as follows: TCAM resources are shared if a specific ACL (included in one or more route maps) is applied to multiple ports.

When you change the TCAM profile type, also update cam sharing based on the limitation of the new profile. TCAM sharing is not supported for user-defined ACLs or for ACLs that are applied for rate limiting.

For the new setting to take effect, you need to run the **copy running-config startup-config** to reload the device. Run this command during a maintenance window so that the profile changes are activated without interrupting normal network services.

Use the **no** form of the command to disable TCAM sharing.

Examples

This example enables TCAM cam sharing for Layer 2 ingress ACL.

```
device(config)# hardware
device(config-hardware)# profile tcam cam-share l2-ingress-acl
**Warning: To activate the new profile config, please run
'copy running-config startup-config' followed by 'reload system'.
```

This example disables TCAM cam sharing.

```
device(config)# hardware
device(config-hardware)# no profile tcam cam-share
**Warning: To activate the new profile config, please run
'copy running-config startup-config' followed by 'reload system'.
```

protocol

Configures the authentication protocol to use for communication with the Remote Authentication Dial-In User Service (RADIUS) server.

Syntax

protocol { **chap** | **pap** | **peap** }

no protocol

Command Default

The default protocol is Challenge Handshake Authentication Protocol (CHAP).

Parameters

chap

Specifies using CHAP for communication with the RADIUS server.

pap

Specifies using Password Authentication Protocol (PAP) for communication with the RADIUS server.

peap

Specifies using Protected Extensible Authentication Protocol (PEAP) for communication with the RADIUS server.

Modes

RADIUS server host VRF configuration mode

Usage Guidelines

The **no** form of the command restores the command default value.

Examples

The following example shows how to configure PAP as the authentication protocol for communication with the RADIUS server.

```
device# configure terminal
device(config)# radius-server host 10.37.73.180 use-vrf green-vrf
device(config-host-10.37.73.180/green-vrf)# protocol pap
```

protocol cfm

Enables the CFM protocol globally on the devices and enter into the CFM Protocol Configuration mode.

Syntax

protocol cfm

no protocol cfm

Command Default

This command is executed on the local switch.

Modes

Privileged EXEC mode

Usage Guidelines

The no form of this command disables the CFM protocol on the device.

Examples

```
device#(config)protocol cfm
device(config-cfm)#
```

protocol link-oam

Allows you to enter the link OAM global configuration mode.

Syntax

protocol link-oam

Command Default

This command is executed on the local switch.

Modes

Privileged EXEC mode

Examples

```
device# configure terminal
device(config)#protocol link-oam
device(config-link-oam)#
```

protocol lldp

Enters the Link Layer Discovery Protocol (LLDP) configuration mode.

Syntax

protocol lldp

no protocol lldp

Command Default

LLDP protocols are enabled.

Modes

Global configuration mode

Usage Guidelines

Enter **no protocol lldp** to restore the default settings.

Examples

To enter LLDP mode:

```
device# configure terminal
device(config)# protocol lldp
device(conf-lldp)#
```

To reset all LLDP configurations:

```
device# configure terminal
device(config)# no protocol lldp
device(conf-lldp)#
```

protocol loop-detection

Enables the loop detection (LD) feature globally and enters Protocol Loop Detection configuration mode.

Syntax

protocol loop-detection

no protocol loop-detection

Command Default

This feature is disabled.

Modes

Global configuration mode

Usage Guidelines

Use the no form of this command to disable loop detection globally.

Examples

To enable loop detection globally and enter Protocol Loop Detection configuration mode:

```
device# configure terminal
device(config)# protocol loop-detection
device(config-loop-detect)#
```

To disable loop detection globally:

```
device# configure terminal
device(config)# no protocol loop-detection
```

protocol mvrp

Enables Multiple VLAN Registration Protocol (MVRP) globally on the device and accesses MVRP configuration mode.

Syntax

protocol mvrp

no protocol mvrp

Command Default

MVRP is disabled globally and on all interfaces by default.

Modes

Global configuration mode

Usage Guidelines

This feature is supported on the SLX 9250, SLX 9540, SLX 9640, SLX 9740, Extreme 8720, and Extreme 8820 devices.

The no form of this command disables MVRP globally on the device and on all interfaces enabled with MVRP.

For an interface to participate in MVRP, you must configure MVRP on the interface through the **mvrp enable** command.

You cannot enable MVRP when the following features are enabled on the device and vice versa:

- PVST
- RPVST
- MSTIs for MSTP
- Topology groups
- Ring protocols

Examples

The following example shows the enabling of MVRP globally.

```
device# configure terminal
device (config)# protocol mvrp
device (config-mvrp)#
```

protocol spanning-tree

Designates the context for spanning tree.

Syntax

protocol spanning-tree { **mstp** | **rstp** | **stp** | **pvst** | **rpvst** }

no protocol spanning-tree

Command Default

STP is not enabled. STP is not required in a loop-free topology.

Parameters

mstp

Specifies the Multiple Spanning Tree Protocol (MSTP).

rstp

Specifies the Rapid Spanning Tree (RSTP).

stp

Specifies the Spanning Tree Protocol (STP).

pvst

Specifies Per-VLAN Spanning Tree Protocol Plus (PVST+).

rpvst

Specifies Rapid Per-VLAN Spanning Tree Protocol Plus (R-PVST+).

Modes

Global configuration mode

Usage Guidelines

Consider enabling STP to detect or avoid loops. You must turn off one form of STP before turning on another form.

Packet drops or packet flooding may occur if you do not enable xSTP on all devices connected on both sides of parallel links.

Enter **no protocol spanning-tree** to delete the context and all the configurations defined within the context or protocol for the interface.

Examples

To enable the Spanning Tree Protocol:

```
device# configure terminal
device(config)# protocol spanning-tree stp
```

protocol udld

Enables and/or enters unidirectional link detection (UDLD) protocol configuration mode.

Syntax

protocol udld

no protocol udld

Command Default

This protocol is disabled by default.

Modes

Global configuration mode

Usage Guidelines

UDLD detects and blocks a physical link that becomes unidirectional. A unidirectional link can cause traffic in a network to loop endlessly. When the link becomes bidirectional again, UDLD unblocks the link.

This protocol applies only to physical ports. In addition to running this command, you must also enable each desired port for UDLD in interface subconfiguration mode.

Use the **no protocol udld** command to disable the UDLD protocol and revert all UDLD configuration to defaults.

Examples

To enable the unidirectional link detection (UDLD) protocol:

```
 device# configure terminal
device(config)# protocol udld
```

protocol vrrp

Globally enables Virtual Router Redundancy Protocol (VRRP).

Syntax

protocol vrrp

no protocol vrrp

Command Default

VRRP is not enabled.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command globally disables VRRP.

Examples

To enable VRRP:

```
device# configure terminal
device(config)# protocol vrrp
```

protocol vrrp-extended

Globally enables VRRP-Extended.

Syntax

protocol vrrp-extended

no protocol vrrp-extended

Command Default

Disabled

Modes

Global configuration mode

Usage Guidelines

The **no protocol vrrp-extended** command globally disables VRRP-E.

Examples

To enable VRRP-Extended:

```
device# configure terminal
device (config)# protocol vrrp-extended
```

prune-wait

Configures the amount of time a PIM device waits to stop traffic after receiving a Prune message from a neighboring device.

Syntax

prune-wait *seconds*

no prune-wait

Command Default

The default wait time is 3 seconds.

Parameters

seconds

Specifies the wait time in seconds. Valid values range from 0 through 30 seconds.

Modes

PIM router configuration mode

Usage Guidelines

A smaller prune wait time reduces flooding of unwanted traffic. A prune wait time of 0 causes the PIM device to stop traffic immediately upon receiving a prune message.

Do not configure a prune wait time when there are two or more neighbors on the physical port. One neighbor may send a prune message while the other sends a join message at the same time, or within less than 3 seconds.

The **no prune-wait** form of this command restores the default wait time of 3 seconds.

Examples

This example configures a wait time of 0 seconds for IPv4 PIM.

```
device(config)# router pim
device(config-pim-router)# prune-wait 0
```

This example configures a wait time of 10 seconds for IPv6 PIM.

```
device(config)# ipv6 router pim
device(config-ipv6-router-pim-vrf-default-vrf)# prune-wait 10
```

pw-profile

Creates a pseudowire (PW) profile that can be shared across multiple Virtual Private LAN Services (VPLS) bridge domains.

Syntax

pw-profile [*pw-profile-name* [**mtu** *mtu-value*] [**mtu-enforce** { *false* | *true* }] [**vc-mode** { **raw** | **raw-passthrough** | **tag** }]

no pw-profile *pw-profile-name* [**mtu**] [**mtu-enforce**] [**vc-mode**]]

Command Default

No PW profile is configured.

Parameters

pw-profile-name

Specifies the name of a PW profile.

mtu *mtu-value*

Specifies the maximum transmission unit (MTU) for the PW profile. The range is from 64 through 15966.

mtu-enforce

Configures MTU enforcement check during PW signaling.
false

Enables the MTU enforcement check.

true

Disables the MTU enforcement check.

vc-mode

Note
When a pseudowire profile is attached to a bridge domain, on which routing is enabled (by using the **router-interface** command), you are not allowed to change the pseudowire profile **vc-mode** configuration to **raw**.

Configures the virtual connection (VC) mode for the profile:
raw

Specifies using raw mode. At VC label imposition, when a tagged packet is received on a tagged AC endpoint, the VLAN tag is removed before it is sent out on the wire. When an untagged packet is received on an untagged AC endpoint it is encapsulated as is and sent out on the wire.

raw-passthrough

Specifies using raw-passthrough mode which enables interoperation with third-party devices. When all endpoints are configured as tagged endpoints, raw

passthrough mode behaves the same way as tagged mode. When all endpoints are configured as untagged endpoints, raw-passthrough mode behaves the same way as raw mode. Select the **raw-passthrough** option, when all endpoints are configured as untagged endpoints (even when peer devices signal the PW VC mode as raw).

tag

Specifies using tag mode. At VC label imposition, when a tagged packet is received on a tagged AC endpoint, the packet is encapsulated as is and sent out on the wire. When an untagged packet is received on an untagged AC endpoint, a dummy tag is added and it is sent out on the wire.

Modes

Global configuration mode.

Usage Guidelines

You can configure up to 64 PW profiles.

The **no** form of the command removes the PW profile configuration.

Examples

The following example shows how to create a PW profile named test specifying that the VC mode for the profile is raw-passthrough.

```
device# configure terminal
device(config)# pw-profile test vc-mode raw-passthrough
```

pw-profile (bridge domain)

Configures a pseudowire (PW) profile for a bridge domain.

Syntax

pw-profile *pw-profile-name*

no pw-profile

Command Default

A PW profile is not configured.

Parameters

pw-profile-name

Specifies the name of the PW profile to attach to the bridge profile.

Modes

Bridge-domain configuration mode.

Usage Guidelines

The **no** form of the command removes the PW profile from the bridge-domain configuration.

Examples

The following example shows how to configure a PW profile named test for bridge domain 1.

```
device# configure terminal
device(config)# bridge-domain 1
device(config-bridge-domain-1)# pw-profile test
```

python

Launches an interactive Python shell, with an option to launch a Python script.

Syntax

python [*python-statement* | *python-script-filename*] [*script-arguments*]

Parameters

python-statement

Must be a valid python interpreter argument.

python-script-filename

Runs a Python script file. Valid values range from 4 through 32 characters (including the **.py** extension). The first character must be alphabetic.

script-arguments

Passes one or more arguments defined in the script.

Modes

Privileged EXEC mode

Usage Guidelines

This command is available only to users with admin-level permissions.

Entering **python**—with no additional parameters—launches an interactive Python shell.

Entering **python** *python-statement* launches an interactive Python shell and runs a valid *python-statement* that you enter. For example, entering `python -h` invokes the Python shell and displays Python options and arguments.

Entering **python** *python-script-filename* launches an interactive Python shell and runs the Python file. (To make a Python file available to this command, copy the Python file to the `flash://` location on the device, using the **copy** command.)

Note the following divergence between SLX-OS CLI syntax and Python syntax:

- Although in general, SLX-OS CLI syntax is not case-sensitive, Extreme Networks convention is to use lower-case.
- Python syntax is case sensitive.

To exit the Python environment and return to the CLI, enter either:

- **exit()**
- **Ctrl-D**

Examples

The following example launches the Python shell and then both assigns an SLX CLI operational command to a Python variable and runs that command.

```
device# python
Python 3.5.2 (default, Apr 11 2019, 13:05:18)
[GCC 4.8.2] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> cmd_show_users = CLI('show users')
!Command: show users
!Time: Tue Aug  9 09:09:39 2016

**USER SESSIONS**
Username            Role       Host IP       Device  Time Logged In
jdoe                admin      10.11.12.13   Cli     2016-08-09 09:06:46
admin               admin      127.1.0.1     Cli     18640
**LOCKED USERS**
Username
no locked users
>>>
```

The following example (partial) launches the Python shell to run a Python script-file.

Note
For an annotated text of this script, refer to the *Extreme SLX-OS Management Configuration Guide* > "Python Event-Management and Scripting" > "Python scripts and run-logs."

```
SLX# python create_po.py                                                    !
Command: show running-config vlan
!Time: Fri Dec 16 18:35:41 2016

vlan 1
!
vlan dot1q tag native

!Command: config
 vlan 101-105
!Time: Fri Dec 16 18:35:41 2016

!Command: show running-config vlan
!Time: Fri Dec 16 18:35:41 2016

vlan 1
!
vlan 101
!
vlan 102
!
vlan 103
!
vlan 104
!
vlan 105
!
vlan dot1q tag native

!Command: show running-config int po
!Time: Fri Dec 16 18:35:41 2016

% No entries found.
```

```
!Command: config
 int po 10
 switchport
 switchport mode trunk
 switchport trunk allowed vlan add 101-105
 switchport trunk tag native-vlan ; no shut
!Time: Fri Dec 16 18:35:41 2016


!Command: show running-config int po
!Time: Fri Dec 16 18:35:42 2016

interface Port-channel 10
 switchport
 switchport mode trunk
 switchport trunk allowed vlan add 101-105
```

The following example launches the Python shell to test an event-handler script-file.

Note
For more information, refer to the "Python Event-Management and Scripting" > "Guidelines for writing Python scripts" topic in the *Extreme SLX-OS Management Configuration Guide*.

```
device# python script.py --raslog-triggers {"SH-1002":" Event: exit, Status: success,
Info: User [admin] successfully exited from SLXVM Linux shell. Exit Time: Thu Apr 12
17:29:44 2018"}
```

qos cos

Changes the interface default Class of Service (CoS) value.

Syntax

qos cos *cos_value*

Command Default

The default is 0.

Parameters

value

Specifies the CoS value. Valid values range from 0 through 7.

Modes

Interface configuration mode

Usage Guidelines

Examples

To set the CoS value to 2 on a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 1/3
device(conf-if-eth-1/3)# qos cos 2
```

To set the CoS value to 2 on a specific port channel interface:

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos cos 2
```

qos cos-mutation

Applies a user configured QoS CoS-to-CoS mutation map to an interface.

Syntax

qos cos-mutation *cos_map_name*

Command Default

No explicit QoS CoS-to-CoS mutation map is applied; the inbound CoS equals the outbound CoS.

Parameters

cos_map_name

The name of the CoS mutation map.

Modes

Interface configuration mode

Usage Guidelines

Mutation mapping is a method of modifying a QoS field in all packets on an interface. On ingress, mutation mapping occurs before traffic classification and all other actions. On egress, mutation mapping occurs after traffic classification and before all other actions.

Examples

Follow this example to apply a QoS CoS-to-CoS mutation map to a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 1/3
device(conf-if-eth-1/3)# qos cos-mutation cos_mutation_map
```

To apply a QoS CoS-to-CoS mutation map to a specific port -channel interface:

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos cos-mutation cos_mutation_map
```

qos cos-mutation

Applies a CoS Mutation map on a physical or a port channel interface. Use this command to apply the *all-zero-map* special CoS Mutation map.

Syntax

qos cos-mutation [**all-zero-map** | *cos-mutation-map-name*]

no qos cos-mutation [**all-zero-map**]

Parameters

all-zero-map

Applies the special *all-zero-map* CoS Mutation map where any incoming CoS value is mapped to the value 0 (zero) before the packet is sent out.

cos-mutation-map-name

Applies the named CoS Mutation map to the interface.

Modes

Interface Configuration mode

Usage Guidelines

This command can only be applied to physical and port channel interfaces in the *Layer 2 Trunk* mode.

The *no* form of this command disassociates the QoS map from the interface.

This command returns an error when it is applied on a Layer 3 physical or a port channel interface.

This command returns an error when it is applied on a Layer 2 physical or a port channel interface in *Layer 2 Access* mode.

You cannot change the physical or port channel's mode after applying a CoS Mutation map.

Supported In

SLX 9740 and Extreme 8820

Examples

This example shows the application of a CoS Mutation map on a physical interface. The QoS CoS Mutation map should already exist.

```
SLX# configure terminal
SLX (config)# interface Ethernet 0/3
SLX (conf-if-eth-0/3)# qos cos-mutation test-cos-mut-map-1
SLX (conf-if-eth-0/3)#
```

This example show the application of the special *all-zero-map* QoS CoS Mutation map on to a physical interface.

```
SLX# configure terminal
SLX (config)# interface Ethernet 0/3
SLX (conf-if-eth-0/3)# qos cos-mutation all-zero-map
SLX (conf-if-eth-0/3)#
```

This example shows how to remove a QoS CoS mutation map that is associated with a physical interface.

```
SLX# configure terminal
SLX (config)# interface Ethernet 0/3
SLX (conf-if-eth-0/3)# no qos cos-mutation
SLX (conf-if-eth-0/3)#
```

Related Commands

- map cos to cos on page 1080
- qos map cos-mutation on page 1437
- show qos maps cos-mutation on page 2259

qos cos-traffic-class

Applies a Quality of Service (QoS) CoS-to-traffic class mutation map on an interface.

Syntax

qos cos-traffic-class *cos_map_name*

Command Default

No explicit QoS CoS-to-traffic class mutation map is applied; the inbound CoS equals the outbound CoS.

Parameters

cos_tc_map_name

The name of the CoS-to-traffic class mutation map.

Modes

Interface configuration mode.

Usage Guidelines

Mutation mapping is a method of modifying a QoS field in all packets on an interface. On ingress, mutation mapping occurs before traffic classification and all other actions. On egress, mutation mapping occurs after traffic classification and before all other actions.

Examples

To activate a QoS CoS-to-traffic class mutation map named `cosMutMap` on a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 1/3
device(conf-if-eth-1/3)# qos cos-mutation cosMutMap
```

To activate a QoS CoS-to-traffic class mutation map from a specific port channel interface:

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos cos-mutation cosMutMap
```

qos cpu slot

Configures the Traffic Manager CPU port shaper rate (all towers) to the line card CPU.

Syntax

qos cpu slot *line-card-number* { **group** *group_id* { **prio** { *priority* | **all** } | **shaper rate** *shaper_rate* **burst** *burst_size* | **wfq weight** *weight_value* }

qos cpu slot *line-card-number* { **port shaper rate** *shaper_rate* **burst** *burst_size* }

no qos cpu slot *line-card-number* { **group** *group_id* { **prio** { *priority* | **all** } | **shaper rate** *shaper_rate* **burst** *burst_size* | **wfq weight** *weight_value* }

no qos cpu slot *line-card-number* { **port shaper rate** *shaper_rate* **burst** *burst_size* }

Command Default

The Traffic Manager CPU group or port shaper rate is not set.

Parameters

line-card-number

The values are 0 on Pizzabox platforms, 1 through 4 on F4 platforms, and 1 through 8 on F8 platforms.

group *group_id*

Configures a CPU group.

shaper rate *shaper_rate*

Configures the Traffic Manager CPU shaper rate (all towers) to the line card CPU for CPU groups. The rate is in kilo bits per second (Kbps) with a range from 0 through 100000.

prio *priority*

Configures the Traffic Manager CPU shaper rate (all towers) to the line card CPU for individual priority VoQs in a CPU group. The priority value ranges from 0 through 7.

burst *burst_size*

Configures the CPU burst size. The burst size value ranges from 1 through 64 KB.

wfq weight *weight_value*

Configures the CPU group's weighted fair queue value (all towers). The weight value ranges from 1 through 128.

port

Configures a CPU port.

Modes

Global configuration mode.

Usage Guidelines

The **no** form of the command removes the QoS CPU shaper configuration.

Examples

This example sets the Traffic Manager CPU port shaper on slot 1 to priority 5, with a rate of 4500 Kbps, and a burst size of 1KB.

```
device# configure terminal
device(config)# qos cpu slot 1 port shaper rate 4000 burst 1
```

This example sets the Traffic Manager CPU port shaper on slot 1 to 4000 Kbps with a burst size of 1KB.

```
device# configure terminal
device(config)# qos cpu slot 1 port shaper rate 4000 burst 1
```

This example sets the Traffic Manager CPU on slot 1 group 1 priority to 5, with a rate of 4500 Kbps, and a burst size of 1KB.

```
device# configure terminal
device(config)# qos cpu slot 1 group 1 priority 5 shaper rate 4500 burst 1
```

qos dscp-cos

Applies a user configured QoS DSCP-to-CoS mutation map to an interface.

Syntax

qos dscp-cos *dscp_cos_map_name*

Command Default

No explicit QoS DSCP-to-CoS mutation map is applied.

Parameters

dscp_cos_map_name

Name of DSCP-to-COS mutation map

Modes

Interface configuration mode.

Usage Guidelines

Mutation mapping is a method of modifying a QoS field in all packets on an interface. On ingress, mutation mapping occurs before traffic classification and all other actions. On egress, mutation mapping occurs after traffic classification and before all other actions.

Examples

Follow this example to apply a user configured QoS DSCP-to-COS mutation map named `dscpMap` to a specific Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 2/2
device(conf-if-eth-2/2)# qos dscp-cos dscpMap
```

Follow this example to apply a user configured QoS DSCP-to-COS mutation map named `dscpMap` to a specific port channel interface.

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos dscp-cos dscpMap
```

qos dscp-mutation

Applies a user configured QoS DSCP mutation map to an interface.

Syntax

qos dscp-mutation *dscp_map_name*

Command Default

No explicit user configured QoS DSCP-to-DSCP mutation map is applied; the inbound DSCP equals the outbound DSCP.

Parameters

dscp_map_name

The name of the DSCP mutation map

Modes

Interface subtype configuration mode

Usage Guidelines

Mutation mapping is a method of modifying a QoS field in all packets on an interface. On ingress, mutation mapping occurs before traffic classification and all other actions. On egress, mutation mapping occurs after traffic classification and before all other actions.

Examples

Follow this example to apply a QoS DSCP-to-DSCP mutation map to a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 1/3
device(conf-if-eth-1/3)# qos dscp-mutation dscp_mutation_map
```

To apply a QoS DSCP-to-DSCP mutation map to a specific port channel interface:

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos dscp-mutation dscp_mutation_map
```

qos dscp-traffic-class

Applies a user configured QoS DSCP-to-traffic- class mutation map to an interface.

Syntax

qos dscp-traffic-class *dscp_tc_name*

Command Default

No explicit user configured QoS DSCP-to-traffic class map is enabled on the interface.

Parameters

dscp_tc_name

Name of DSCP-to-traffic class map

Modes

Interface configuration mode

Usage Guidelines

Mutation mapping is a method of modifying a QoS field in all packets on an interface. On ingress, mutation mapping occurs before traffic classification and all other actions. On egress, mutation mapping occurs after traffic classification and before all other actions.

Examples

Follow this example to apply a QoS DSCP-to-traffic class mutation map to a specific 40-gigabit Ethernet interface

```
device# configure terminal
device(config)# interface ethernet 2/2
device(conf-if-eth-2/2)# qos dscp-traffic-class dscp_tc_map
```

Follow this example to apply a QoS DSCP-to-traffic class mutation map to a specific port channel interface

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos dscp-traffic-class dscp_tc_map
```

qos-dscp-mode

This command is configures the mode selection for a VxLan Tunnel. When selected, the mode selection takes effect only at the *Egress VTEP*.

Syntax

qos-dscp-mode [**uniform** | **pipe**]

Syntax

[no] qos-dscp-mode [**uniform** | **pipe**]

Parameters

uniform

When set as *Uniform* mode. Post decapsulation at the Egress VTEP, the packet DSCP is copied from the incoming packet **outer** header DSCP value.

pipe

When set as *Pipe* mode. This is the default mode. Post decapsulation at the Egress VTEP, the packet DSCP is copied from the incoming packet **inner** DSCP value.

Modes

VXLAN Overlay Gateway Configuration mode

Usage Guidelines

This configuration is only available on the SLX 9150, SLX 9250, SLX 9740, Extreme 8520, Extreme 8720, and Extreme 8820 platforms.

Examples

The following example configures the default *Pipe* mode for VxLAN QoS.

```
SLX(config)# overlay-gateway 1
SLX(config-overlay-gw-1)# qos?
Possible completions:
    qos-dscp-mode Gateway QOS DSCP mode (Default: pipe)
SLX(config-overlay-gw-1)# qos-dscp-mode ?
Possible completions:
    pipe     Pipe
    uniform     Uniform
SLX(config-overlay-gw-1)# qos-dscp-mode pipe
```

qos flowcontrol

Configures link-level flow control (IEEE 802.3x Flow Control) in the transmission and reception direction on an interface or enables priority flow control on a CoS of an SLX 9150 or SLX 9250 interface.

Syntax

qos flowcontrol [**pfc** *CoS-number*]**tx** { **on** | **off** } **rx** { **on** | **off** }

no qos flowcontrol

Command Default

By default, link-level flow control (LLFC) reception is enabled.

Parameters

pfc *CoS-number*

(Optional) Enables priority flow control (PFC) on the specified CoS of an SLX 9150 or SLX 9250 interface. For the *CoS-number* variable, enter an integer from 0 to 7.

tx { **on** | **off** }

Activates or deactivates the transmission portion of flow control.

rx { **on** | **off** }

Activates or deactivates the reception portion of flow control.

Modes

Interface configuration mode

Usage Guidelines

LLFC alleviates system congestion by pausing data transmission. LLFC allows a congested receiver to communicate a PAUSE frame to a transmitter to stop data transmission until the congestion is cleared.

The device supports the transmission (Tx) and reception (Rx) of PAUSE frames for each physical interface or port channel.

LLFC can be configured only at the interface level.

Before configuring LLFC on an interface, stop the traffic on the interface.

Use the **no** form of this command to reset the default behavior.

Examples

The following example configures flow control on an interface.

```
device# configure terminal
device(config)# interface ethernet 1/4
device(conf-eth-1/4)# qos flowcontrol tx on rx on
```

The following example enables PFC on CoS 2 of an SLX 9150 interface.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-eth-0/1)# qos flowcontrol pfc 2 tx on rx on
```

qos map cos-mutation

Creates a QoS map for performing CoS-to-CoS mutation.

Syntax

qos map cos-mutation *name cos0 cos1 cos2 cos3 cos4 cos5 cos6 cos7*

no qos map cos-mutation *name*

Command Default

No CoS-to-CoS mutation QoS maps are defined.

Parameters

name

Specifies a unique name across all CoS-to-CoS mutation QoS maps defined within the system. If the named CoS-to-CoS mutation QoS map does not exist, then it is created. If the named CoS-to-CoS mutation QoS map already exists, then it is updated and new mapping is automatically propagated to all interfaces bound to the QoS map.

cos#

Specifies the outbound CoS value.

CoS value	Description
cos0	Sets the outbound CoS value for all packets with inbound CoS 0.
cos1	Sets the outbound CoS value for all packets with inbound CoS 1.
cos2	Sets the outbound CoS value for all packets with inbound CoS 2.
cos3	Sets the outbound CoS value for all packets with inbound CoS 3.
cos4	Sets the outbound CoS value for all packets with inbound CoS 4.
cos5	Sets the outbound CoS value for all packets with inbound CoS 5.
cos6	Sets the outbound CoS value for all packets with inbound CoS 6.
cos7	Sets the outbound CoS value for all packets with inbound CoS 7.

Modes

Global configuration mode

Usage Guidelines

A CoS-to-CoS mutation takes an inbound CoS value and maps it to an outbound CoS value. The inbound CoS value is the user priority after any interface ingress QoS trust and Interface default CoS policy have been applied. The outbound CoS value is used in selecting Traffic Class and egress packet marking.

Enter **no qos map cos-mutation** *name* command to delete the named CoS-to-CoS mutation QoS map. A QoS map can only be deleted if it is not bound to any interface.

Examples

To create a CoS-to-CoS QoS mutation map to swap CoS 4 and CoS 5 and apply it on an interface, for example having inbound CoS 4 mapped to outbound CoS 5 and inbound CoS 5 mapped to outbound CoS 4; but all other CoS values go through unchanged:

```
device# configure terminal
device(config)# qos map cos-mutation cosMap 0 1 2 3 5 4 6 7
device(config)# interface ethernet 2/1
device(conf-if-eth-2/1)# qos cos-mutation cosMap
```

To delete a CoS-to-CoS QoS mutation map:

```
device# configure terminal
device(config)# no qos map cos-mutation cosMap
```

qos map cos-mutation

Creates a QoS CoS mutation map.

Syntax

qos map cos-mutation *map-name*

Parameters

map-name

The name of the QoS CoS mutation map to be created. The name can be up to 64 characters. It should start with an alphabet and can only contain - (hyphen) and _ (underscore) special characters.

Modes

Global Configuration Mode

Usage Guidelines

This command creates a QoS CoS Mutation map and further configuration must be performed within its context.

Supported In

SLX 9740 and Extreme 8820

Examples

The following example shows how to create a QoS CoS mutation map.

```
SLX# configure terminal
SLX (config)# qos map cos-mutation test-cos-mut-map-1
SLX (cos-mutation-test-cos-mut-map-1)#
```

The following example shows how to delete an existing QoS CoS mutation map.

```
SLX# configure terminal
SLX (config)# no qos map cos-mutation test-cos-mut-map-1
SLX (config)#
```

Related Commands

- map cos to cos on page 1080
- qos cos-mutation on page 1424
- show qos maps cos-mutation on page 2259

qos map cos-traffic-class

Configures a QoS CoS-to-traffic-class mutation map.

Syntax

qos map cos-traffic-class *name*

no qos map cos-traffic-class *name*

Command Default

If CoS-to-traffic class mutation map is not defined, the default CoS-to-traffic class map is used, which is a one-to-one map for each priority.

Parameters

name

Specifies a unique name for the CoS-to-traffic class mutation QoS map. If the named map does not exist, then it is created. If the map already exists, then it is updated and new mapping is automatically propagated to all interfaces bound to the map.

Modes

Global configuration mode

Usage Guidelines

A CoS-to-traffic class mutation map takes an inbound CoS value and maps it to an outbound traffic class (priority queue) value. The inbound CoS value is the user priority after any interface ingress QoS trust and Interface default CoS policy have been applied.

Use the **no** form of the command to delete the named map.

A QoS map can only be deleted if it is not bound to an interface.

Examples

This example creates a QoS CoS-to-traffic-class mutation map and assigns it to the specified Ethernet interface. The *drop-precedence* parameter is mandatory.

```
device# configure terminal
device(config)# qos map cos-traffic-class tcmap1
device(cos-traffic-class-tcmap1)# map cos 2 to traffic-class 4 drop-precedence 0
device(cos-traffic-class-tcmap1)# map cos 3 to traffic-class 4 drop-precedence 1
device(cos-traffic-class-tcmap1)# map cos 3 to traffic-class 6 drop-precedence 1
device(cos-traffic-class-tcmap1)# interface ethernet 1/1
device(conf-if-eth-1/1)# qos cos-traffic-class tcmap1
```

This example removes the mutation map that is bound to the specified Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1
device(conf-if-eth-1/1)# no qos cos-traffic-class tcmap1
device(conf-if-eth-1/1)# exit
device(config)# no qos map cos-traffic-class tcmap1
```

qos map dscp-cos

Creates a QoS map where the ingress DSCP value is mapped to outgoing 802.1P values. This configures a DSCP-to-CoS map on the ingress interface.

Syntax

qos map dscp-cos *name*

no qos map dscp-cos *name*

map dscp *ingress dscp values* **to cos** *cos*

Command Default

DSCP-to-CoS mutation is not enabled.

Parameters

name

Name of DSCP-to-CoS map

map dscp

Ingress DSCP values.

cos

Egress CoS values.

ingress dscp values

Input DSCP values. The range of ingress DSCP values is 0 through 63.

cos

CoS value. The range is 0 through 7.

Modes

dscp-cos mode for the QoS **map dscp** commands

Global configuration mode

Usage Guidelines

This command remaps the incoming DSCP values of the ingress packet to egress CoS 802.1P values.

When you enter **qos map dscp-cos**, the system is placed in dscp-cos mode for the configured map. At this point, you can map ingress DSCP values to egress CoS values using the **map dscp** command.

Enter **qos dscp-cos** *name* while in configuration mode for a specific interface to apply the DSCP-to-CoS map to that interface.

Enter **no qos dscp-cos** *name* while in the interface configuration mode to remove the DSCP-to-CoS map from the interface.

Enter **no map dscp-cos** *name* while in global configuration mode to remove the DSCP-to-CoS map.

Examples

To create a QoS DSCP-to-CoS map and place system into dscp-cos mode:

```
device# configure terminal
device(config)# qos map dscp-cos test
device(dscp-cos-test)#
```

To map an ingress DSCP value to egress CoS value while in dscp-cos mode:

```
device# configure terminal
device(config)# qos map dscp-cos test
device(dscp-cos-test)# map dscp 43 to cos 4
```

To map multiple ingress DSCP values to egress CoS values while in dscp-cos mode:

```
device# configure terminal
device(config)# qos map dscp-cos test
device(dscp-cos-test)# map dscp 43 to cos 4
device(dscp-cos-test)# map dscp 63 to cos 6
device(dscp-cos-test)# map dscp 53 to cos 5
device(dscp-cos-test)# map dscp 23 to cos 2
```

To remove a QoS DSCP-CoS map while in global configuration mode:

```
device# configure terminal
device(config)# no qos map dscp-cos test
```

qos map dscp-mutation

Creates a DSCP mutation by mapping the incoming DSCP value of the ingress packet to outgoing DSCP values.

Syntax

qos map dscp-mutation *name*

no map qos dscp-mutation *name*

map dscp *ingress dscp values* **to dscp** *egress dscp value*

Command Default

DSCP mutation is not enabled.

Parameters

name

Name of DSCP mutation map

map dscp

Inbound DSCP values.

ingress dscp values

The ingress DSCP values. The range is from 0 through 63.

dscp

Outbound DSCP values.

egress dscp values

The egress DSCP value. The range is from 0 through 63.

Modes

dscp-mutation mode for the DSCP mutation map

Global configuration mode

Usage Guidelines

Enter **qos dscp-mutation** *name* while in configuration mode for a specific interface to apply the DSCP mutation map to that interface. When you enter **qos map dscp-mutation**, the system is placed in dscp-mutation mode for the configured map. At this point, you can map ingress DSCP values to egress DSCP values using the **dscp map** command.

Enter **no qos dscp-mutation** *name* while in interface configuration mode to remove the DSCP mutation map from that interface.

Enter **no map dscp-mutation** *name* while in global configuration mode to remove the DSCP mutation map.

Examples

To create a QoS DSCP mutation map and place system into dscp-mutation mode:

```
device# configure terminal
device(config)# qos map dscp-mutation test
device(dscp-mutation-test)#
```

To map an ingress DSCP value to egress DSCP values while in dscp-mutation mode:

```
device# configure terminal
device(config)# qos map dscp-mutation test
device(dscp-mutation-test)# map dscp 1,3,5,7 to dscp 40
```

To map multiple ingress DSCP values to egress DSCP values while in dscp-mutation mode:

```
device# configure terminal
device(config)# qos map dscp-mutation test
device(dscp-mutation-test)# map dscp 60 to dscp 40
device(dscp-mutation-test)# map dscp 24 to dscp 50
device(dscp-mutation-test)# map dscp 33 to dscp 35
device(dscp-mutation-test)# map dscp 53 to dscp 61
```

To remove a QoS DSCP mutation map while in global configuration mode:

```
device# configure terminal
device(config)# no qos map dscp-mutation test
```

qos map dscp-traffic-class

Creates a QoS map for performing DSCP-to-traffic class mapping. You use the **qos traffic-class-dscp** command to apply the map to an interface.

Syntax

qos map dscp-traffic-class *name*

no qos map dscp-traffic-class *name*

map dscp *ingress dscp values* **to traffic-class** *traffic class* [**drop-precedence** *out drop precedence*]

Command Default

DSCP-to-traffic class mutation is not enabled.

Parameters

name

Name of the QoS DSCP-to-traffic clas map.

map dscp

Ingress DSCP values. The range of ingress DSCP values is 0 through 63.

traffic-class

Egress traffic class values. The range of ingress traffic class values is from 0 through 7.

drop-precedence

Drop precedence value given egress packets. The range is 0 through 3.

ingress dscp values

Range of input DSCP values. The range is 0 through 63.

traffic class

The traffic class value. the range is from 0 through 7.

out drop precedence

Value of the output drop precedence. The range is 0 through 3.

Modes

dscp-traffic-class mode for the DSCP-to-traffic class map

Global configuration mode

Usage Guidelines

Enter **qos dscp-traffic-class** *name* to apply the QoS DSCP-Traffic-Class map to that interface. When you enter **qos map dscp-traffic-class**, the system is placed in dscp-traffic-class mode for the configured map. At this point, you can map ingress DSCP values to traffic class values using the **mark** command.

Enter **no qos dscp-traffic-class** *name* while in the interface mode to remove the map from that interface.

Note
This command is is supported on the Extreme 8820, Extreme 8720, Extreme 8520, SLX 9740, SLX 9250, and SLX 9150 devices only.

Examples

This example creates a QoS DSCP-to-traffic class map and places the system into dscp-traffic-class mode.

```
device# configure terminal
device(config)# qos map dscp-traffic-class test
device(dscp-traffic-class-test)#
```

This example maps ingress DSCP values to a traffic class.

```
device# configure terminal
device(config)# qos map dscp-traffic-class test
device(dscp-traffic-class-test)# map dscp 1,3,5,7 to traffic-class 1 drop-precedence 1
```

This example maps multiple ingress DSCP values to traffic classes and drop precedence.

```
device# configure terminal
device(config)# qos map dscp-traffic-class test
device(dscp-traffic-class-test)# map dscp 10 to traffic-class 3 drop-precedence 1
device(dscp-traffic-class-test)# map dscp 40 to traffic-class 4 drop-precedence 1
device(dscp-traffic-class-test)# map dscp 45 to traffic-class 5 drop-precedence 0
device(dscp-traffic-class-test)# map dscp 52 to traffic-class 3 drop-precedence 1
```

This example removes a QoS DSCP-traffic-class map.

```
device# configure terminal
device(config)# no qos map dscp-traffic-class test
```

qos map traffic-class-cos

A QoS traffic class-to-CoS mutation map can be configured to create a priority mapping table using a traffic-class-cos map. The traffic class-to-CoS map is then applied to an egress interface to effect the priority re-mapping.

Syntax

qos map traffic-class-cos name

no qos map traffic-class-cos *name*

Command Default

If a QoS traffic class-to-CoS mutation map is not defined, the default traffic class-to-CoS map is used, which is a one-to-one map for each priority.

Parameters

name

Specifies a unique name for the QoS traffic class-to-CoS mutation map. If the named map does not exist, then it is created. If the map already exists, then it is updated and new mapping is automatically propagated to all interfaces bound to the map.

Modes

Global configuration mode

Usage Guidelines

A traffic class can be mapped to the outgoing PCP value when a packet egresses the switch. You can create a priority mapping table using a traffic class-to-CoS map. This traffic class-to-CoS map can then be applied to an egress interface to effect the priority re-mapping. This feature only maps the internal traffic class to outgoing priority.

Enter **no qos map traffic-class-cos** *name* command to delete the named QoS traffic class-to-CoS mutation map.

A QoS map can only be deleted if it is not bound to an interface.

This command is not available on the SLX 9740 and Extreme 8820 devices.

Supported In

SLX 9150, SLX 9250, Extreme 8520, and Extreme 8720

Examples

To create and apply a QoS traffic class-to-CoS mutation map use the following command:

```
 device# configure terminal
device(config)# qos map traffic-class-cos CoSMap
device(traffic-class-cos-CoSMap)# map traffic-class 3 drop-precedence 1 to cos 2
device(traffic-class-cos-CoSMap)# map traffic-class 4 drop-precedence 1 to cos 3
device(traffic-class-cos-CoSMap)# map traffic-class 5 drop-precedence 2 to cos 4
device(conf-if-eth-1/4)# qos traffic-class-cos tcCos1
```

To delete a QoS traffic class-to-CoS mutation map that is bound to an interface follow this example.

```
 device# configure terminal
device(config)# interface ethernet 1/4
device(conf-if-eth-1/4)# no qos traffic-class-cos CoSMap
device(conf-if-eth-1/4)# exit
device(config)# no qos map traffic-class-cos CoSMap
```

qos port-speed-up

Increases the egress throughput rate on a Traffic Manager port on 10G or 100G ports.

Syntax

qos port-speed-up *rate*

no qos port-speed-up

Parameters

rate

Increased rate in thousand bits per second. For a 10G port, enter an integer from 300000 to 13000000 (equivalent to 300Mb to 13Gb). For a 100G port, enter an integer from 300000 to 130000000 (equivalent to 300Mb to 130Gb).

Command Default

The default throughput rate of the port.

Modes

Interface configuration mode

Usage Guidelines

Use the **no** form of the command to reset the default setting.

If you configured a breakout connector on an Ethernet interface, you can also increase the egress throughput rate on the breakout port.

The maximum speed supported by an interface is 130% of the default interface speed.

Examples

The following example increases the egress throughput rate by 300Mb on Ethernet port 0/1.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# qos port-speed-up 300000
```

The following example increases the egress throughput rate by 325Mb on Ethernet breakout port 0/53:4.

```
device# configure terminal
device(config)# interface ethernet 0/53:4
device(conf-if-eth-0/53:4)# qos port-speed-up 325000
```

qos random-detect traffic-class

Configures Random Early Detect (RED) profile on a traffic class of an interface

Syntax

qos random-detect traffic-class *traffic-class* **drop-precedence** *value* **red-profile-id** *ID*

no qos random-detect traffic-class *traffic-class* **drop-precedence**

Parameters

traffic-class

Specifies the traffic class to apply the RED profile. Enter an integer from 0 through 7.

drop-precedence *value*

Specifies the drop precedence value for the traffic class. Enter an integer from 1 from 3.

red-profile-id *ID*

Specifies the RED profile to assign to traffic class on the interface. Enter the identifier for a configured profile.

Modes

Interface configuration mode

Usage Guidelines

Use the **no** form of the command to remove the RED profile from the interface or the drop precedence for the traffic class on the interface.

Examples

The following example configures a RED profile on an interface.

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# qos random-detect traffic-class 4 drop-precedence 1 red-profile-id 22
```

qos red-profile

Configures a weighted random early detection (WRED) profile which includes the setting of the thresholds and drop probability by percentage. The command also enables or disable Explicit Congestion Notification (ECN) feature.

Syntax

qos red-profile *profile-ID* **min-threshold** *min-percentage* **max-threshold** *max-percentage* **drop-probability** *percentage* **ecn** { *on* | *off* }

no qos red-profile *profile-ID*

Parameters

profile-ID

Specifies the profile identifier. Enter an integer from 0 to 383.

min-threshold *min-percentage*

Specifies the minimum average queue size in percentage for randomly dropping packets. Enter an integer from 0 through 100.

max-threshold *max-percentage*

Specifies the maximum average queue size in percentage which all packets are accepted by the device. Enter an integer from 0 through 100.

drop-probability *percentage*

Specifies the drop probability in percentage when the queue size is at the maximum. Enter an integer from 0 through 100.

ecn *on off*

Enables or disables Explicit Congestion Notification (ECN) feature.

Modes

Global configuration mode

Usage Guidelines

You can configure a maximum on 256 profiles.

After configuring the profile, apply it to an interface with the **qos random-detect traffic-class** command.

Use the **no** form of this command to delete the profile.

Use the **ecn {on | off}** command to enable or disable Explicit Congestion Notification (ECN) for this device. ECN allows the routers and switches to signal the traffic end-points of the congestion without dropping any frames, and thus the end-

points can adjust their transmission rates without the added latency and jitter that would have been introduced by dropped frames.

When a device detects a congestion, it is imperative that the device indicates to the other end-points about the congestion as soon as it is detected. Since a congestion in one direction need not imply a congestion in its opposite direction, this device has to indicate to the other end-point so that it, the other end-point, can take appropriate action.

ECN requires that Random Early Detection (RED) profiles are created using the **red-profile** command and applied to the interface. ECN is only available for Unicast frames.

Examples

The following example is a WRED configuration.

```
device# configure terminal
device(config)# qos red-profile 1 min-threshold 30 max-threshold 60 drop-probability 44
ecn on
```

qos remark dscp

Enables Remark DSCP for physical and Port Channel interfaces.

Syntax

[no] qos remark dscp

Modes

Interface Configuration Mode

Usage Guidelines

Interface must be configured as switchport to enable remark DSCP.

The `no` form of the command disables remark DSCP on the interface.

This feature is supported on SLX 9150, SLX 9250, Extreme 8720, and Extreme 8520 devices.

Examples

The following example enables Remark DSCP on an ethernet interface.

```
NH3(conf-if-eth-0/4)# qos remark dscp
NH3# show run int eth 0/4
interface Ethernet 0/4
switchport switchport mode access
switchport access vlan 1
qos remark dscp
no shutdown
!
```

qos rx-queue cos-threshold

Configures the QoS ingress queue cost of service (CoS) thresholds.

Syntax

qos rx-queue cos-threshold *threshold_value_0 threshold_value_1 threshold_value_2 threshold_value_3 threshold_value_4 threshold_value_5 threshold_value_6 threshold_value_7*

[no] qos rx-queue cos-threshold

Command Default

The CoS threshold values for the ingress queue are not configured.

Parameters

threshold_value_n

There are eight entries for this parameter with each entry representing a percentage. Each position matches a specific inbound CoS with the first position (**cos_threshold_0**) representing CoS 0, the second CoS 1, and so on.

Modes

Ethernet interface configuration mode.

Usage Guidelines

The total of all the entries cannot exceed 100%.

A 0 may be entered for any of the values.

Examples

Follow this example to configure the QoS ingress queue CoS thresholds on a specific Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# qos rx-queue cos-threshold 10 10 10 10 10 20 20 10
```

qos rx-queue multicast

Configures the multicast packet handling on an interface for virtual output queueing.

Syntax

qos rx-queue multicast { **best-effort-rate** | **guarantee-rate** } *kbps*

qos rx-queue multicast traffic class *number* **min-queue-size** *Mbytes* **max-queue-size** *Mbytes*

no qos rx-queue multicast best-effort-rate | **guarantee-rate**

no qos rx-queue multicast traffic class *number* **min-queue-size** *Mbytes* **max-queue-size** *Mbytes*

Parameters

best-effort-rate *kbps*

Specifies the multicast best effort data rate in kilobits per second (kbps). Enter an integer from 704 through 600000000.

guarantee-rate *kbps*

Specifies the multicast data guarantee data rate in kilobits per second (kbps). Enter an integer from 704 through 600000000.

traffic class *number*

Specifies the traffic class on the interface. Enter an integer from 0 to 7.

min-queue-size *Mbytes*

Specifies the minimum queue size in megabytes per second. Enter an integer from 0 through 1024.

max-queue-size *Mbytes*

Specifies the maximum queue size in megabytes per second. Enter an integer from 0 through 2048.

Modes

Interface configuration mode

Usage Guidelines

Use the **no** form of this command to remove the packet handling configuration.

Examples

The following example configures the multicast packet handling on the interface for virtual output queueing.

```
device# configure terminal
device(config)# interface ethernet 1/2
```

```
device(conf-if-eth-1/2)# qos rx-queue multicast best-effort-rate 3000
device(conf-if-eth-1/2)# qos rx-queue multicast guarantee-rate 30000
device(conf-if-eth-1/2)# qos rx-queue multicast traffic-class 3 min-queue-size 512 max-
queue-size 1024
```

qos rx-queue unicast traffic-class

Configures the ingress queue unicast packet traffic class parameter on an Ethernet interface.

Syntax

qos rx-queue unicast traffic-class *traffic_class* **min-queue-size** *minimum_size* **max-queue-size** *maximum_size*

no qos rx-queue unicast traffic class *number* **min-queue-size** *Mbytes* **max-queue-size** *Mbytes*

Parameters

traffic class *number*

Specifies the traffic class on the interface. Enter an integer from 0 to 7.

min-queue-size *Mbytes*

Specifies the minimum queue size in megabytes per second. Enter an integer from 0 through 1024.

max-queue-size *Mbytes*

Specifies the maximum queue size in megabytes per second. Enter an integer from 0 through 2048.

Modes

Ethernet interface configuration mode

Examples

The following example configures tan Ethernet interface ingress queue minimum and maximum queue size by a traffic class. .

```
device# configure terminal
device(config)# interface ethernet 1/2
device(conf-if-eth-1/2)# qos rx-queue unicast traffic-class 3 min-queue-size 128 max-
queue-size 1024
```

qos service-policy

Applies a policy map to all inbound traffic.

Syntax

qos service-policy in *service_policy_name*

no qos service-policy in *service_policy_name*

Parameters

in

Applies the service policy to inbound traffic.

service_policy_name

The name of the policy map.

Modes

Global configuration mode.

Usage Guidelines

The policy map has been preconfigured.

Enter **no qos service-policy in** *service_policy_name* to return to the default.

Examples

This example binds a service policy to inbound traffic at the system level.

```
device# configure terminal
device(config)# qos service-policy in policyMap1
device(config-service-policy-in/policyMap1)# end
```

qos traffic-class

Applies a QoS default traffic class value to an interface.

Syntax

qos traffic-class *default_tc_value*

Command Default

No explicit user configured QoS default traffic class priority value is configured.

Parameters

default_tc_value

The assigned traffic class priority value. The traffic class priority values range from 0 through 7.

Modes

Interface configuration mode

Examples

Follow this example to apply a default traffic class value to a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 1/3
device(conf-if-eth-1/3)# qos traffic-class 3
```

Follow this example to apply a default traffic class value to a specific port channel interface:

```
device# configure terminal
device(config)# interface port-channel 22
device(config-port-channel-22)# qos traffic-class 3
```

qos traffic-class-cos

Applies a user configured QoS traffic class-to-CoS mutation map to an interface.

Syntax

qos traffic-class-cos *tc_cos_map*

Command Default

No explicit user configured QoS traffic class-to-CoS mutation maps are applied. The outbound traffic class equals the inbound traffic class.

Parameters

tc_cos_map

The name of the user configured QoS traffic class-to-CoS mutation map.

Modes

Interface configuration mode.

Usage Guidelines

The mutation maps are preconfigured.

Mutation mapping is a method of modifying a QoS field in all packets on an interface. On ingress, mutation mapping occurs before traffic classification and all other actions. On egress, mutation mapping occurs after traffic classification and before all other actions.

Supported In

SLX 9150, SLX 9250, Extreme 8520, and Extreme 8720

Examples

Follow this example to apply a user configured QoS traffic class-to-CoS mutation map to an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# qos traffic-class-cos tc_cos_map
```

Follow this example to apply a user configured QoS traffic class-to-CoS mutation map) to a port channel interface.

```
device# configure terminal
```

```
device(config)# interface port-channel 22
device(config-port-channel-22)# qos traffic-class-cos tc_cos_map
```

qos trust dscp

Enables Trust DSCP for Layer 2 Physical and Port Channel interfaces.

Syntax

[no] qos trust dscp

Modes

Interface Configuration Mode

Usage Guidelines

The interface must be configured as a switchport to enable Trust DSCP.

The `no` form of the command disables Trust DSCP on the interface.

Examples

The following example enables Trust DSCP on the ethernet interface 0/4.

```
SLX(conf-if-eth-0/4)# qos trust dscp
SLX show run int eth 0/4
 interface Ethernet 0/4
 switchport
 switchport mode access
 switchport access vlan 1
 qos trust dscp
 no shutdown
 !
```

qos-mpls map dscp-exp

Creates and populates an MPLS QoS differentiated services code point (DSCP) to EXP mutation map.

Syntax

qos-mpls map dscp-exp *mapname* { **dscp** *dscp_value* **to exp** *exp_value* }

[no] qos-mpls map dscp-exp *mapname* [**dscp** *dscp_value*]

Parameters

mapname

The name of the MPLS QoS DSCP-to-EXP mutation map. The name can be up to 64 characters.

dscp

Sets the ingress DSCP value.
dscp_value

The ingress DSCP value. The range is from 0 through 63.

exp

Specifies that the egress EXP value follows.
exp_value

The egress EXP value. The range is from 0 through 7.

Modes

Global configuration mode

`dscp-exp-mapname` configuration mode

Usage Guidelines

Creating the map and setting the initial mutation places the device into `dscp-exp-mapname` configuration mode where you continue to populate the map using the **dscp** command.

MAC filter and DSCP marking cannot be configured on the same port.

This command is supported on the Extreme 8820 and SLX 9740 devices only.

Examples

Follow this example to create an MPLS QoS DSCP-to-EXP mutation map.

```
device# configure terminal
device(config)# qos-mpls map dscp-exp dscpExpMap dscp 0 to exp 1
device(dscp-exp-dscpExpMap)# dscp 3 to exp 2
```

```
device(dscp-exp-dscpExpMap)# dscp 17 to exp 4
device(dscp-exp-dscpExpMap)# dscp 61 to exp 5
```

qos-mpls map exp-dscp

Creates and populates an MPLS QoS EXP to differentiated services code point (DSCP) mutation map.

Syntax

qos-mpls map exp-dscp *mapname* { **exp** *exp_value* **to dscp** *dscp_value* }

[no] qos-mpls map exp-dscp *mapname* [**exp** *exp_value*]

Parameters

mapname

The name of the MPLS QoS EXP-to_DSCP mutation map. The name can be up to 64 characters.

exp

Sets the ingress EXP value.
exp_value

The ingress EXP value. The range is from 0 through 7.

dscp

Specifies that the egress DSCP value follows.
dscp_value

The egress DSCP value. The range is from 0 through 63.

Modes

Global configuration mode

`exp-dscp-mapname` configuration mode

Usage Guidelines

Creating the map and setting the initial mutation places the device into `exp-dscp-mapname` configuration mode where you continue to populate the map using the **exp** command.

This command is supported on the Extreme 8820 and SLX 9740 devices only.

Examples

Follow this example to create an MPLS QoS EXP-to-DSCP mutation map.

```
device# configure terminal
device(config)# qos-mpls map exp-dscp expDscpMap exp 1 to dscp 2
device(exp-dscp-expDscpMap)# exp 2 to dscp 4
device(exp-dscp-expDscpMap)# exp 4 to dscp 8
device(exp-dscp-expDscpMap)# exp 6 to dscp 12
```

qos-mpls map exp-traffic-class

Creates and populates an MPLS QoS EXP to traffic class mutation map.

Syntax

qos-mpls map exp-traffic-class *mapname* { **exp** *exp_value* **to traffic-class** *traffic_class_value* **drop-precedence** *drop_precedence_value* }

[no] qos-mpls map exp-traffic-class *mapname* [**exp** *exp_value*]

Parameters

mapname

The name of the MPLS QoS EXP-to-traffic class mutation map. The name can be up to 64 characters.

exp

Sets the ingress EXP value.
exp_value

The ingress EXP value. The range is from 0 through 7.

traffic-class

Specifies that the egress traffic class value follows.
traffic_class_value

The egress traffic class value. The range is from 0 through 63.

drop-precedence

Specifies that the traffic class drop precedence value follows.
drop_precedence_value

The egress traffic class drop precedence value. The range is from 0 through 3.

Modes

Global configuration mode

`exp-traffic-class-mapname` configuration mode

Usage Guidelines

Creating the map and setting the initial mutation places the device into `exp-traffic-class-mapname` configuration mode where you continue to populate the map using the **exp** command.

This command is supported on the Extreme 8820 and SLX 9740 devices only.

Examples

Follow this example to create an MPLS QoS EXP-to-traffic class mutation map.

```
device# configure terminal
device(config)# qos-mpls map exp-traffic-class expTCMap exp 1 to traffic-class 2 drop-
precedence 2
device(exp-traffic-class-expTCMap)# exp 2 to traffic-class 4 drop-precedence 2
device(exp-traffic-class-expTCMap)# exp 4 to traffic-class 8 drop-precedence 2
device(exp-traffic-class-expTCMap)# exp 6 to traffic-class 12 drop-precedence 2
```

qos-mpls map-apply dscp-exp

Applies an MPLS DSCP to EXP mutation map globally.

Syntax

qos-mpls map-apply dscp-exp { *map_name* | **all-zero-map** } { **all** }

[no] qos-mpls map-apply dscp-exp

Parameters

map_name

The name of the user-defined map that you are applying.

all-zero-map

Maps the DSCP values to EXP 0.

all

Applies the map globally.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the Extreme 8820 and SLX 9740 devices only.

Examples

Follow this example to apply a MPLS DSCP to EXP mutation map.

```
device# configure terminal
device(config)# qos-mpls map-apply dscp-exp dscpExpMap all
```

qos-mpls map-apply exp-dscp

Applies an MPLS EXP to DSCP mutation map globally.

Syntax

qos-mpls map-apply exp-dscp { *map_name* | **all-zero-map** } { **all** }

[no] qos-mpls map-apply exp-dscp

Parameters

map_name

The name of the user-defined map that you are applying.

all-zero-map

Maps the EXP values to DSCP 0.

all

Applies the map globally.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the Extreme 8820 and SLX 9740 devices only.

Examples

Follow this example to apply a MPLS EXP to DSCP mutation map.

```
device# configure terminal
device(config)# qos-mpls map-apply exp-dscp expDscppMap all
```

qos-mpls map-apply exp-traffic-class

Applies an MPLS EXP to traffic class mutation map globally.

Syntax

qos-mpls map-apply exp-traffic-class { *map_name* | **all-zero-map** } { **all** }

[no] qos-mpls map-apply exp-traffic-class

Parameters

map_name

The name of the user-defined map that you are applying.

all-zero-map

Maps the EXP values to internal traffic class 0 and drop precedence 0.

all

Applies the map globally.

Modes

Global configuration mode

Usage Guidelines

This command is supported on the Extreme 8820 and SLX 9740 devices only.

Examples

Follow this example to apply a MPLS EXP to traffic class mutation map.

```
device# configure terminal
device(config)# qos-mpls map-apply exp-traffic-class expTrafficClassMap all
```

qos-ttl-mode

Configures QoS support for MPLS policies and VXLAN Layer 2 gateways, Layer 3 gateways, and Layer 2 and Layer 3 gateway interconnections.

Syntax

qos-ttl-mode [**uniform** | **pipe**]

no qos-ttl-mode

Parameters

uniform

QoS is supported by the router MPLS policy or VXLAN gateway uniformly. This setting is the default.

pipe

QoS is supported by the router MPLS policy pipe or VXLAN gateway pipe.

Modes

Router MPLS policy configuration mode

VXLAN overlay gateway configuration mode

Usage Guidelines

Use the **no** form of the command to remove the QoS support from the router MPLS policy or VXLAN gateway.

Note
The gateway must first be configured with the **type layer2-extension** command for QoS support on the VXLAN gateway. For example, the following is displayed in the output when the **show overlay-gateway** command is entered:

```
Type Layer2-Extension, Tunnel mode VXLAN
```

MPLS is supported only on devices based on the DNX chipset family. For a list of such devices, see "Supported Hardware".

Examples

The following example shows how to configure uniform QoS support on a VXLAN gateway.

```
device# configure terminal
device(config)# overlay-gateway gateway_L2
device(config-overlay-gw-gateway_L2)# type layer2-extension
device(config-overlay-gw-gateway_L2)# ip interface loopback 1
device(config-overlay-gw-gateway_L2)# qos-ttl-mode uniform
```

```
device(config-overlay-gw-gateway_L2)# map vni auto
device(config-overlay-gw-gateway_L2)# activate
```

The following example shows how to configure QoS support on a VXLAN pipe.

```
device# configure terminal
device(config)# overlay-gateway gateway_L2
device(config-overlay-gw-gateway_L2)# type layer2-extension
device(config-overlay-gw-gateway_L2)# ip interface loopback 1
device(config-overlay-gw-gateway_L2)# qos-ttl-mode pipe
device(config-overlay-gw-gateway_L2)# map vni auto
device(config-overlay-gw-gateway_L2)# activate
```

The following example shows how to configure QoS support on the router MPLS policy pipe.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# qos-ttl-mode pipe
```

qos tx-queue scheduler strict-priority

Configures the strict priority (SP) value for the egress queue traffic class scheduler and assigns a deficit weighted round robin (DWRR) weight.

Syntax

qos tx-queue scheduler strict-priority *traffic_class dwrr dwrr_weight*

[no] qos tx-queue scheduler strict-priority *traffic_class dwrr dwrr_weight*

Command Default

The SP value for the egress queue traffic class scheduler is not configured.

Parameters

tarffic_class

There are eight raffic class values:

Value	Traffic class
0	No strict priority queue.
1	Traffic class 7 strict priority queue.
2	Traffic class 6 through 7 strict priority queues.
3	Traffic class 5 through 7 strict priority queues.
4	Traffic class 4 through 7 strict priority queues.
5	Traffic class 3 through 7 strict priority queues.
6	Traffic class 2 through 7 strict priority queues.
7	Traffic class 1 through 7 strict priority queues.

dwrr *dwrr_weight*

Configure the DWRR queue weights. There are eight entries for this parameter with each entry representing a percentage. Tthe total of all the entries cannot exceed 100%. Each entry position represents a specific traffic class:

Place	Assignment
1	Traffic class 0 DWRR weight.
2	Traffic class 1 DWRR weight.
3	Traffic class 2 DWRR weight.
4	Traffic class 3 DWRR weight.

Place	Assignment
5	Traffic class 4 DWRR weight.
6	Traffic class 5 DWRR weight.
7	Traffic class 6 DWRR weight.
8	Traffic class 7 DWRR weight.

Modes

Global configuration mode

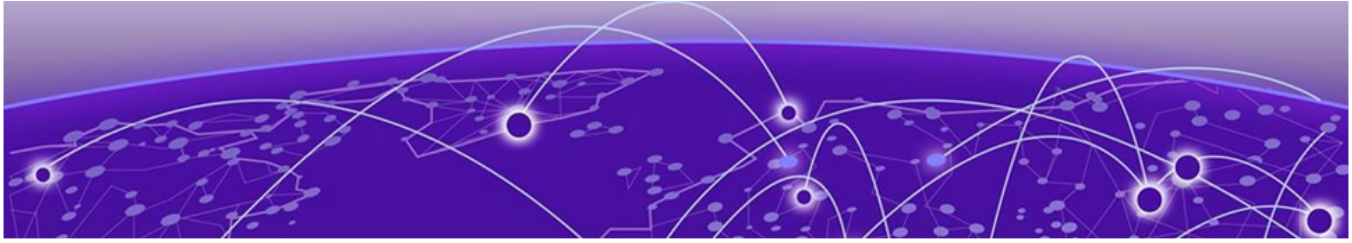
Usage Guidelines

The no form, of the command removes the SP value for the egress queue traffic class scheduler.

Examples

Use the following command to assign traffic classes 6 through 7 to a SP queue and assign DWRR weights.

```
device# configure terminal
device(config)# qos tx-queue scheduler strict-priority 2 dwrr 20 5 5 5 20 20
```



Commands R - Sh

radius-server host on page 1477
raps-default-mac on page 1480
raps-mel on page 1481
raslog-duration on page 1482
rate-monitoring on page 1483
rd (EVPN VLAN/BD) on page 1485
rd auto (EVPN) on page 1486
reconnect-time on page 1487
record on page 1488
record-route on page 1489
recovery-time on page 1490
redistribute on page 1491
redundant-management enable on page 1495
refresh-reduction on page 1496
region on page 1498
registrar-server on page 1499
registrar-port on page 1500
reliable-messaging on page 1501
reload on page 1503
reload-delay on page 1504
reload-delay enable on page 1505
remark on page 1506
remote-mep on page 1507
rename on page 1508
reoptimize-timer on page 1509
resequence access-list on page 1511
reservable-bandwidth on page 1513
resilient-hash on page 1515
retain route-target all on page 1517
retransmit-interval on page 1518
retries on page 1519
retry-limit on page 1520
retry-time on page 1521
reverse-metric on page 1522

revert-timer on page 1524
revertive global on page 1526
revertive hold-time on page 1528
revision on page 1529
rfc1583-compatibility (OSPF) on page 1530
rib-route-limit on page 1531
right-interface vlan on page 1533
rpl on page 1535
rpl-owner on page 1537
rpki priority on page 1538
server ssh on page 1539
server tcp on page 1541
rmon alarm on page 1543
rmon collection history on page 1545
rmon collection stats on page 1547
rmon event on page 1548
role name on page 1549
rollback apply checkpoint on page 1551
rollback checkpoint on page 1553
rollback enable on page 1555
root access console on page 1556
root enable on page 1557
route-map (BGP) on page 1558
route-precedence on page 1560
route-target on page 1562
route-target (EVPN) on page 1563
route-target (EVPN VLAN/BD) on page 1565
router bgp on page 1567
router isis on page 1568
router mpls on page 1569
router ospf on page 1570
router pim on page 1571
router-interface on page 1572
rp-address on page 1574
rp-candidate on page 1576
rpf ecmp rebalance on page 1578
rpf-mode on page 1579
rsvp on page 1581
rsvp-flooding-threshold on page 1582
rsvp-periodic-flooding-time on page 1584
rule on page 1585
rule-name on page 1587

rx-label-silence-time on page 1588
secure-port on page 1589
sample-recording on page 1590
scheduler on page 1592
seq (rules in IPv4 extended ACLs) on page 1594
seq (rules in IPv4 extended bACLs) on page 1599
seq (rules in IPv4 standard ACLs) on page 1603
seq (rules in IPv6 extended ACLs) on page 1606
seq (rules in IPv6 standard ACLs) on page 1611
seq (rules in IPv4 standard bACLs) on page 1614
seq (rules in MAC extended ACLs) on page 1617
seq (rules in MAC standard ACLs) on page 1623
service password-encryption on page 1625
service-policy (control plane) on page 1626
service-policy (interface) on page 1627
session on page 1629
set extcommunity on page 1631
set interface on page 1633
set ip dscp on page 1634
set ip interface null0 on page 1635
set ip mirror on page 1636
set ip next-hop on page 1637
set ipv6 interface null0 on page 1639
set ipv6 next-hop on page 1640
set large-community on page 1642
set large-community-list delete on page 1644
set police cir on page 1645
set sflow on page 1646
set traffic-action continue on page 1647
set-debug on page 1648
set-overload-bit on page 1649
sflow agent-address on page 1651
sflow collector on page 1653
sflow enable on page 1655
sflow polling-interval (global version) on page 1656
sflow sample-rate on page 1657
sflow update-destination-mac on page 1659
sflow update-dst-mac(global version) on page 1661
sflow source-interface on page 1662

radius-server host

Configures a RADIUS server to connect for external server authentication.

Syntax

radius-server host { *ip-address* | *host-name* } [**use-vrf** { **mgmt-vrf** | **default-vrf** |*vrf-name* }][**auth-port** *portnum*] [**radsec**] [**timeout** *secs*] [**retries** *num*] [**key** *shared-secret*] [**protocol** { **chap** | **pap** | **peap**}] [**encryption-level** *value-level*]

no radius-server host { *ip-address* | *host-name* } [**use-vrf** { **mgmt-vrf** | **default-vrf** |*vrf-name* }][**auth-port** *portnum*] [**radsec**] [**timeout** *secs*] [**retries** *num*] [**key** *shared-secret*] [**protocol** { **chap** | **pap** | **peap**}] [**encryption-level** *value-level*]

Command Default

By default, a RADIUS server is not configured.

Parameters

ip-address

Specifies the RADIUS server IP address. Both IPv4 and IPv6 addresses are supported.

host-name

Specifies the host name of the RADIUS server. The maximum supported length for the host name is 40 characters.

use-vrf

(Optional) Causes communication with the RADIUS server through a specific VRF and enters configuration mode for RADIUS server communications through that VRF.

mgmt-vrf

Specifies the management VRF.

default-vrf

Specifies the default-vrf.

vrf-name

Specifies a VRF name.

auth-port *portnum*

Specifies the port for authentication. The default is UDP port is 1812. The default TCP port (used for RADIUS over TLS) is 2083.

radsec

Specifies that RADIUS over TLS is to be used instead of RADIUS over UDP.

encryption-level*value-level*

Designates the encryption level for the shared secret key operation. This operand supports JITC certification and compliance. The valid values are 0 and 7, with 0 being clear text and 7 being the most heavily encrypted. The default value is 7.

key *shared-secret*

Specifies the text string that is used as the shared secret between the device and the RADIUS server to make the message exchange secure. The key must be between 1 and 40 characters in length.

In RADIUS over UDP mode, the default key is **sharedsecret**. In RADIUS over TLS mode, the default key is **radsec**, which must not be modified per RFC 6614.

The exclamation mark (!) is supported in RADIUS and TACACS+ servers. You can specify the password in either double quotes or with the escape character (\), for example **"secret!key"** or **secret\!key**. The only other valid characters are alphanumeric characters (a-z and 0-9) and underscores. No other special characters are allowed.

protocol {**chap** | **pap** | **peap**}

Specifies the authentication protocol. Options include CHAP, PAP, and PEAP. The default is CHAP.

retries *num*

Specifies the number of attempts allowed to connect to a RADIUS server. The default is 5 attempts.

Modes

Global configuration mode

Usage Guidelines

When a RADIUS server with the specified IP address or hostname does not exist, it is added to the server list. When the RADIUS server already exists, this command modifies the configuration.

The **no** form of the command removes the indicated configuration.

Note
When only one RADIUS is configured, you can remove the RADIUS server configuration only when both login (EXEC) and command accounting are disabled by using, for example, the **no aaa accounting** command and when the authentication mode has been set to "non-radius" with the **no aaa authentication login radius** command.

If the **encryption-level** is zero (0) but the key entered is encrypted then the following error message is displayed: `Error: Input key must be plain text when encryption-level selected is 0.`

Examples

This example configures a RADIUS server.

```
device# configure terminal
device(config)# radius-server host 10.24.65.6
device(config-radius-server-10.24.65.6/mgmt-vrf)#
```

This example configures a RADIUS server and specifies that communication with the server takes place through the green-vrf.

```
device# configure terminal
device(config)# radius-server host 10.24.65.6 use-vrf green-vrf
device(config-radius-server-10.24.65.6/green-vrf)#
```

raps-default-mac

Sets the default Ring Automatic Protection Switching (R-APS) destination MAC address for Ethernet Ring Protection (ERP).

Syntax

raps-default-mac

no raps-default-mac

Command Default

The default RAPS destination MAC address is 01:19:A7:00:00:01 for all ring ID and R-APS messages.

Modes

ERP configuration mode

Usage Guidelines

The device appends the number configured by this command to the end of the permanent portion of the ERP MAC address 01:19:A7:00:00:<01 or ERP ID> in R-APS messages. By default, 01:19:A7:00:00:01 is used as the destination MAC address, which is always used by Version 1 of ITU-T 8032.

If Version 2 is configured, use the **no raps-default-mac** command to revert to a non-default R-APS destination MAC address. The configured ERP ID appears as the last 8-bit number in the destination MAC address.

Examples

The following example sets a default R-APS destination MAC address.

```
device# configure terminal
device(config)# erp 1
device(config-erp-1)# raps-default-mac
```

raps-mel

Configures a Ring Automatic Protection Switching (R-APS) Maintenance Entity Group Level (MEL) value for Ethernet Ring Protection (ERP).

Syntax

raps-mel *mel_value*

no raps-mel

Command Default

The default is 7.

Parameters

mel_value

Specifies a R-APS MEL value. Range is from 0 through 7.

Modes

ERP configuration mode

Usage Guidelines

The R-APS MEL value is carried in ERP PDUs.

Use the **no** form of this command to revert to the default.

Examples

The following example configures a nondefault value.

```
device# configure terminal
device(config)# erp 1
device(config-erp-1)# raps-mel 5
```

raslog-duration

Configures the interval between RASLog messages that are sent when a port is disabled by the loop detection (LD) protocol.

Syntax

raslog-duration {*minutes* }

no raslog-duration

Command Default

See the Usage Guidelines.

Parameters

minutes

Message interval in minutes. Range is from 10 through 1440. The default is 10.

Modes

Protocol Loop Detection configuration mode

Usage Guidelines

Use the no form of this command to revert to the default interval.

Examples

To specify a RASLog message interval of 20 minutes:

```
device# configure terminal
device(config)# loop-detection
device(config-loop-detect)# raslog-duration
```

To revert to the default interval:

```
device# configure terminal
device(config)# loop-detection
device(config-loop-detect)# no raslog-duration 20
```

rate-monitoring

Adds the interface to a tracked list of interfaces monitored for link utilization.

Syntax

rate-monitoring threshold *threshold-value*

[no] rate-monitoring

Command Default

The default threshold is 90% (percent) of the initial rate. You can also configure a specific threshold value.

Parameters

threshold

threshold-value

Set a value in the range 100 to 256000000 kbps.

Modes

Maintenance sub-mode under Interface Configuration context.

Usage Guidelines

If **rate-monitoring**, under the Maintenance Mode sub-mode, is configured on an Ethernet or Port Channel interface, link utilization for that interface is monitored when maintenance mode is enabled.

The *no* format of the command removes the configured Ethernet or Port Channel interface from the list of monitored interfaces.

Note
This configuration must be applied on all uplinks from a Leaf to have optimum convergence.

When an interface, that is monitored on the SLX-OS device, shows a drop of 90% in traffic, the interface is then shutdown. When all monitored interfaces on the SLX-OS device are shutdown, then the device can enter into the Maintenance Mode.

Examples

The following example configures rate-monitoring to the default value on the ethernet interface 0/1.

```
SLX # configure terminal
SLX (config) # interface Ethernet 0/1
SLX (config-if-eth-0/1)# maintenance-mode
```

```
SLX (config-if-eth-0/1-maintenance)# rate-monitoring
SLX (conf-if-eth-0/1-maintenance)#
```

The following example configures rate-monitoring to a specific value on the ethernet interface 0/1.

```
SLX # configure terminal
SLX (config) # interface Ethernet 0/1
SLX (config-if-eth-0/1)# maintenance-mode
SLX (config-if-eth-0/1-maintenance)# rate-monitoring threshold 10000000
SLX (conf-if-eth-0/1-maintenance)# exit
SLX (conf-if-eth-0/1)# exit
SLX (config)#
SLX (config)# do show running-config interface Ethernet 0/1
interface Ethernet 0/1
  maintenance-mode
  rate-monitoring threshold 10000000
  !
  no shutdown
```

rd (EVPN VLAN/BD)

Configures a Virtual Private Network (VPN) route distinguisher for a VLAN/bridge domain (BD) in an Ethernet VPN (EVPN) default instance.

Syntax

rd { *admin-value*:*arbitrary-value* | *IP-address*:*arbitrary-value* }

Parameters

admin-value

The administrative number assigned to the route. This can be a local ASN number or an IP address. The ASN number can be either a 2-byte number (from 0 through 65535) or a 4-byte number (from 0 through 4294967295).

arbitrary-value

An arbitrary number you choose. The range of valid values is from 0 through 65535 if the ASN is is an IP address or a 2 byte ASN. The range is 0 through 4294967295 if the ASN is a 4 byte ASN.

IP-address

An IPv4 or IPv6 address.

Modes

EPVN VLAN/BD configuration mode

Examples

The following example configures an RD and assigns the local ASN number 200:1.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# bridge-domain 200
device(config-bridge-domain-200)# rd 200:1
```

The following example configures an RD and assigns the IP address 10.1.1.1:1.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# bridge-domain 200
device(config-bridge-domain-200)# rd 10.1.1.1:1
```

rd auto (EVPN)

Enables auto-generation of a route distinguisher (RD) for an Ethernet Virtual Private Network (EVPN) default instance.

Syntax

rd auto

no rd auto

Command Default

Disabled.

Modes

EVPN configuration mode

Usage Guidelines

Use the **no** form of this command to disable autogeneration of an RD.

Examples

The following example enables autogeneration of an RD on an EVPN default instance.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# rd auto
```

reconnect-time

Specifies the amount of time that a graceful restart (GR) neighbor must wait for the LDP session to be reestablished.

Syntax

reconnect-time *seconds*

no reconnect-time *seconds*

Command Default

The default reconnect time is 120 seconds.

Parameters

seconds

Specifies the amount of time in seconds that a GR neighbor must wait for the LDP session to be reestablished. This value is advertised to the neighbor using the FT Reconnect Timeout field in the FT Session TLV. Enter a integer from 60 to 300. The default setting is 120.

Modes

MPLS LDP GR configuration mode

Usage Guidelines

The **no** form of the command resets the default time of 120 seconds.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example sets the LDP GR timer to 180 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# graceful-restart
device(config-router-mpls-ldp-gr)# reconnect-time 180
```

record

The user can configure the record route option using the **record** command.

Syntax

record { **enable** | **disable** }

Command Default

The record route option is enabled by default.

Parameters

enable

Enables the record route option

disable

Disables the record route option.

Modes

MPLS router Bypass LSP configuration mode.

Usage Guidelines

When enabled, the RSVP session messages of the bypass LSP records the bypass LSP actual path.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example enables the record route option for bypass LSP *my-bypass-lsp*.

```
device>configure
device(config)# router mpls
device(config-router-mpls)# bypass-lsp my-bypass-lsp
device(config-router-mpls-bypass-lsp-my-bypass-lsp)# record enable
```

record-route

Use the **record-route** command's enable or disable options to set the record route option for the dynamic bypass LSPs to be created for the MPLS protected interface.

Syntax

record-route { **disable** | **enable** }

Command Default

Record route is enabled by default.

Parameters

disable

Disable the **record-route** command.

enable

Enables the **record-route** command.

Modes

MPLS router MPLS interface dynamic bypass configuration mode (config-router-mpls-if-ethernet-*slot/port*-dynamic-bypass).

Usage Guidelines

Based on the value of the parameter, dynamic bypass LSPs create with their record-route option enabled or disabled.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example enables record-route on the dynamic bypass MPLS Ethernet interface *0/8* .

```
device>configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/8
device(config-router-mpls-if-ethernet-0/8)# dynamic-bypass
device(config-router-mpls-if-ethernet-0/8-dynamic-bypass)#  record-route enable
```

recovery-time

Specifies the amount of time that this device retains its MPLS forwarding state across LDP graceful restart (GR).

Syntax

recovery-time *seconds*

no recovery-time *seconds*

Command Default

The default recovery time is 120 seconds.

Parameters

seconds

Specifies the amount of time in seconds that this router retains its MPLS forwarding state across restart. This value is advertised to the neighbor using the Recovery Time field in the FT Session TLV. Enter a integer from 60 to 3600.

Modes

MPLS LDP GR configuration mode

Usage Guidelines

The recovery time must be chosen accordingly taking into account the time it takes for RTM to recompute the routes and the number of Layer 3 FECs that need to be recovered as part of the LDP GR recovery. This is applicable to GR processing on ingress as well as transit LSRs.

The **no** form of the command resets the default time of 120 seconds.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example sets the LDP GR timer to 240 seconds.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# graceful-restart
device(config-router-mpls-ldp-gr)# recovery-time 240
```

redistribute

Configures the device to redistribute IPv4 and IPv6 routes from one routing domain to another.

Syntax

redistribute isis [**level-1** | **level-1-2** | **level-2** | **metric** *num* | **route-map** *string*]

redistribute isis { **level-1 into level-2** } [**prefix-list** *name*]

redistribute isis { **level-2 into level-1** } [**prefix-list** *name*]

redistribute ospf [**match** { **external1** | **external2** | **internal** } | **metric** *num* | **metric-type** { **type1** | **type2** } | **route-map** *string*]

redistribute { *source-protocol* } [**metric** *num* | **metric-type** { **type1** | **type2** } | **route-map** *string*]

redistribute { *source-protocol* } [**level-1** | **level-1-2** | **level-2** | **metric** *num* | **metric-type** { **type1** | **type2** } | **route-map** *string*]

no redistribute isis [**level-1** | **level-1-2** | **level-2 metric** *num* | **route-map** *string*]

no redistribute isis { **level-1 into level-2** } [**prefix-list** *name*]

no redistribute isis { **level-2 into level-1** } [**prefix-list** *name*]

no redistribute ospf [**match** { **external1** | **external2** | **internal** } | **metric** *num* | **metric-type** { **type1** | **type2** } | **route-map** *string*]

no redistribute { *source-protocol* } [**metric** *num* | **metric-type** { **type1** | **type2** } | **route-map** *string*]

Command Default

The device does not redistribute routing information.

Parameters

isis

Specifies the IS-IS protocol.

level-1

Specifies L1 LSP, L1 CSNP, and LI PSNP packets.

level-1-2

Specifies L1 LSP, L1 CSNP, and LI PSNP packets and L2 LSP, L2 CSNP, and L2 PSNP packets.

level-2

Specifies L2 LSP, L2 CSNP, and L2 PSNP packets.

metric *num*

Specifies a metric for redistributed routes. Valid values range from 1 through 65535 in OSPFv2 and OSPFv3 configuration mode. Valid values range from 1 through 4261412863 in ISIS address-family IPv4/IPv6 unicast configuration mode and BGP address-family IPv4/IPv6 unicast configuration mode.

route-map *string*

Specifies a route map to be consulted before a route is added to the routing table.

level-1 into level-2

Redistributes Level 1 routes into Level 2.

level-2 into level-1

Redistributes Level 2 routes into Level 1.

prefix-list *name*

Specifies a prefix-list.

ospf

Specifies the OSPF protocol.

match

Specifies the type of route.

external1

Specifies OSPF Type 1 external routes.

external2

Specifies OSPF Type 2 external routes.

internal

Specifies OSPF internal routes.

metric-type

Specifies the external link type associated with the default route advertised into the OSPF routing domain.

type1

Specifies a type 1 external route.

type2

Specifies a type 2 external route.

source-protocol

Specifies the source protocol from which routes are being redistributed. It can be one of the following keywords: **bgp**, **connected**, or **static**.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

ISIS address-family IPv4 unicast configuration mode

ISIS address-family IPv6 unicast configuration mode

OSPF router configuration mode

OSPFv3 router configuration mode

OSPF router VRF configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Routes can be filtered by means of an associated route map before they are distributed.

The **metric-type** { **type1** | **type2** } option is only available in OSPFv3 router, OSPFv3 router VRF, and ISIS address-family /IPv4/IPv6 unicast configuration mode.

The **redistribute** { *source-protocol* } [**level-1** | **level-1-2** | **level-2**] option is only available in ISIS address-family IPv4/IPv6 unicast configuration mode.

The **match**, **metric**, and **metric-type** options are not available in OSPF VRF configuration mode.

Note
The **default-metric** command does not apply to the redistribution of directly connected routes. Use a route map to change the default metric for directly connected routes.

The no form of the command restores the defaults.

Examples

The following example redistributes IS-IS routes, specifying level 1 packets, in BGP address-family IPv4 unicast configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# redistribute isis level-1
```

The following example redistributes all IPv4 IS-IS routes from Level 2 into Level 1.

```
device# configure terminal
device(config)# router isis
```

```
device(config-bgp-isis)# address-family ipv4 unicast
evice(config-bgp-ipv4u)# redistribute isis level-2 into level-1
```

The following example redistributes OSPF external type 1 routes with a metric of 200 in BGP address-family IPv4 unicast configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# redistribute ospf match external1 metric 200
```

The following example redistributes OSPFv3 external type 2 routes in BGP address-family IPv6 unicast configuration mode.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# redistribute ospf match external2
```

The following example redistributes static routes into BGP4 and specifies a metric of 200.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# redistribute static metric 200
```

The following example redistributes directly connected routes into BGP4+.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# redistribute connected
```

The following example redistributes directly connected routes into IS-IS.

```
device# configure terminal
device(config)# router bgp
device(config-isis-router)# address-family ipv6 unicast
device(config-router-isis-ipv6u)# redistribute connected
```

The following example redistributes BGP routes and specifies that route-map "rm7" be consulted in OSPF VRF configuration mode.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# redistribute bgp route-map rm7
```

The following example redistributes OSPF routes and specifies a type1 external route in OSPFv3 VRF configuration mode.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# redistribute ospf metric-type type1
```

redundant-management enable

Enables or disables Redundant Management Interface feature on the device.

Syntax

redundant-management enable

[no] redundant-management enable

Command Default

Redundant Management Interface is disabled by default and need to be configured and enabled on the interface that is selected as being the redundant management interface. Only one front panel user port can be used as the redundant management interface.

Parameters

enabled

Enables this interface as the Redundant Management Interface.

Modes

Interface Ethernet

Usage Guidelines

Uses Linux *bonding* feature.

Any front panel interface on the device can be made the standby redundant management interface.

On breakout boards, if used with Mellanox Adaptor, Redundant Management Interface can only be enabled on the first port.

Examples

The following example configures the interface *eth 0/15* as the Redundant Management Interface.

```
device(config)# interface ethernet 0/15
device(conf-if-eth-0/15)# redundant-management enable
device(conf-if-eth-0/15)# no shut
device(conf-if-eth-0/15)# exit
```

refresh-reduction

When the user enables either of the refresh reduction extensions on an interface, outgoing RSVP packets sent on that interface sets the refresh reduction capability bit in the common RSVP header to indicate that the device is capable of receiving and processing refresh reduction messages and related objects.

Syntax

refresh-reduction bundle-message [**bundle-send-delay** *milliseconds*] | **summary-refresh**

no refresh-reduction bundle-message [**bundle-send-delay** *milliseconds*] | **summary-refresh**

Command Default

The RSVP bundle messages on the interface are disabled, by default.

Parameters

bundle-message

bundle-send-delay *milliseconds*

Specifies the bundle send delay value in milliseconds. the range is 20-1000 milliseconds, with a default of 40 milliseconds.

summary-refresh

Activates the refresh-reduction summary refresh.

Modes

MPLS RSVP mode (config-router-mpls-rsvp).

MPLS interface RSVP mode (config-router-mpls-eth-x/x-rsvp).

Usage Guidelines

Summary refresh is a more effective tool for RSVP refresh message overhead reduction.

Use the **no** version of the command to disable RSVP bundle messages.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following commands enable RSVP bundle messages on interface *0/13* with a bundle-send-delay of *20* milliseconds.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/13
device(config-router-mpls-eth-0/13)# rsvp
device(config-router-mpls-eth-0/13-rsvp)# refresh-reduction bundle-message bundle-send-
delay 20
```

region

Assigns a name to a Multiple Spanning Tree Protocol (MSTP) region.

Syntax

region *region-name*

no region

Parameters

region-name

Assigns a name to an MSTP region.

Modes

Spanning tree MSTP configuration mode

Usage Guidelines

The *region-name* string must be between 1 and 32 ASCII characters in length, and is case-sensitive.

Enter **no region** to delete the region name.

Examples

To assign a name to an MSTP region named extreme1:

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# region extreme1
```

registrar-server

Configures the various settings for accessing the remote *Keylime* Remote Attestation server.

Syntax

registrar-server *ip-address* **use-vrf** *vrf-name*

Parameters

ip-address

IP address of the remote *Keylime* Remote Attestation server. IPv4 or IPv6 addresses can be used.

use-vrf *vrf-name*

The VRF on which the remote Remote Attestation server can be accessed.

Modes

Remote Attestation mode.

Usage Guidelines

If your Remote Attestation server is listening on a non standard port, configure the port using the **registrar-port** command. The standard port for the *Keylime* server is 8890.

Examples

The following example configures the connection details of the *Keylime* Remote Attestation server. The IP address of the server is 10.1.1.10 and it can be accessed through the default VRF.

```
SLX (config-remote-attestation)# registrar-server 10.1.1.10 user-vrf default-vrf
SLX (config-remote-attestation)#
```

Platform Availability

This command and mode is only available on the Extreme 8720 and Extreme 8520 devices.

registrar-port

Configures the port on which the *Keylime* Remote Attestation server is listening for incoming connections.

Syntax

registrar-port *port*

Command Default

The default port value is 8890.

Parameters

port

Configures the port on which the *Keylime* Remote Attestation server is listening for incoming connections.

Modes

Registrar Server VRF Mode.

Examples

This example configures default port as the port on which the Remote Attestation server is listening for connections.

```
SLX (config)# remote-attestation
SLX (config-remote-attestation)# registrar-server 10.1.1.10 use-vrf default-vrf
SLX (config-remote-attestation-10.1.1.10/default-vrf)# registrar-port
SLX (config-remote-attestation-10.1.1.10/default-vrf)# exit
SLX (config-remote-attestation)# exit
SLX (config)#
```

Platform Availability

This command and mode is only available on the Extreme 8720 and Extreme 8520 devices.

reliable-messaging

When RSVP reliable messaging is enabled on an interface of the SLX-OSdevice, RSVP trigger messages sent out on that interface includes a message ID and a request for acknowledgment from the RSVP neighbor.

Syntax

reliable-messaging [**rapid-retrans-decay** *percent*] | [**rapid-retrans-interval** *milliseconds*] | [**rapid-retry-limit** *number*]

no reliable-messaging [**rapid-retrans-decay** *percent*] | [**rapid-retrans-interval** *milliseconds*] | [**rapid-retry-limit** *number*]

Command Default

The command is disabled, by default.

Parameters

rapid-retrans-decay *percent*

Specifies the percentage increase in the rapid transmission interval for each consecutive unacknowledged RSVP message. The range is from 0 - 100, with a default of 100.

rapid-retrans-interval *milliseconds*

Specifies the interval, in milliseconds, for an unacknowledged message to be resent. The range is from 100-30000 milliseconds, with a default of 2000 milliseconds.

rapid-retry-limit *number*

Specifies the maximum number of retries for an unacknowledged message. The range is 1-16, with a default value of 5.

Modes

MPLS interface RSVP mode (config-router-mpls-eth-x/x).

MPLS RSVP mode (config-router-mpls-rsvp).

Usage Guidelines

When acknowledgment is not received, the trigger message is re-transmitted using the retransmission parameters configured on the interface.

The **no** form of the command removes reliable messaging.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example enables RSVP reliable messaging on MPLS interface *0/13* .

```
device# configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/13
device(config-router-mpls-eth-0/13)# rsvp
device(config-router-mpls-eth-0/13-rsvp)# reliable-messaging
```

The following example configures the rapid-retrans-decay option to *1* percent, the rapid-retrans-interval option to *100* milliseconds, and the rapid-retry-limit option to *1* try.

```
device# configure
device(config)# router-mpls
device(config-router-mpls)# rsvp
device(config-router-mpls-rsvp)#  reliable-messaging rapid-retrans-decay 1 rapid-retrans-
interval 100 rapid-retry-limit 1
```

reload

Reboots the device.

Syntax

reload [**system**]

Parameters

system

Reboots the device.

Modes

Privileged EXEC mode

Usage Guidelines

All reboot operations are disruptive, and the commands prompt for confirmation before executing. When you reboot a device, all traffic to and from it stops. All ports on that device remain inactive until the device comes back online.

The **reload** command reboots the VM in the device.

Note
Do not use the **reload** command without the **system** parameter.

Examples

The following example performs a reboot of the device.

```
device# reload system
```

reload-delay

Sets the wait time before allowing traffic to be routed through interfaces.

Syntax

reload-delay *delay-time*

no reload-delay

Command Default

No global reload-delay setting is configured.

Parameters

delay-time

Specifies the length of time before allowing traffic to be routed through an interface. The range is 1 though 3600 seconds.

Modes

Privileged EXEC mode

Usage Guidelines

If a node is reloaded and the traffic flow is directed to an interface before it is operational, the traffic is dropped. Setting the reload-delay timer allows the interface to become fully operational before traffic is routed to it.

Use **reload-delay** to set the delay time for all interfaces where the feature is enabled, but no delay time is configured. Setting the global reload-delay time is optional, but useful when there are many interfaces to be configured with the same delay-time.

By default, interface level settings override global settings. If there is no setting at the interface level, the global setting is used. If no delay-time is set either on the interface or globally, the configuration is ignored.

If **reload-delay** is not enabled at the interface, a configuration error is raised.

Examples

The following example configures a global reload-delay time of 240 seconds.

```
device(config)# reload-delay 240
```

The following example removes the global configuration of a reload-delay timer.

```
device(config)# no reload-delay
```

reload-delay enable

Enables reload delay on a physical, port-channel, or loopback interface.

Syntax

reload-delay enable *delay-time*

no reload-delay enable

Command Default

No interface level reload-delay is enabled.

Parameters

delay-time

(Optional) Set the length of time before allowing traffic to be routed through an interface. The range is 1 through 3600 seconds.

Modes

Privileged EXEC mode

Usage Guidelines

If a node is reloaded and the traffic flow is directed to an interface before it is operational, the traffic is dropped. Setting the reload-delay timer allows the interface to become fully operational before traffic is routed to it.

Use the **reload-delay enable** command to enable reload-delay on an interface. This is a required configuration; if **reload-delay enable** is not set at the interface, a configuration error is raised. By default, interface level settings override global settings.

The reload-delay time on an interface is optional. If there is no delay-time set at the interface level, the global setting is used. If no delay-time is set either on the interface or globally, the configuration is ignored.

Examples

The following example configures a reload-delay time of 120 seconds on a port-channel.

```
device(config)# interface port-channel 10
    device(config-Port-channel)# reload-delay enable 120
```

The following example removes a reload-delay time from a port-channel.

```
device(config)# interface port-channel 10
    device(config-Port-channel)# no reload-delay enable
```

remark

Enables adding a meaningful, human readable description to an IP access list definition. This is applicable to both IPv4 and IPv6 Access Lists.

Syntax

remark *acl-remark-string*

Parameters

acl-remark-string

Enables adding a meaningful, human readable description to an IP access list definition. Maximum length 256 characters.

Modes

- IPv4 Access List Configuration mode.
- IPv6 Access List Configuration mode.

Examples

The following example enables the adding of a description to a IPv4 access list configuration.

```
SLX (config)# ip access-list standard test_acl_config
SLX (config-ipacl-std)# remark Configuration-for-DHCP
SLX (config-ipacl-std)#
```

The following example enables the adding of a description to a IPv6 access list configuration.

```
SLX (config)# ipv6 access-list standard test_acl_config
SLX (config-ip6acl-std)# remark IPv6-Configuration-for-DHCP
SLX (config-ip6acl-std)#
```

remote-mep

Associates an action profile to a RMEP for a scheduled Two-Way ETH-SLM or Two-Way ETH-DM.

Syntax

remote-mep *rmep-id* **action-profile** *profile-name*

no remote-mep

Parameters:

rmep-id

Specifies the RMEP ID.

action-profile

Specifies the action profile.

profile-name

Specifies the profile name.

Modes

config-cfm-md-ma-mep configuration mode

Usage Guidelines

Use the **no** form of the command delete the RMEP action profile associations.

Examples

This example shows how to associate an action profile to a RMEP for a scheduled Two-Way ETH-SLM.

```
device# configure terminal
device(config)# protocol cfm
device(config-cfm)# domain-name md1 level 4
device(config-cfm-md-md1)# ma-name ma1 id 1 vlan-id 30 priority 3
device(config-cfm-md-ma-ma1)# mep 1 down Ethernet 1/2
device(config-cfm-md-ma-mep-1)#  remote-mep 2
device(config-cfm-md-ma-mep-1)#  remote-mep 2 action-profile my_action_profile
```

rename

Renames a file in the device flash memory.

Syntax

rename *current_name new_name*

Parameters

current_name

Specifies the file name you want to change.

new_name

Specifies the new file name.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local device.

System configuration files cannot be renamed. If you try to rename a system file, a warning message is displayed.

Examples

The following example renames a file in the flash memory.

```
device# rename myconfig myconfig_20101010
```

reoptimize-timer

The user can set a timer to optimize a specific LSP path on a periodic basis.

Syntax

reoptimize-timer { *seconds* }

no reoptimize-timer { *seconds* }

Command Default

The re-optimize timer is disabled, by default. Not configurable for a non-adaptive bypass LSP.

Parameters

seconds

Specifies the length, in seconds, from the beginning of one re-optimization attempt to the beginning of the next attempt. The range is 300-65535 seconds.

Modes

MPLS LSP configuration mode (config-router-mpls-lsp-*lsp_name*).

MPLS router Bypass LSP configuration mode (config-router-mpls-bypass-lsp-*bypass_name*).

MPLS router dynamic bypass configuration mode (config-router-mpls-dynamic-bypass).

Usage Guidelines

Until a commit is issued the re-optimize timer is disabled.

Configuring a re-optimization timer does not interfere with running the manual **reoptimize** command.

Time-triggered re-optimizing does not apply to LSPs within a FRR network.

When upgrading software, the configured adaptive LSPs are initialized with the no re-optimization timer.

Use the **reoptimize-timer** command to configure a re-optimization timer for dynamic bypasses.

Dynamic bypass LSP re-optimization is enabled when the re-optimization value is set to a non-zero value, and the timer is set for the specified amount of seconds.

The **reoptimize-timer** value can also be configurable on MPLS interface mode. The global set value is applicable to all dynamic bypass LSPs for which the corresponding interface level re-optimization timer value is not set.

Use the **reoptimize-timer** command to configure a re-optimization timer value for all the dynamic bypass LSPs that are being created corresponding to a protected interface. When configured, this value overrides the global mode **reoptimize-timer** configured value.

When a dynamic bypass is non-adaptive, the **reoptimize-timer** is not considered for the dynamic bypass LSP.

The no form of the command removes the **reoptimize-timer** and sets it to the value set in the dynamic bypass global mode.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

In the following example, the re-optimize time is configured to 1000 seconds, which specifies the number of seconds from the beginning of one re-optimization attempt to the beginning of the next attempt.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp to20
device(config-router-mpls-lsp-to20)# reoptimize-timer 1000
device(config-router-mpls-lsp-to20)# commit
```

The following example configures the **reoptimize-timer** to 300 seconds under the MPLS router dynamic bypass configuration mode.

```
device>configure
device(config)# router-mpls
device(config-router-mpls)# dynamic-bypass
device(config-router-mpls-dynamic-bypass)# reoptimize-timer  360
```

The following example configures the reoptimize-timer to 360 seconds for dynamic bypass MPLS ethernet interface *2/8*.

```
device>configure
device(config)# router-mpls
device(config-router-mpls)# mpls-interface ethernet 0/8
device(config-router-mpls-if-ethernet-0/8)# dynamic-bypass
device(config-router-mpls-if-ethernet-0/8-dynamic-bypass)# reoptimize-timer 360
```

resequence access-list

Reassigns sequence numbers to entries of an existing MAC, IPv4, or IPv6 access list.

Syntax

resequence access-list { **ip** | **ipv6** | **mac** } *name seq_num increment*

Parameters

ip | **ipv6** | **mac**

Specifies the Layer 2 or Layer 3 ACL bound to an interface.

name

Specifies the name of a standard or an extended ACL. A maximum of 63 characters is allowed.

seq_num

Specifies the starting sequence number in the ACL. Valid values range from 1 through 65535.

increment

Specifies a value to increment the sequence number between rules. Valid values range from 1 through 65534.

Modes

Privileged EXEC mode

Usage Guidelines

Reordering the sequence numbers is useful when you need to insert rules into an existing ACL and there are not enough sequence numbers available. When all sequence numbers between rules are exhausted, this feature allows the reassigning of new sequence numbers to entries of an existing access list.

Examples

The following example reorders the rules in a MAC ACL.

```
device# show running-config mac access-list test
!
mac access-list standard test
 seq 1 permit 0011.2222.3333
 seq 2 permit 0011.2222.4444
 seq 3 permit 0011.2222.5555
 seq 4 deny 0011.2222.6666
!
device# resequence access-list mac test 10 10

device# show running-config mac access-list test
!
mac access-list standard test
```

```
 seq 10 permit 0011.2222.3333
 seq 20 permit 0011.2222.4444
 seq 30 permit 0011.2222.5555
 seq 40 deny 0011.2222.6666
!
```

The following example reorders the rules in an IPv6 ACL.

```
device# show running-config ipv6 access-list distList
!
ipv6 access-list standard distList
 seq 10 deny 2001:125:132:35::/64
 seq 20 deny 2001:54:131::/64
 seq 30 deny 2001:5409:2004::/64
 seq 40 permit any!
device# resequence access-list ipv6 distList 100 100

device# show running-config ipv6 access-list distList
!
ipv6 access-list standard distList
 seq 100 deny 2001:125:132:35::/64
 seq 200 deny 2001:54:131::/64
 seq 300 deny 2001:5409:2004::/64
 seq 400 permit any
!
```

reservable-bandwidth

The **reservable-bandwidth** command is configurable on an MPLS-enabled interface at any time. The configuration of the command takes effect immediately upon preemption of the LSP.

Syntax

reservable-bandwidth { *decimal* | [**percentage** *decimal*] }

no reservable-bandwidth { *decimal* | [**percentage** *decimal*] }

Command Default

The default value is the total physical bandwidth of the interface.

Parameters

decimal

The decimal variable specifies a value from 0 through 2,000,000,000 in kbps.

percentage *decimal*

The percentage decimal parameters specify a value from 0 through 100. The percentage value of 100 specifies that the entire interface bandwidth can be used by MPLS LSPs, when needed.

Modes

MPLS interface mode (config-router-mpls-if-eth).

Usage Guidelines

The no form of the command sets the maximum reservable bandwidth back to the default value.

When the maximum reservable bandwidth is configured as a percentage value for LAGs and VE interfaces, and ports go down, or new ports are added to the interface, the reservable bandwidth is recalculated as a percentage of the newly available bandwidth for that interface.

When the maximum reservable bandwidth is configured as either an absolute value, or a percentage value, the value is recalculated and updated to the latest value.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The example below shows the configuration of the maximum reservable bandwidth for MPLS LSPs with an absolute value of 10000 kbps.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/1
device(config-router-mpls-if-eth-0/1)# reservable-bandwidth 10000
```

The following example configures the maximum reservable bandwidth as a percentage (80%) of the total interface bandwidth for the MPLS LSPs on the interface.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/1
device(config-router-mpls-if-eth-0/1)# reservable-bandwidth percentage 80
```

The following example shows when the maximum reservable bandwidth is changed from an absolute value to a percentage value, and vice versa, the following advisory message displays on the console to indicate the configuration change.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/1
device(config-router-mpls-if-eth-0/1)# reservable-bandwidth percentage 40
Maximum reservable bandwidth is changed from 30 kbps to 40%
```

The following example shows using the **no** form of the command to set the maximum reservable bandwidth back to the default value (the total physical bandwidth of the interface) when using the absolute value or percentage value.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/1
device(config-router-mpls-if-eth-0/1)# no reservable-bandwidth percentage 80
```

resilient-hash

Resilient Hashing is a feature that ensures that there is minimal disruption in traffic flow when there is a disruption due to a link failure or a link addition. Resilient Hashing is supported for L3 traffic routed using BGP (support for both IPv4 and IPv6 traffic) and Static Routes. The **resilient-hash** is used to enable and disable this feature as well as configuring the maximum path value.

Syntax

resilient-hash ecmp enable

resilient-hash max-path [*8* | *16* | *64* | *128*]

no resilient-hash ecmp enable

no resilient-hash max-path

Command Default

The default value for `max-path` is eight (8).

Parameters

ecmp *enable*

Enables or disables Resilient Hashing.

max-path [*8* | *16* | *64* | *128*]

Sets the maximum path value for ECMP group for this VRF.

Modes

Global configuration and VRF configuration modes

Usage Guidelines

Warning

Enabling or disabling Resilient Hashing or making changes to the *max-path* configuration value will cause traffic disruption for the corresponding VRF. This is by design. This is because, by design, routes and next-hops are re-downloaded to both the software and hardware routing tables for programming *Special Attributes*.

BFD sessions in unrelated VRFs are not affected. Additionally, when the device boots up, Resilient Hashing configuration replay will not cause BFD session flap.

Note

SLX 9540 and SLX 9640 support 64 maximum paths.

Examples

The following example enables Resilient Hashing at a global level and sets the *max-path* value to 128. The **show running-config resilient-hash** command is used to verify the configuration.

```
SLX # conf term
SLX (config)#
SLX (config)# resilient-hash ecmp enable
SLX (config)# resilient-hash max-path 128
SLX (config)#
SLX (config)# do show running-config resilient-hash
resilient-hash ecmp enable
resilient-hash max-path 128

SLX (config)#
```

The following example enables Resilient Hashing at a VRF level and sets the *max-path* value to 64. The **show running-config vrf <vrf-name>** command is used to verify the configuration.

```
SLX # conf term
SLX (config)#
SLX (config)# vrf vrf2
SLX (config-vrf-vrf2)#
SLX (config-vrf-vrf2)# resilient-hash ecmp enable
SLX (config-vrf-vrf2)# resilient-hash max-path 64
SLX (config-vrf-vrf2)# do show running-config  vrf vrf2
vrf vrf2
 resilient-hash ecmp enable
 resilient-hash max-path 64
 address-family ipv4 unicast
 !
 address-family ipv6 unicast
 !
!
SLX (config-vrf-vrf2)#
```

retain route-target all

Configures a route reflector (RR) to accept all route targets (RTs).

Syntax

retain route-target all

no retain route-target all

Command Default

This feature is disabled.

Modes

BGP address-family L2VPN EVPN configuration mode

Usage Guidelines

The **no** form of the command disables the retaining of all RTs.

Examples

The following example configures a RR to accept all RTs.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# retain route-target all
```

retransmit-interval

Sets the time the device waits before it retransmits Link State PDUs (LSPs).

Syntax

retransmit-interval *interval*

no retransmit-interval *interval*

Command Default

The default retransmission interval is 5 seconds.

Parameters

secs

Specifies the retransmission interval in seconds. Valid values range from 1 through 65535 seconds. The default is 5 seconds.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command removes the configured interval.

Examples

The following example changes the retransmission interval to 7 seconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# retransmit-interval 7
```

retries

Configures the number of retries allowed to establish a connection with the Remote Authentication Dial-In User Service (RADIUS) server.

Syntax

retries *num*

no retries

Command Default

The number of retries allowed is 5.

Parameters

num

Specifies the number of retries allowed to connect to a RADIUS server. The range is from 0 through 100. The default value is 5.

Modes

RADIUS server host VRF configuration mode

Usage Guidelines

The **no** form of the command restores the command default value.

Examples

The following example shows how to set the number of retries allowed (to establish a connection with the RADIUS server) to 10.

```
device# configure terminal
device(config)# radius-server host 10.37.73.180 use-vrf green-vrf
device(config-host-10.37.73.180/green-vrf)# retries 10
```

retry-limit

Configures a limit on the number of times the ingress LER tries to connect to the egress LER in a signaled LSP.

Syntax

retry-limit *number*

no retry-limit

Command Default

The command is disabled, by default.

Parameters

number

Specifies a limit on the number of LSP connection attempts.

Modes

MPLS policy mode.

Usage Guidelines

The **no** form of the command disables the configuration.

When the connection is established, the retry counter is reset to zero.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

In the following example, when the LSP needs to be established again, the ingress LER makes 20 attempts to establish a connection to the egress LER.

```
device # configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# retry-limit 20
```

retry-time

Configures the amount of time the ingress LER waits between connection attempts.

Syntax

retry-time *seconds*

no retry-time

Command Default

The command is disabled, by default.

Parameters

seconds

Specifies the LSP retry time in seconds. The default is 30 seconds.

Modes

MPLS policy mode

Usage Guidelines

When a signaled LSP is enabled, the ingress LER attempts to connect to the egress LER over the primary path specified in the LSPs configuration. When the connection is not successful, by default the ingress LER waits 30 seconds before attempting the connection again.

The **no** form of the command disables the configuration.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures the retry time to 45 seconds.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# retry-time 45
```

reverse-metric

Configures the reverse metric value at the Intermediate System-to-Intermediate System (IS-IS) router level.

Syntax

reverse-metric [*value*] [**te-def-metric**] [**whole-lan**]

reverse-metric tlv-type [*value*]

no reverse-metric [*value*] [**te-def-metric**] [**whole-lan**]

no reverse-metric tlv-type [*value*]

Command Default

The **reverse-metric** command is disabled by default.

Parameters

reverse-metric

Specifies the reverse metric parameter at the IS-IS router level.

value

Specifies the reverse metric value in metric style. The metric style consists of narrow or wide style. The narrow metric range is from 1 through 63. The wide metric range is from 1 through 16777215. The default value is 16777214 irrespective of the metric style configured.

te-def-metric

Specifies that the device sends a traffic engineering (TE) default metric sub-type-length-value (TLV) within the reverse-metric TLV.

whole-lan

Specifies that the configured reverse metric value affects the entire LAN.

tlv-type *value*

Specifies the TLV type for the reverse metric value. The default value is 254.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

If the reverse-metric value is configured, the local LSP is updated with the sum of the default metric and the reverse metric value. When the IS-IS neighbor device receives the reverse metric value through the IS hello, the neighbor router updates the cost to

reach the original IS-IS router with the sum of default metric and the reverse metric value.

The **whole-lan** option only takes effect on the multi-access LAN. IS-IS point-to-point interfaces are not affected when the **whole-lan** option is used.

The **no** form of the command specified with the configured value resets the metric value to the default value of 16777214. The **no reverse-metric** command removes the entire reverse metric configuration.

Examples

The following example changes the reverse metric value for the entire LAN to 50.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# reverse-metric 50 whole-lan
```

The following example configures the reverse metric TLV type in the range of unassigned IS-IS TLV values.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# reverse-metric tlv-type 230
```

revert-timer

The path selection revert timer provides an option to stabilize a path before traffic is switched to it. Without a configured path selection revert timer, the router switches between a primary and secondary path immediately after the current working path goes down.

Syntax

revert-timer *timer_value*

no revert-timer

Command Default

There is no revert-timer in the default command mode.

Parameters

timer_value

The number of seconds that the router waits after the primary or selected path comes up before traffic reverts to that path. The range is 1- 65,535 seconds.

Modes

MPLS LSP configuration mode (config-router-mpls-lsp-*lsp_name*).

Usage Guidelines

The **revert-timer** command has no effect on the unconditional select mode. Traffic is unconditionally switched to the user selected path and stays on it.

The path stability test used with the revert timer is based on the uptime of the latest instance of the path. This value can be different when the selected path has gone through a "make-before-break" procedure.

For an LSP going through re-optimization, the new LSP does not carry traffic until the revert timer expires.

When a user changes the revert timer, the basis of counting is the uptime of the path and is independent of the sequence or combination of configurations.

The **no** form of the command removes the revert-timer.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures the revert-timer to 10 seconds.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp samplelsp
device(config-router-mpls-lsp-samplelsp)# revert-timer 10
```

revertive global

The revertive mode global command can be executed only on LSPs with FRR and adaptive enabled.

Syntax

revertive global [**disable** | **enable**]

no revertive mode global

Command Default

Global revertiveness is enabled by default for LSPs with FRR and adaptive enabled.

Parameters

disable

Disables global revertiveness.

enable

Enables global revertiveness.

Modes

MPLS LSP Fast Reroute.

Usage Guidelines

The **no** option disables global revertiveness on an LSP.

When adaptive is disabled, then global revertiveness is also disabled.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example enables global revertiveness on LSP *t1*.

```
device# config
device(config)# router mpls
device(config-router-mpls)# lsp t1
device(config-router-mpls-lsp-t1)# adaptive
device(config-router-mpls-lsp-t1)# frr
device(config-router-mpls-lsp-t1-frr)# revertive global enable
```

The following example is of an adaptive LSP.

```
device# configure terminal
device(config)# router mpls
device(config-mpls)# lsp t1
device(config-router-mpls-lsp-t1)# to 10.3.3.3
```

```
device(config-router-mpls-lsp-t1)# from 10.2.2.2
device(config-router-mpls-lsp-t1)# traffic-eng mean-rate 1000
device(config-router-mpls-lsp-t1)# adaptive
device(config-router-mpls-lsp-t1)# frr
device(config-router-mpls-lsp-t1-frr)# facility-backup
device(config-router-mpls-lsp-t1-frr)# exit
device(config-router-mpls-lsp-t1)# enable
device(config-router-mpls)#
```

The following example changes the FRR bandwidth for an adaptive LSP.

```
device(config)#
device(config)# router mpls
device(config-router-mpls)# lsp t1
device(config-router-mpls-lsp-t1)# frr
device(config-router-mpls-lsp-t1-frr)# bandwidth 1000
device(config-router-mpls-lsp-t1-frr)# exit
device(config-router-mpls-lsp-t1)# commit
```

The following example show how global revertiveness is enabled by default in FRR mode for an adaptive LSP.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# retry-limit 20
device(config-router-mpls-policy)# exit
device(config-router-mpls)# lsp t1
device(config-router-mpls-lsp-t1)# adaptive
device(config-router-mpls-lsp-t1)# frr
device(config-router-mpls-lsp-t1-frr)# revertive mode global
device(config-router-mpls-lsp-t1-frr)# revertive holdtime 20
device(config-router-mpls-lsp-t1-frr)# exit
device(config-router-mpls-lsp-t1)# commit
device(config-router-mpls-lsp-t1)#
```

revertive hold-time

Specifies the time, in seconds, the LSP holds before attempting a new path on the FRR LSP.

Syntax

revertive holdtime *value*

no revertive holdtime

Command Default

The default is five seconds.

Parameters

value

Specifies the hold time value in seconds. The hold-time ist he time between the primary LSP failure and the trigger of new instanceof LSP by global revertiveness. The range is one through 60 seconds.

Modes

MPLS LSP fast reroute mode (config-router-mpls-lsp-*lsp_name*-frr).

Usage Guidelines

The **no** form of the command removes the revertive hold time.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures the revertive hold time to 20 seconds.

```
device# configure
device(Config)# router mpls
device(config-router-mpls)# lsp t1
device(config-router-mpls-lsp-t1)# adaptive
device(config-router-mpls-lsp-t1)# frr
device(config-router-mpls-lsp-t1-frr)# revertive mode global
device(config-router-mpls-lsp-t1-frr)# revertive holdtime 20
```

revision

Assigns a version number to the Multiple Spanning Tree Protocol (MSTP) configuration.

Syntax

revision *number*

no revision

Command Default

The default is 0.

Parameters

number

Specifies the revision or version number of the MSTP region. Valid values range from 0 through 255.

Modes

Spanning tree MSTP configuration mode

Usage Guidelines

The **no** form of the command resets the default value of 0.

Examples

This example assigns a configuration revision of 1.

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# revision 1
```

rfc1583-compatibility (OSPF)

Configures compatibility with RFC 1583.

Syntax

rfc1583-compatibility

no rfc1583-compatibility

Command Default

OSPF is compatible with RFC 1583 (OSPFv2).

Modes

OSPF router configuration mode

OSPF router VRF configuration mode

Usage Guidelines

OSPF is compatible with RFC 1583 (OSPFv2) and maintains a single best route to an autonomous system (AS) boundary router in the OSPF routing table. Disabling this compatibility causes the OSPF routing table to maintain multiple intra-AS paths, which helps prevent routing loops.

Enter **no rfc1583-compatibility** to disable compatibility with RFC 1583.

Examples

The following example disables compatibility with RFC 1583.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# no rfc1583-compatibility
```

rib-route-limit

Limits the maximum number of BGP Routing Information Base (RIB) routes that can be installed in the Routing Table Manager (RTM).

Syntax

rib-route-limit *num*

no rib-route-limit

Command Default

No maximum number of RIB routes is set.

Parameters

num

Decimal value for the maximum number of RIB routes to be installed in the RTM. Valid values range from 1 through 4294967295.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

This command controls the number of routes installed by BGP, irrespective of whether those BGP routes are the preferred routes in the system. BGP locally tracks the number of routes installed and the number of routes withdrawn from RIB. If the total number of routes installed exceeds the value specified by *num*, routes will not be installed.

If *num* is increased, route calculation is automatically triggered.

If *num* is decreased, the user is prompted to clear the BGP RTM.

Examples

The following example configures the device to limit the maximum number of BGP4 RIB routes that can be installed in the RTM.

```
device# configure terminal
device(config)# router bgp
```

```
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# rib-route-limit 10000
```

The following example configures the device to limit the maximum number of BGP4+ RIB routes that can be installed in the RTM.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast
device(config-bgp-ipv6u)# rib-route-limit 32000
```

right-interface vlan

Configures an Ethernet Ring Protection (ERP) right interface.

Syntax

right-interface vlan *vlan_id* { **ethernet** *slot/port* | **port-channel** *number* }

no right-interface vlan *vlan_id* { **ethernet** *slot/port* | **port-channel** *number* }

Command Default

No ERP right interface is configured by default.

Parameters

vlan_id

Specifies the VLAN ID of the ERP right ring interface. Range is from 1 through 4090.

ethernet *slot/port*

Specifies an Ethernet interface.

port-channel *number*

Specifies a port-channel.

Modes

ERP configuration mode

Usage Guidelines

Each Ethernet Ring Node (ERN) in a major ring must have explicitly defined left and right interfaces so that ERP can function properly. ERNs in a sub-ring must have at least one interface defined so that ERP can function properly.

For proper operation you must configure the interfaces following the same manner on each ERN, such as left/ right, left/ right, and so on.

You must configure the VLAN and configure the Ethernet or port-channel interfaces as switchport, and then add the VLAN to the interfaces either in trunk or access mode. This is a prerequisite to configuring the ERP left interface and right interface.

Use the **no** form of this command to delete the configuration.

Examples

The following example configures a right interface on an Ethernet interface.

```
device# configure terminal
device(config)# erp 1
device(config-erp-1)# right-interface vlan 5 ethernet 0/1
```

rpl

Configures an Ethernet Ring Protection (ERP) Ring Protection Link (RPL).

Syntax

rpl {**vlan***vlan_id* [**ethernet** *slot/port* |**port-channel** *number*] }

no rpl {**vlan***vlan_id* [**ethernet** *slot/port* |**port-channel** *number*] }

Command Default

No RPL is configured by default.

Parameters

vlan_id

Specifies the VLAN ID of the ERP left or right ring interface and interface number. Range is from 1 through 4090.

ethernet *slot/port*

Specifies an Ethernet interface.

port-channel *number*

Specifies a port-channel.

Modes

ERP configuration mode

Usage Guidelines

Each ring needs to have one RPL owner for each ring. The RPL owner's role is to block traffic on one port when no failure exists in the ring. The blocked port will be the left interface that you initially configured. After configuring the ERN to be the RPL owner, by means of the **rpl-owner** command, you next must set the RPL, by means of the **rpl** command.

You must configure the VLAN and configure the Ethernet or port-channel interfaces as switchport, then add the VLAN to the interfaces in either trunk or access mode. This is a prerequisite to configuring the **rpl** command.

Use the **no** form of this command to delete the configuration.

Examples

The following example configures an RPL.

```
device# configure terminal
device(config)# erp 1
device(config-erp-1)# rpl vlan 5 ethernet 0/1
```

rpl-owner

Set an Ethernet Ring Protection (ERP) bridge as a Ring Protection Link (RPL) owner.

Syntax

rpl-owner

no rpl-owner

Command Default

The RPL owner is not set by default.

Modes

ERP configuration mode

Usage Guidelines

Each ring needs to have one RPL owner. The RPL owner role is to block traffic on one port when no failure exists in the ring. After configuring the ERN to be the RPL owner, by means of the **rpl-owner** command, you next must set the RPL, by means of the **rpl** command.

This command is required to set one of the nodes in an ERP ring as the RPL owner.

Use the **no** form of this command to unset the RPL owner.

Examples

The following example sets the ERP bridge as an RPL owner.

```
device# configure terminal
device(config)# erp 1
device(config-erp-1)# rpl-owner
```

rpki priority

This command sets the priority of a server configured in the Resource Public Key Infrastructure's (RPKI) RPKI to Router Protocol (RTR) library. This command sets the priority of the RPKI Server contained in it. A RPKI server in a priority with a lower value will be chosen over a server in priority with a higher value.

Syntax

rpki priority *<1-100>*

[no] rpki priority *<1-100>*

Parameters

<1-100>

The cache server priority number.

Modes

router bgp

Usage Guidelines

At least one RPKI priority value must exist in the RTR library. A maximum of 100 RTR priority values can be created. RTR priority values are numbered 1 to 100. Values over this range will report an error. Each RTR priority can store one RPKI server information.

A value greater than 100 will report an error.

Use the **no** format of the command to delete a RTR priority value.

Examples

This example shows the steps to create a new **rpki priority** entry in the RTR library.

```
SLX(config)#router bgp

SLX(config-bgp-router)# rpki priority ?
Priority:<1-100>

SLX(config-bgp-router)# rpki priority 1
SLX(config-bgp-router)#
```

server ssh

This command establishes a SSH connection to the configured cache server. Establishing this connection enables the validation of prefixes with the RPKI server. Only one (1) cache server can be configured under one priority. Attempting to configure another RPKI server will report an error. The RPKI server connection is attempted through the Management VRF. Use the **no** format of this command to remove the configured RPKI server from the priority.

Syntax

server ssh { *name* | *ipv4/ipv6 address* } **port** *port no* **username** *username* **password-file** *client private key path*

[no] server ssh { *name* | *ipv4/ipv6 address* } **port** *port no* **username** *username* **password-file** *client private key path*

Syntax

Parameters

name

The hostname of the remote RPKI cache server. You can use one of *hostname* or IP *address*.

ipv4/ipv6 address

The IPv4 or IPv6 IP address of the remote RPKI server. You can use one of *hostname* or IP *address*.

port *port no*

The configured SSH port number on the remote RPKI server. The default SSH port is 22. Port numbers are in the range of 1-65535.

username

The Username of the account used to connect to the remote RPKI server. This value cannot be longer than 63 characters.

password-file

The key file for this user credentials. This key file is provided by the operator of the remote RPKI server. Contact the administrator/operator of the server to get this key. An error is reported when this file is not found at the supplied path when this server entry is created.

Modes

RPKI Priority

Use the [no] format of this command to remove a configured RPKI server from the current RPKI priority.

Usage Guidelines

Only one RPKI Server can be configured in a priority. Attempts to configure more than one server in a priority will report an error.

Warning

Every time this command is run, there is a possibility that your CLI console response may become slow. This is due to the SLX-OS performing CPU intensive tasks of caching ROAs from the remote RPKI server and then revalidating RPKI state for all existing prefixes. This has been observed in systems with fully scaled routes in RIB-in when adding a server in the highest RPKI priority group. Adding servers in the lower priority groups does not cause this issue.

This slowdown is also possible when the connection to the existing RPKI server fails and the system fails over to the server with the next priority.

Examples

This example shows the steps to add a SSH connection to the configured cache server in the **rpki priority** within the **router bgp** configuration mode. This example also shows adding a SSH server to another RPKI priority.

```
SLX(config)# router bgp
SLX(config-bgp-router)# rpki priority 1
SLX(config-bgp-rpki-grp)# server ssh rpki.realmv6.org port 22 username rtr-ssh password-
file "/root/.ssh/id_rsa_realmv6-org"
SLX(config-bgp-rpki-grp)# exit
SLX(config-bgp-router)# rpki priority 2
SLX(config-bgp-rpki-grp)# server ssh 10.10.11.152 port 2200 username rtr-admin-g1
password-file "/root/.ssh/id_rsa_10-10-11-152"
SLX(config-bgp-rpki-grp)#
```

server tcp

This command establishes a TCP connection to the configured cache server. TCP connections are not secured by nature. Establishing this connection enables the validation of prefixes with the RPKI server. Only one (1) cache server can be configured under one priority. Attempting to configure another RPKI server will report an error. The RPKI server connection is attempted through the Management VRF. Use the **no** format of this command to remove the configured RPKI server from the priority.

Syntax

server tcp { *name* | *ipv4/ipv6 address* } **port** *port no*

[no] server tcp { *name* | *ipv4/ipv6 address* } **port** *port no*

Parameters

name

The hostname of the remote RPKI server. You can use one of *hostname* or IP *address*.

ipv4/ipv6 address

The IPv4 or IPv6 IP address of the remote RPKI server. You can use one of *hostname* or IP *address*.

port *port no*

The configured SSH port number on the remote RPKI server. Port numbers are in the range of 1-65535.

Modes

RPKI Priority

Usage Guidelines

Only one RPKI Server can be configured in a priority. Attempts to configure more than one server in a priority will report an error.

Use the [no] format of this command to remove a configured RPKI server from the current RPKI priority priority.

Warning

Every time this command is run, there is a possibility that your CLI console response may become slow. This is due to the SLX-OS performing CPU intensive tasks of caching ROAs from the remote RPKI server and then revalidating RPKI state for all existing prefixes. This has been observed in systems with fully scaled routes in RIB-in when adding a server in the highest RPKI priority group. Adding servers in the lower priority groups does not cause this issue.

This slowdown is also possible when the connection to the existing RPKI server fails and the system fails over to the server with the next priority.

Examples

This example shows the steps to add a TCP connection to the configured cache server in the **rpki priority** within the **router bgp** configuration mode. This example also shows adding a server to another RPKI priority.

```
SLX(config)# router bgp
SLX(config-bgp-router)# rpki priority 1
SLX(config-bgp-rpki-grp)# server tcp rpki.realmv6.org port 113
SLX(config-bgp-rpki-grp)# exit
SLX(config-bgp-router)# rpki priority 2
SLX(config-bgp-rpki-grp)# server tcp 10.10.11.152 port 113
SLX(config-bgp-rpki-grp)#
```

rmon alarm

Sets the RMON alarm conditions.

Syntax

rmon alarm *index snmp_oid* **interval** *seconds* [**absolute** | **delta**] **rising-threshold** *value* **event** *number* [**falling-threshold** *value* **event** *number* [**owner** *name*]

no rmon alarm

Command Default

No alarms are configured.

Parameters

index

Specifies the RMON alarm index. Valid values range from 1 through 65535.

snmp_oid

Specifies the MIB object to monitor. The variable must be in the SNMP OID format, for example, 1.3.6.1.2.1.16.1.1.1.5.65535. The object type must be a counter32.

interval *seconds*

Specifies the RMON alarm sample interval in seconds. Valid values range from 1 through 2147483648.

absolute

Sets the sample type as absolute.

delta

Sets the sample type as delta.

rising-threshold *value*

Specifies the RMON alarm rising threshold. Valid values range from 0 through 4294967295.

event *number*

Specifies the event for the rising alarm. Valid values range from 1 through 65535.

falling-threshold *value*

Specifies the RMON alarm falling threshold. Valid values range from 0 through 4294967295.

event *number*

Specifies the event for the rising alarm. Valid values range from 1 through 65535.

owner *name*

Specifies the identity of the owner. The maximum number of characters is 32.

Modes

Global configuration mode

Usage Guidelines

Enter **no rmon alarm** to disable the alarm conditions.

Examples

To set RMON alarm conditions:

```
device# configure terminal
device(config)# rmon alarm 100 1.3.6.1.2.1.16.1.1.1.5.65535 interval 5 absolute rising-
threshold 10000 event 100 falling-threshold 1000 event 101 owner admin
```

rmon collection history

Collects Ethernet group statistics for later retrieval.

Syntax

rmon collection history *number* [**buckets** *bucket_number* | **interval** *seconds* | **owner** *name*]

no romn collection history *number*

Command Default

RMON history collection is not enabled.

Parameters

number

Specifies the RMON collection control index value. Valid values range from 1 through 65535.

buckets *bucket_number*

Specifies the maximum number of buckets for the RMON collection history. Valid values range from 1 through 65535.

interval *seconds*

Specifies the alarm sample interval in seconds. Valid values range from 1 through 3600. The default value is 1800.

owner *name*

Specifies the identity of the owner. The maximum number of characters is 15.

Modes

Interface subtype configuration mode

Usage Guidelines

This command collects periodic statistical samples of Ethernet group statistics on a specific interface for later retrieval.

Enter **no rmon collection history** *number* to disable the history of statistics collection.

Examples

To collect RMON statistics, with an RMON collection control index value of 5 for the owner named admin, on a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 1/6
device(conf-if-eth-1/6)# rmon collection history 5 owner admin
```

rmon collection stats

Collects Ethernet group statistics n a specific interface.

Syntax

rmon collection stats *number* [**owner** *name*]

no rmon collection stats *number*

Command Default

RMON statistic collection is not enabled.

Parameters

number

Specifies the RMON collection control index value. Valid values range from 1 through 65535.

owner *name*

Specifies the identity of the owner.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no rmon collection stats** *number* to disable the collection of statistics.

Ethernet group statistics collection is not supported on ISL links.

Examples

The following example shows how to collect RMON statistics, with an RMON collection control index value of 2 for the owner named admin, on a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 1/6
device(conf-if-eth-1/6)# rmon collection stats 2 owner admin
```

rmon event

Adds or removes an event in the RMON event table associated to the RMON alarm number.

Syntax

rmon event *index* [**description** *word* | **log** | **owner** *name* | **trap** *word*]

no rmon event

Command Default

No events are configured.

Parameters

index

Specifies the RMON event number. Valid values range from 1 through 65535.

description *word*

Specifies a description of the event.

log

Generates an RMON log when an event is triggered.

owner *name*

Specifies the owner of the event. The *name* string must be between 1 and 32 characters in length.

trap *word*

Specifies the SNMP community or string name to identify this trap.

Modes

Global configuration mode

Usage Guidelines

Enter **no rmon event** to remove the event configuration.

Examples

To configure an RMON event:

```
device# configure terminal
device(config)# rmon event 2 log description "My Errorstoday" owner gjack
```

role name

Creates or modifies a non-default role.

Syntax

role name *role_name* [**desc** *description*]

no role name *role_name* [**desc** *description*]

Parameters

role_name

Specifies the name of the role.

desc *description*

Specifies an optional role description.

Modes

Global configuration mode

Usage Guidelines

For each role that you create, you define one or more rules. Each user is associated with one—and only one—role.

Role names are from 4 through 32 characters, must begin with a letter, and can contain alphanumeric characters and underscores. The name cannot be same as that of an existing user.

The description field supports up to 64 characters and can include any printable ASCII character, except for the following characters: single quotation mark (‘), double quotation mark ("), exclamation point (!), colon (:), and semi-colon (;). If the description contains spaces, enclose the text in double quotation marks.

The maximum number of roles supported is 64, including the user and admin default roles.

To delete a role description, enter **no role name** *role_name* **desc**.

To delete a role, enter **no role name** *role_name*.

Examples

The following example creates a role.

```
device# configure terminal
device(config)# role name tempAdmin desc "Daily admin functions"
```

The following example deletes the role.

```
device# configure terminal
device(config)# no role name tempAdmin
```

rollback apply checkpoint

Reverts the system's running configuration to the configuration in a specified or most recent checkpoint file.

Syntax

```
rollback apply checkpoint [ cp-name [ best-effort | stop-at-first-
   failure ] [ verbose ] ]
```

Command Default

The **best-effort** mode is applied if it is not specified.

Parameters

cp-name

Specifies the name of a checkpoint.

best-effort

Implements a rollback and skips any errors.

stop-at-first-failure

Implements a rollback and stops at the first failure.

verbose

Displays the execution log.

Modes

Privileged EXEC mode

Usage Guidelines

A configuration checkpoint must exist before this command is issued.

Rollback is not permitted when any of the following is in progress:

- Configuration replay
- File replay
- Another rollback operation
- Checkpoint creation

Configuration parameters that have changed are first removed and the previous values are then reapplied. If *cp-name* is not specified, the configuration rolls back to the most recent created checkpoint. This is not the same as an undo/redo scenario. Once the rollback process is complete, the system runs with the exact configurations in the checkpoint file.

Once the rollback is successfully completed, the execution of the **show rollback diff checkpoint** command, comparing the checkpoint and the running configuration file, should not report any differences.

The user can view any errors/warnings encountered during the rollback operation. The user is responsible for cleaning up the already applied changes before the error has occurred, by viewing the configuration differences between checkpoint and the running configuration.

Use of the Control+C key combination is not recommended during the rollback operation. Although Control+C is not blocked, it could leave the device with an indeterminate configuration. When the user issues the rollback command, a warning is issued that tells the user not to abort an ongoing rollback session.

The following table lists additional error conditions and messages.

Table 19: Error conditions and messages

Condition	Message
All the north bound configurations are blocked when rollback operation is in progress.	`%ERROR: Rollback configuration is in progress.` `Please try after sometime.`
Configuration replay is in progress.	`%ERROR: The node is not ready to handle all` `commands`
File replay is in progress.	`%ERROR: Configuration rollback not allowed when` `file replay is in progress, try again later`
Another rollback operation is in progress.	`%ERROR: There is another configuration rollback` `session in progress, try again later`

Examples

This example reverts the configuration to a checkpoint named "user_checkpoint1".

```
device# rollback apply checkpoint user_checkpoint1
This operation will modify the running configuration of the system. Do you want to
continue? [Y/N]y
% Warning: Configuration Rollback is in-progress.
Please do not abort an ongoing session as it can leave the system with an inconsistent
configuration.
......
Rollback completed successfully.
```

rollback checkpoint

Creates or removes a rollback configuration checkpoint, with an optional name and description.

Syntax

rollback checkpoint [*cp-name* [**description** *string*]]

no rollback checkpoint { **all** | *cp-name* }

Command Default

A checkpoint is not created by default.

Parameters

cp-name

Specifies the name of a checkpoint.

description *string*

Specifies a description for the checkpoint. See the Usage Guidelines.

all

Specifies all checkpoints.

Modes

Privileged EXEC mode

Usage Guidelines

The user must have admin privileges to execute this command.

The checkpoint name must exist in device flash memory.

Only one user can perform a checkpoint operation at a time.

The checkpoint name and description string can be any alphanumeric string. The description string must be inside quotation marks. Checkpoint names must be 64 characters or less. Checkpoint descriptions must be 128 characters or less.

When the checkpoint name is not specified, the checkpoint is created with a timestamp in YYYMMDD_HHMISS format. For example, 20180511_23435.

The **no** form of this command removes all checkpoints or a specified checkpoint. The **no rollback checkpoint all** command deletes all checkpoints in the device flash memory.

Examples

This example creates the rollback checkpoint "test" with description "testing checkpoint".

```
device# rollback checkpoint test description "testing checkpoint"
Checkpoint "test" creation completed successfully.
```

This example deletes the rollback checkpoint "test".

```
device# no rollback checkpoint test
Warning: Checkpoint "test" will be deleted!!
Do you want to continue? [y/n]:
```

This example deletes all rollback checkpoints.

```
device# no rollback checkpoint all
Warning: Checkpoint "test" will be deleted!!
Do you want to continue? [y/n]:
```

rollback enable

Enables configuration rollback.

Syntax

rollback enable

no rollback enable

Command Default

Rollback is disabled.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **no** form of this command to clean up all the checkpoints present in the system.

If rollback is not enabled, all rollback-related commands result in errors.

Examples

This example enables rollback.

```
device# configure terminal
device(config)# rollback enable
```

This example disables rollback.

```
device(config)# no rollback enable
%%WARN: All checkpoints and rollback logs will be cleared!
Do you want to continue? [y/n]:
```

root access console

Restricts the root access to the device to the console only.

Syntax

root access console

no root access console

Modes

Global configuration mode

Usage Guidelines

The **no root access console** allows root access to the device through all terminals (SSH, Telnet, and console).

Examples

Typical command output:

```
device# configure terminal
device(config)# do show running-config | include root
% No entries found.
device(config)# root access console
device(config)# do show running-config | include root
root access console
device(config)#
```

root enable

Enables root access to the device following a firmware configuration.

Syntax

root enable

no root enable

Modes

Global configuration mode

Usage Guidelines

The **no root enable** command disables root access to the device.

Examples

Typical command output:

```
device# configure terminal
device(config)# do show running-config | include root
% No entries found.
device(config)# root enable
% Info: Root password is at system default, for better security, you may want to change
it.
device(config)# do show running-config | include root
root enable
device(config)#
```

route-map (BGP)

Creates or modifies a route-map under Border Gateway Protocol (BGP).

Syntax

route-map *name* { **permit** | **deny** } *stanza*

no route-map *name* { **permit** | **deny** } *stanza*

Parameters

name

Specifies the name of the route map. The string must be between 1 and 63 ASCII characters in length.

permit

Allows a matching pattern.

deny

Disallows a matching pattern.

stanza

Specifies the stanza ID. Valid values range from 1 through 65535. A route map can support up to 1024 stanzas.

Modes

Global configuration mode

Usage Guidelines

This command is used in conjunction with the **match** and **set** commands.

The **continue** command configures the route map to continue to evaluate and execute match statements after a successful match occurs. The **continue** statement proceeds to the route map with the specified sequence number. If no sequence number is specified, the statement proceeds to the route map with the next sequence number (as an "implied" continue).

The **no** form of this command deletes a route-map stanza.

Examples

The following example configures a route map that allows a matching pattern.

```
device# configure terminal
device(config)# route-map test permit 5
```

The following example configures continue statements in a route map.

```
device# configure terminal
device(config)# route-map mcontroutemap1 permit 1
device(config-route-map-mycontroutemap/permit/1)# match metric 10
device(config-route-map-mycontroutemap/permit/1)# set weight 10
device(config-route-map-mycontroutemap/permit/1)# match metric 10
device(config-route-map-mycontroutemap/permit/1)# continue 2
device(config-route-map-mycontroutemap/permit/1)# route-map mcontroutemap1 permit 2
device(config-route-map-mycontroutemap/permit/2)# match tag 10
device(config-route-map-mycontroutemap/permit/2)# set weight 20
```

route-precedence

Defines the order (precedence) in which unicast routes are selected from the unicast routing table (uRTM) for Reverse Path Forwarding resolution.

Syntax

```
route-precedence {none [ priority-1| priority-2 | priority-3 ] | uc-
   default [ priority-1| priority-2 | priority-3 ] | uc-non-default
   [ priority-1| priority-2 | priority-3 ] }

no route-precedence
```

Command Default

The default route precedence is uc-non-default followed by uc-default.

Parameters

none

Specifies that this type of route is to be ignored. You can specify this option for any multicast or unicast route type.

uc-non-default

Specifies the precedence for the non-default unicast route table (uRTM).

uc-default

Specifies the precedence for the default unicast route table (uRTM).

priority-1| priority-2 | priority-3

Specifies the unique priority for the selected route.

Modes

Router PIM configuration mode

Usage Guidelines

The order in which you place the keywords determines the route precedence.

The **no route-precedence** form of this command restores the default route precedence settings.

Examples

The following example configures the route precedence for IPv4 PIM.

```
device(config)# router pim
device(config-pim-router)# route-precedence uc-default uc-non-default none
```

The following example configures the route precedence for IPv6 PIM.

```
device(config)# ipv6 router pim
device(config-ipv6-router-pim-vrf-default-vrf)# route-precedence none priority-3 uc-non-
default
priority-2 uc-default priority-1
```

route-target

Configures route-target for distribution of routes between VPN routing tables.

Syntax

route-target { **import** | **export** | **both** } *ASN-nn*

no route-target

Parameters

import

Specifies export.

export

Specifies export.

both

Specifies both export and import.

ASN-nn

Composed of the local ASN number followed by a colon ":" and a unique arbitrary number. For example 3:6.

Modes

VRF configuration mode

Usage Guidelines

The **no** form of the command to delete configuration for the route-target for distribution.

Examples

The following example shows how to configures route-target for distribution of routes between VPN routing tables.

```
device# configure terminal
device(config)# vrf vpn1
device#(config-vrf-vpn1)# rd1 1:2
device#(config-vrf-vpn1)# vpn-statistics
device#(config-vrf-vpn1)# address-family ipv4 unicast
device#(config-vrf-vpn1-ipv4-unicast)# route-target-import 100:1
device#(config-vrf-vpn1-ipv4-unicast)# route-target-export 100:1
```

route-target (EVPN)

Enables auto-generation of the import and export route-target community attributes for an Ethernet Virtual Private Network (EVPN) default instance.

Syntax

route-target { **both** | **import** } **auto** [**ignore-as**]

route-target export auto

no route-target { **both** | **import** } **auto** [**ignore-as**]

no route-target export auto

Command Default

Disabled.

Parameters

both auto

Specifies auto-generation of the import and export route-target community attributes.

ignore-as

Specifies that the autonomous system (AS) number be ignored.

export auto

Specifies auto-generation of the export route-target community attribute.

import auto

Specifies auto-generation of the import route-target community attribute.

Modes

EVPN configuration mode

Usage Guidelines

The **no** form of this command removes configured route target parameters.

Examples

The following example configures auto-generation of the import and export route-target community attributes for EVPN default instance.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# route-target both auto
```

The following example configures auto-generation of the import route-target community attribute and specifies that the AS path be ignored to the route for EVPN default instance.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# route-target import auto ignore-as
```

The following example configures auto-generation of the export route-target community attribute for EVPN myinstance instance.

```
device# configure terminal
device(config)# evpn myinstance
device(config-evpn-myinstance)# route-target export auto
```

route-target (EVPN VLAN/BD)

Enables auto-generation of the import and export route-target community attributes for a VLAN/bridge domain (BD) in an Ethernet Virtual Private Network (EVPN) default instance.

Syntax

route-target { **both** | **import** } **auto** [*admin-value*:*arbitrary-value*]

route-target export auto [*admin-value*:*arbitrary-value*]

no route-target { **both** | **import** } **auto** [**ignore-as**]

no route-target export auto

Command Default

Disabled.

Parameters

both auto

Specifies auto-generation of the import and export route-target community attributes.

export auto

Specifies auto-generation of the export route-target community attribute.

import auto

Specifies auto-generation of the import route-target community attribute.

admin-value

The administrative number assigned to the route. This can be a local ASN number or an IP address. The ASN number can be either a 2-byte number (from 0 through 65535) or a 4-byte number (from 0 through 4294967295).

arbitrary-value

An arbitrary number you choose. The range of valid values is from 0 through 65535 if the ASN is is an IP address or a 2-byte ASN. The range is 0 through 4294967295 if the ASN is a 4-byte ASN.

Modes

EVPN VLAN/BD configuration mode

Usage Guidelines

The **no** form of this command removes configured route target parameters.

Examples

The following example configures auto-generation of the import and export route-target community attributes for EVPN VLAN/BD 200.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# bridge-domain 200
device(config-bridge-domain-200)# route-target both 200:1
```

router bgp

Enables BGP routing.

Syntax

router bgp

no router bgp

Command Default

BGP routing is not enabled.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command disables BGP routing.

Examples

The following example enables BGP routing.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)#
```

The following example displays maximum paths for EBGP.

```
SLX(config)# router bgp
SLX(config-bgp-router)# address-family ipv4 unicast
SLX#(config-bgp-ipv4u)# maximum-paths ?
Possible completions:
 <1-128> Number of load-sharing paths, default is 1
 ebgp Number of EBGP paths for load sharing
 ibgp Number of IBGP paths for load sharing
 use-load-sharing Number of load-sharing paths: using load-sharing value
SLX#(config-bgp-ipv4u)# maximum-paths 128
SLX(config-bgp-ipv4u)# maximum-paths ebgp ?
Possible completions:
 <1-128> Number of EBGP paths, default - all
 <cr>
SLX(config-bgp-ipv4u)# maximum-paths ebgp 128
SLX(config-bgp-ipv4u)# maximum-paths ibgp ?
Possible completions:
 <1-128> Number of IBGP paths for load sharing, default - all
 <cr>
SLX(config-bgp-ipv4u)# maximum-paths ibgp 128
```

router isis

Enables Intermediate System-to-Intermediate System (IS-IS) routing.

Syntax

router isis

no router isis

Command Default

Disabled

Modes

Global configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command disables IS-IS routing.

Examples

The following example enables IS-IS routing.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)#
```

router mpls

Enables MPLS and accesses MPLS configuration mode

Syntax

router mpls

no router mpls

Command Default

MPLS is disabled by default.

Modes

Global configuration mode

Usage Guidelines

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of this command disables MPLS on the device.

Examples

The following example enables MPLS on the device and accesses MPLS configuration mode.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)#
```

router ospf

Enables and configures the Open Shortest Path First version 2 (OSPFv2) routing protocol.

Syntax

router ospf [**vrf** *name*]

no router ospf

Parameters

vrf *name*

Specifies a nondefault VRF.

Modes

Global configuration mode

Usage Guidelines

Use this command to enable the OSPFv2 routing protocol and enter OSPF router or OSPF router VRF configuration mode. OSPFv2 maintains multiple instances of the routing protocol to exchange route information among various VRF instances.

The **no** form of the command deletes all current OSPF configuration and blocks any further OSPFv2 configuration.

Examples

The following example enables OSPFv2 on a default VRF and enters OSPF VRF router configuration mode.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)
```

router pim

Configures basic global protocol-independent multicast (PIM) Sparse parameters on a device within the PIM Sparse domain and enters PIM-router configuration mode.

Syntax

router pim

no router pim

Command Default

PIM Sparse is not configured.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command disables PIM and removes all configuration for PIM multicast on the device (**router pim** level) only.

You do not need to globally enable IP multicast routing when configuring PIM Sparse.

After you enable IP multicast routing and PIM Sparse at the global level, you must enable it on the individual interfaces connected to the PIM Sparse network.

If you configure PIM Sparse on an interface that is on the border of the PIM Sparse domain, you also must also configure the **ip pim border** command on the interface.

You must configure the **bsr-candidate ethernet** command to identify an interface on at least one device as a candidate PIM Sparse Bootstrap router (BSR) and candidate PIM Sparse Rendezvous Point (RP).

You can configure the **rp-address** command to explicitly identify an RP, including an ACL-based RP, by its IP address instead of having it identified by the RP election process.

Examples

This example configures basic global PIM Sparse parameters.

```
device(config)# router pim
```

router-interface

Binds a router interface to a tunnel or bridge domain.

Syntax

router-interface ve *num*

no router-interface

Command Default

A router interface is not configured.

Parameters

ve *num*

Specifies a virtual interface number on the router.

Modes

Bridge domain configuration mode

Tunnel interface configuration mode

Usage Guidelines

Note
You cannot enable routing on a VPLS instance when the **vc-mode** option on the PW attached to the instance is set to **raw**.

When routing is enabled on a VPLS instance that has only one PW and no local endpoints, the VPLS instance is brought to an active state; this state enables routing when the next hop is the PW endpoint.

The **no** form of the command removes the router interface configuration.

On the MCT bridge-domain VE interface, you can enable routing protocols, such as IS-IS IPv4 or IPv6, OSPF v2 or v3, and BGP IPv4 or IPv6.

Examples

The following example shows how to attach a virtual router interface to a tunnel.

```
device# configure terminal
device(config)# interface tunnel 5
device(config-intf-tunnel-5)# mode gre ip
device(config-intf-tunnel-5)# source 10.1.1.10
device(config-intf-tunnel-5)# source ve 4
```

```
device(config-intf-tunnel-5)# destination 10.1.1.11
device(config-intf-tunnel-5)# router-interface ve 3
```

The following example shows how to bind a virtual router interface to a bridge domain.

```
device# configure terminal
device(config)# bridge-domain 100
device(config-bridge-domain-100)# router-interface ve 100
```

rp-address

Configures a device interface as a static rendezvous point (RP) for IPv4 PIM.

Syntax

rp-address *ip-address*[*group-range-prefix-list*]

no rp-address *ip-address*

Command Default

The RP is selected by the PIM-SM (Sparse Mode) RP election process.

Parameters

ip-address

Specifies the IPv4 address of the RP.

group-range-prefix-list

Specifies the IPv4 multicast group range to be mapped to the RP. The default group range for IPv4 is 224/4.

Modes

Router PIM configuration mode

Usage Guidelines

Devices in the PIM-SM domain use the specified static RP and ignore group-to-RP mappings received from the bootstrap router (BSR).

The RP is the meeting point for PIM-SM sources and receivers. A PIM-SM domain can have multiple RPs, but each PIM-SM multicast group address can have only one active RP. PIM-SM routers learn the addresses of RPs and the groups for which they are responsible from one of the following sources.

- The static RP configuration on each PIM-SM router
- Messages that the BSR sends to each PIM-SM router

The **no rp-address** form of this command restores the default functionality, in which the RP is selected by the RP election process.

Examples

This example configures the device interface at IP address 4.4.4.4 as the RP. The default group range is 224/4.

```
device(config)# router pim
device(config-pim-router)# rp-address 4.4.4.4
```

This example configures the RP with specific group ranges for IPv4.

```
device(config)# router pim
device(config-pim-router)# rp-address 4.4.4.4 static-rp-plist
device(config)# ip prefix-list static-rp-plist permit 225.1.1.0/24
```

This example configures the device interface at IPv6 address 1234::22 as the RP. The default group range is FF00::/8.

```
device(config)# ipv6 router pim
device(config-ipv6-router-pim-vrf-default-vrf)# rp-address 1234::22
```

This example configures the RP with specific group ranges for IPv6.

```
device(config)# ipv6 router pim
device(config-ipv6-router-pim-vrf-default-vrf)# rp-address 1234::22 group-range-plist1
device(config)# ipv6 prefix-list group-range-plist1 permit ff0e::/16
```

rp-candidate

Configures a device as a candidate rendezvous point (RP) for all multicast groups with the prefix 224.0.0.0/4 (IPv4), by default, or for a specified group range.

Syntax

rp-candidate [**interface** {**ethernet** | **loopback** | **port-channel** | **ve**}*interface-number*] | [**prefix** *prefix-list*]

Command Default

By default, the PIM router is not available for selection as an RP.

Parameters

interface ethernet | **loopback** | **port-channel** | **ve** *interface-number*

Specifies an interface for the candidate RP and the interface number in slot or slot/port format.

prefix *prefix-list*

Specifies the list that identifies the IPv4 or IPv6 group address range.

Modes

Router PIM configuration mode

Usage Guidelines

The RP is the meeting point for PIM-SM (Sparse Mode) sources and receivers. A PIM-SM domain can have multiple RPs, but each PIM-SM multicast group address can have only one active RP. PIM-SM routers learn the addresses of RPs and the groups for which they are responsible from messages that the bootstrap router (BSR) sends to PIM-SM router.

Although you can configure the device as only a candidate BSR or an RP, a best practice is to configure the same interface on the same device as both a BSR and an RP.

The **no rp-candidate** form of the command makes the PIM router cease to act as a candidate RP.

Examples

This example configures a physical device as a candidate RP.

```
device(config)# router pim
device(config-pim-router)# rp-candidate interface ethernet 1/1
```

This example configures a loopback interface as a candidate RP.

```
device(config)# router pim
device(config-pim-router)# rp-candidate interface loopback 11
device(config-pim-router)# rp-candidate prefix my-rp-cand-list
device(config)# ip prefix-list my-rp-cand-list permit 226.1.1.0/24
device(config)# ip prefix-list my-rp-cand-list permit 228.1.1.0/24
```

This example configures an IPv6 physical device as a candidate RP.

```
device(config)# ipv6 router pim
device(config-ipv6-router-pim-vrf-default-vrf)# rp-candidate interface ethernet 1/1
```

This example configures the candidate RP with an IPv6 prefix list.

```
device(config)# ipv6 router pim
device(config-ipv6-router-pim-vrf-default-vrf)# rp-candidate prefix group-plist1
```

This example configures an IPv6 loopback interface as a candidate RP.

```
device(config)# ipv6 router pim
device(config-ipv6-router-pim-vrf-default-vrf)# rp-candidate interface loopback 11
device(config-ipv6-router-pim-vrf-default-vrf)# rp-candidate prefix group-plist1
device(config)# ipv6 prefix-list group-plist1 permit ff08::/16
device(config)# ipv6 prefix-list group-plist1 permit ff05::/16
```

rpf ecmp rebalance

Enables multicast ECMP (equal-cost multi-path) load sharing with dynamic rebalancing of traffic to multiple paths through a network.

Syntax

rpf ecmp rebalance

no rpf ecmp rebalance

Modes

Router PIM configuration mode

Usage Guidelines

When ECMP rebalance is enabled, existing flows are redistributed among all available ECMP paths. When a new path is added, some existing flows are redistributed to the new path using the ECMP rebalancing.

The **no rpf ecmp rebalance** form of the command disables ECMP rebalancing.

Examples

The following example enables IPv4 multicast ECMP load sharing with dynamic rebalancing.

```
device(config)# router pim
devic(config-pim-router)# rpf ecmp rebalance
```

The following example enables IPv6 multicast ECMP load sharing with dynamic rebalancing.

```
device(config)# ipv6 router pim
device(config-ipv6-router-pim-vrf-default-vrf)# rpf ecmp rebalance
```

rpf-mode

Enables strict or loose unicast Reverse Path Forwarding (uRPF) mode on an interface.

Syntax

rpf-mode { **loose** | **strict** }

no rpf-mode

Command Default

uRPF mode is not enabled.

Parameters

strict

Specifies uRPF strict mode. For details, see the Usage Guidelines.

loose

Specifies uRPF loose mode. For details, see the Usage Guidelines.

Modes

Interface configuration mode

Hardware configuration mode

Usage Guidelines

This command is applicable only on Layer 3 physical, port-channel, and VE interfaces. On a Layer 3 interface, uRPF is enabled by configuring an uRPF mode on that interface and can be modified to a different mode dynamically on that interface.

On the SLX 9540, RPF mode is not supported when OptiScale is enabled.

Loose mode permits a packet if the source address matches a routing table entry. Packets are dropped only if the source address is not reachable through any device interface.

Strict mode requires a packet to match a known route entry (as described in loose mode) and to arrive at the interface as described in the router table next-hop information. Packets that do not match both of these criteria are dropped.

Neither loose mode nor strict mode includes the default route in the Source IP (SIP) lookup.

Strict mode is not supported for ECMP routes or for IP over MPLS (IPoMPLS).

uRPF is VRF-aware.

Use the **no** form of the command to disable uRPF on an interface.

Examples

The following example enables uRPF in strict mode on an Ethernet interface.

```
device# configure terminal
device(config)# interface eth 1/58
device(conf-if-eth-1/58)# rpf-mode strict
```

rsvp

Accesses MPLS RSVP configuration mode to configure RSVP-TE Hello.

Syntax

rsvp

no rsvp

Command Default

None

Modes

MPLS configuration mode

MPLS interface configuration mode

Usage Guidelines

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example accesses MPLS RSVP configuration mode to configure RSVP-TE Hello globally.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# rsvp
device(config-router-mpls-rsvp)#
```

The following example accesses MPLS RSVP configuration mode to configure RSVP-TE Hello on an MPLS interface.

```
device# configure terminal
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/12
device(config-router-mpls-interface-0/12)# rsvp
device(config-router-mpls-interface-0/12-rsvp)#
```

rsvp-flooding-threshold

The **rsvp-flooding-threshold** command can be executed multiple times for the same interface. The threshold values are added to the existing set of values for the interface.

Syntax

rsvp-flooding-threshold [**down** | **up**] *percent **

no rsvp-flooding-threshold [**down** | **up**] *percent **

Command Default

The command is disabled, by default.

Parameters

down *percent**

The down option sets the thresholds for decreased resource availability. Valid values are from 0 to 99. The default values for down is 100, 99, 98, 97, 96, 95, 90, 85, 80, 75, 60, 45, 30, 15.

The "*" represents multiple percent values can be given. A minimum one percentage value is required.

up *percent**

The up option sets the thresholds for increased resource availability. Valid values are from 1 to 100. The default values for up is 15, 30, 45, 60, 75, 80, 85, 90, 95, 97, 98, 99, 100.

The "*" represents multiple percent values can be given. A minimum one percentage value is required.

Modes

MPLS policy mode.

Usage Guidelines

The **no** form of the command removes the RSVP TE flooding threshold configuration.

Previously configured values are not overwritten. The interface specific configuration overrides the global configuration.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

In the following example, the UP thresholds contain 10, 50, 55, 95, 96, 97, 98, and 100. The DOWN thresholds contain 50, 40, 30, 20, and10.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 0/1
device(config-router-mpls-if-eth-0/1)# rsvp-flooding-threshold up 10 50 55 95
device(config-router-mpls-if-eth-0/1)# rsvp-flooding-threshold up 96 97 98 99 100
device(config-router-mpls-if-eth-0/1)# rsvp-flooding-threshold down 50 40
device(config-router-mpls-if-eth-0/1)# rsvp-flooding-threshold down 30 20 10
```

rsvp-periodic-flooding-time

Sets the interval for RSVP-TE periodic flooding.

Syntax

rsvp-periodic-flooding-time *interval*

no rsvp-periodic-flooding-time

Command Default

All MPLS interfaces are checked every three minutes by default. The length of interval value is set to zero.

Parameters

interval

Specifies the length of interval used for periodic flooding (in seconds). Valid range is zero, 30-3600. For value zero, periodic flooding is turned off.

Modes

MPLS policy mode

Usage Guidelines

TE advertisements are triggered when there is a difference in the available bandwidth and advertised available bandwidth.

The **no** form of the command can be used to set the periodic flooding timer to default value.

Examples

The following example sets the interval as 240, which triggers periodic flooding every four minutes.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# rsvp-periodic-flooding-time 240
device(config-router-mpls-policy)# no rsvp-periodic-flooding-time
```

rule

Creates role-based access permissions (RBAC) associated with a role.

Syntax

rule *index* [**action** { **accept** | **reject** }] [**operation** { **read-only** | **read-write** }] **role** *role_name* **command** *command_name*

no rule *index*

Command Default

The default for **action** is **accept**. The default for **operation** is **read-write**.

Parameters

index

Specifies a numeric identifier for the rule. Valid values range from 1 through 512.

action accept | **reject**

(Optional) Specifies whether the user is accepted or rejected while attempting to execute the specified command. The default value is **accept**.

operation read-only | **read-write**

(Optional) Specifies the type of operation permitted. The default value is **read-write**.

role *role_name*

Specifies the name of the role for which the rule is defined.

command *command_name*

Specifies the command for which access is defined. Separate commands with a space. To display a list of supported commands, type a question mark (?).

Modes

Global configuration mode

Usage Guidelines

For each role that you create, you define one or more rules. Each account is associated with one—and only one—role.

When you create a rule, the *index*, **role**, and **command** operands are mandatory; the **action** and **operation** operands are optional.

The maximum number of rules is 512.

When you modify a rule, all operands except *index* and **role** are optional.

Enter **no rule** *index* to remove the specified rule.

Examples

The following example creates rules enabling the NetworkSecurityAdmin role to create user accounts.

```
device# configure terminal
device(config)# rule 150 action accept operation read-write role NetworkSecurityAdmin
command config
device(config)# rule 155 action accept operation read-write role NetworkSecurityAdmin
command username
```

The following example deletes a rule.

```
device# configure terminal
device(config)# no rule 155
```

rule-name

Enables adding a meaningful, human readable rule name to a route map definition.

Syntax

rule-name *rule-name-string*

no rule-name *rule-name-string*

Parameters

rule-name-string

Enables adding a meaningful, human readable description to a route map as its name. Maximum length 127 characters.

Usage Guidelines

The **no** format of this command removes the assigned descriptive name from this route map.

Modes

Route Map Configuration mode

Examples

The following example enables the adding of a description to route map configuration rule.

```
SLX (config)# route-map rmap1 permit 10
SLX (config-route-map-rmap1/permit/10)# rule-name permit-rule
```

rx-label-silence-time

Defines the length of the receive label silence timer for LDP-IGP synchronization.

Syntax

rx-label-silence-time *milliseconds*

no rx-label-silence-time

Command Default

The default value is 1000 milliseconds.

Parameters

milliseconds

Specifies the length of time in milliseconds of the receive label silence timer. Enter an integer from 100 to 60000.

Modes

MPLS LDP configuration mode

Usage Guidelines

Use the **no** form of the command to reset the default value of 1000 milliseconds.

When labels are not received from the peer for a short period of time, the session is declared In Sync. When a label is received from a peer, then the receive label silence timer is reset.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example sets the receive label silence timer to 80000 milliseconds.

```
device(conf)# router mpls
device(config-mpls)# ldp
device(config-router-mpls-ldp)# rx-label-silence-time 80000
```

secure-port

Configures the port on which the SLX-OS device will listen for incoming secure connections. Configure a port in the range 1024-49151.

Syntax

secure-port *port-number*

[no] secure-port

Command Default

By default, the gNMI server listens on port 9339. Connections on this port are not secured.

Parameters

port-number

Configures the port on which the gNMI server will listen for incoming connections. Configure a port in the range 1024-49151.

Modes

gNMI Server mode.

Usage Guidelines

The presence of this configuration indicates that gNMI access is secure. If this configuration is not present, then the access is insecure. You can also use the default port 9339 as a secure port. To do so, configure the port as the secure port. This configuration works along with the minimum TLS version support to enhance security.

Examples

This example configures the secure gNMI port as 48151

```
SLX (config)# gnmi server
SLX (config-gNMI-server)#  secure-port 48151
```

sample-recording

Configures the template to record the sample history.

Syntax

sample-recording [**disable** | **enable**]

no sample-recording

Command Default

The command is disabled by default.

Parameters

disable

Removes the setting for the sample recording for the selected LSP or autobw-template.

enable

Sets the sample recording for ththe selected LSP or autobw-template.

Modes

MPLS sub-configuration modes.

config-router-mpls-autobw-template-template1

config-router-mpls-lsp-lsp1

Usage Guidelines

The **no** function of the command disables the option.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example shows a configuration to record the sample history for *template1*.

```
device>configure
device(config)# router mpls
device(config-router-mpls)# autobw
device(config-router-mpls-autobw)# template template1
device(config-router-mpls-autobw-template-template1)# sample-recording enable
```

The following example shows a configuration to stop recording sample history for *LSP1*.

```
device>configure
device(config)# router mpls
device(config-router-mpls)# lsp lsp1
device(config-router-mpls-lsp-lsp1)# autobw
device(config-router-mpls-lsp-lsp1-autobw)# sample-recording disable
```

scheduler

Configures the strict priority queues on an interface for QoS egress scheduling.

Syntax

scheduler strict-priority *traffic-class-queues* **dwrr** *TC0-BW% TC1-BW% TC2-BW% TC3-BW% TC4-BW% TC5-BW% TC6-BW% TC7-BW%* [**TC0** *bytes*] [**TC1** *bytes*] [**TC2** *bytes*] [**TC3** *bytes*] [**TC4** *bytes*] [**TC5** *bytes*] [**TC6** *bytes*] [**TC7** *bytes*]

no scheduler strict-priority

Parameters

traffic-class-queues

Specifies the traffic class strict priority queues. Enter one of the following integers:

- 0—No strict priority queues
- 1—Traffic class 7 strict priority queue
- 2—Traffic class 6 through 7 strict priority queues
- 3—Traffic class 5 through 7 strict priority queues
- 4—Traffic class 4 through 7 strict priority queues
- 5—Traffic class 3 through 7 strict priority queues
- 6—Traffic class 2 through 7 strict priority queues
- 7—Traffic class 1 through 7 strict priority queues

drww *TC0-BW% TC1-BW% TC2-BW% TC3-BW% TC4-BW% TC5-BW% TC6-BW% TC7-BW%*

Configures the Deficit Weighted Round Robin queues in percentage for each traffic class, if the priority is in weighted fair queue (WFQ) mode. Enter an integer from 0 through 100 (*TC0-BW* for traffic class 0 through *TC7-BW* for traffic class 7). The total of all values must equal 100%.

TC0 - TC7 *bytes*

Sets the maximum bandwidth the queue can transmit. This value is in bytes.

Modes

Policy-map configuration mode

Usage Guidelines

This command is allowed only for the egress direction.

Use the **no** form of this command to remove QoS egress scheduling from the interface.

Examples

The following example configures QoS egress scheduling on an interface.

```
device# configure terminal
device(config)# policy-map policy_1
device(config-policymap)# class default
device(config-policymap-class)# scheduler strict-priority 1 dwrr 25 25 25 10 5 5 5
```

The following example command configures the QoS egress scheduling on an interface with TC0-TC3 with equal weights and TC4-TC7 as strict, but with queue shapers of 2.0 Gbps, 1.5 Gbps, 1.0 Gbps, and 0.5 Gbps respectively.

```
device# configure terminal
device(config)# policy-map policy_2
device(config-policymap)#class default
device(config-policymap-class)# scheduler strict-priority 4 dwrr 25 25 25 25
        TC4 2000000 TC5 1500000 TC6 1000000 TC7 500000
device(config-policymap-class)# int eth 0/29-30
device(conf-if-eth-0/29-30)# no service-policy out
device(conf-if-eth-0/29-30)# service-policy out h1
```

seq (rules in IPv4 extended ACLs)

Inserts filtering rules in IPv4 extended ACLs. Extended ACLs permit or deny traffic according to source addresses, as well as other parameters.

Syntax

seq *seq-value* { **permit** | **deny** | **hard-drop** } *ip-protocol* { *S_IPaddress mask* | **host** *S_IPaddress* | **any** } [*source-operator* [*S_port-numbers*]] [*TCP-flags*] [**vlan** *vlanID*] [**count**] [**log**] [**mirror**] [**copy-sflow**] [**fragment** | **non-fragment**] [**connlimit** *connlimit-value*]

no seq *seq-value*

{ **permit** | **deny** | **hard-drop** } *ip-protocol* { *S_IPaddress mask* | **host** *S_IPaddress* | **any** } [*source-operator* [*S_port-numbers*]] [*TCP-flags*] [**count**] [**vlan** *vlanID*] [**log**] [**mirror**] [**copy-sflow**] [**fragment** | **non-fragment**] [**connlimit** *connlimit-value*]

no { **permit** | **deny** | **hard-drop** } *ip-protocol* { *S_IPaddress mask* | **host** *S_IPaddress* | **any** } [*source-operator* [*S_port-numbers*]] [*TCP-flags*] [**vlan** *vlanID*] [**count**] [**log**] [**mirror**] [**copy-sflow**] [**fragment** | **non-fragment**] [**connlimit** *connlimit-value*]

Parameters

seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq** *seq-value*, the rule is added at the end of the list.

seq-value

Valid values range from 1 through 65535.

permit

Specifies rules to permit traffic.

deny

Specifies rules to deny traffic.

hard-drop

Overrides the trap behavior for control frames. However, **hard-drop** does not override a **permit** for this address in a preceding rule.

ip-protocol

Indicates the type of IP packet you are filtering. The options are as follows:

<0-255>

Protocol number custom value from 0 through 255.

icmp

Internet Control Message Protocol

ip

Any IP protocol

tcp

(Supported only if the containing ACL is applied to incoming traffic) Transmission Control Protocol

udp

User Datagram Protocol

S_IPaddress

Specifies a source address for which you want to filter the subnet.

mask

Defines a mask, whose effect is to specify a subnet that includes the source address that you specified. For options to specify the mask, see the Usage Guidelines.

host

Specifies a source address.

S_IPaddress

The source address.

any

Specifies all source addresses.

source-operator

If you specified **tcp** or **udp** *ip-protocol*, the following optional operators are available:

eq

The policy applies to the TCP or UDP port name or number you enter after **eq.**

gt

The policy applies to TCP or UDP port numbers equal to or greater than the port number or the numeric equivalent of the port name you enter after **gt.**

lt

The policy applies to TCP or UDP port numbers that are equal to or less than the port number or the numeric equivalent of the port name you enter after **lt.**

neq

The policy applies to all TCP or UDP port numbers except the port number or port name you enter after **neq.**

range

The policy applies to all TCP or UDP port numbers that are between the first TCP or UDP port name or number and the second one you enter following the **range** keyword. The range includes the port names or numbers you enter. For example, to apply the policy to all ports between and including 23 (Telnet) and 53 (DNS), enter the following: range 23 53 (two values separated by a space). The first port number in the range must be lower than the last number in the range.

S_port-numbers

(Valid only when *ip-protocol* is UDP or TCP) Specifies one or more source port numbers.

vlan *vlanID*

Specifies a VLAN interface to which the ACL is bound.

TCP-flags

If you specify **tcp** *ip-protocol*, one or more of the following flags are available:

ack

Filters packets for which the **ack** (acknowledge) flag is set.

fin

Filters packets for which the **fin** (finish) flag is set.

rst

Filters packets for which the **rst** (reset) flag is set.

sync

Filters packets for which the **syn** (synchronize) flag is set.

urg

Filters packets for which the **urg** (urgent) flag is set.

push

Filters packets for which the **psh** (push) flag is set.

count

Enables statistics for the rule.

log

Enables inbound logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

mirror

(Supported for rules in ACLs applied on physical interfaces to inbound traffic. Not supported for PBR, rACLs, or ACL-RL.) Mirrors packets matching the rule.

copy-sflow

For incoming traffic, sends matching packets to the sFlow collector.

fragment

Filter fragmented packets. This keyword and *non-fragment* keyword cannot be used together.

non-fragment

Filter non-fragmented packets. This keyword and *fragment* keyword cannot be used together.

connlimit connlimit-value

Number of connections allowed per IP address.

Modes

ACL configuration mode

Usage Guidelines

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

You can specify a mask in either of the following ways:

- Wildcard mask format—for example, 0.0.0.255. The advantage of this format is that it enables you mask any bit, for example by specifying 0.255.0.255.
- Classless Interdomain Routing (CIDR) format—in which you specify the number of bits of the prefix. For example, appending /24 to an IPv4 address is equivalent to specifying 0.0.0.255 as wildcard mask format.

Although in an extended-ACL rule you can include **log**, **mirror**, and **copy-sflow**, only one of the three is processed, as follows:

- In a permit rule, the order of precedence is **mirror** > **copy-sflow** > **log**.
- In a deny or hard-drop rule, the order of precedence is **log** > **copy-sflow** > **mirror**.

If you are defining rules for a QoS ACL, be aware of the following considerations for ACLs implemented under flow-based QoS. (For details, refer to the *Extreme SLX-OS QoS and Traffic Management Configuration Guide*.)

- Because ACLs applied for QoS use implement a unified counter for all rules in an ACL, rule-level **count** keywords are ignored.
- The **deny** keyword functions as a PASS THROUGH: For a match, QoS action defined for that class is not applied.

For both interface ACLs and receive-path ACLs, you use identical commands to create the ACLs. You also use identical commands to define permit/deny rules in the ACLs. The only variance is the command you use to apply the ACL:

- To apply an interface ACL, from an interface-subtype configuration mode you use the { **ip** | **ipv6** | **mac** } **access-group** command.
- To apply a receive-path ACL, from global configuration mode, you use the { **ip** | **ipv6** } **receive access-group** command.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq** *seq-value*.
- If you do not know the rule number, type **no** followed by the full syntax without **seq** *seq-value*.

Filtering fragmented or non-fragmented packets is only supported on ingress ACLs. On the SLX 9540 and SLX 9640, fragment match is only supported on BGP FS profile. This ACL can also be used with RACL, PBR, and RL. Do not use Layer-4 matching along with fragment matching. Fragmented packets might not have Layer-4 information and

most likely cause issues. ACL filtering of fragmented and non-fragmented packets is not supported on SLX 9150 and SLX 9250 devices.

When configured, the *connlimit* value behaves differently. When used with a *permit* rule, this command will limit the concurrent connections from a particular IP address to this value. When used with a *deny* rule, this command will allow connections up to this limit and deny any more connections from the particular IP address. Also, *connection limiting* is applicable only to the management interfaces and not applicable to the front panel (ethernet) ports. Existing sessions might be disrupted when this value is configured.

Examples

The following example creates an IPv4 extended ACL and defines rules.

```
device(config)# ip access-list extended extdACL5
                    device(conf-ipacl-ext)# seq 5 deny tcp host 10.24.26.145 any eq 23
                    device(conf-ipacl-ext)# seq 7 deny tcp any any eq 80
                    device(conf-ipacl-ext)# seq 10 deny udp any any range 10 25
                    device(conf-ipacl-ext)# seq 15 permit tcp any any
```

The following example creates an IPv4 extended ACL, defines rules in the ACL, and applies it as a receive-path ACL.

```
device(config)# ip access-list extended ipv4-receive-acl-example
                    device(conf-ipacl-ext)# hard-drop tcp host 10.0.0.1 any count
                    device(conf-ipacl-ext)# hard-drop udp any host 20.0.0.1 count
                    device(conf-ipacl-ext)# permit tcp host 10.0.0.2 any eq telnet count
                    device(conf-ipacl-ext)# permit tcp host 10.0.0.2 any eq bgp count
                    device(conf-ipacl-ext)# hard-drop tcp host 10.0.0.3 host 224.0.0.1
count
                    device(conf-ipacl-ext)# exit
                    device(config)# ip receive access-group ipv4-receive-acl-example
```

seq (rules in IPv4 extended bACLs)

Inserts filtering rules in IPv4 extended ACLs crafted as IP broadcast ACLs (bACLs).

Syntax

seq *seq-value* { **permit** | **deny** } *ip-protocol* { *S_IPaddress mask* | **host** *S_IPaddress* | **any** } [*source-operator* [*S_port-numbers*]] [*TCP-flags*] [**vlan** *vlanID*] [**count**] [**fragment** | **non-fragment**]

no seq *seq-value*

{ **permit** | **deny** } *ip-protocol* { *S_IPaddress mask* | **host** *S_IPaddress* | **any** } [*source-operator* [*S_port-numbers*]] [*TCP-flags*] [**count**] [**vlan** *vlanID*] [**fragment** | **non-fragment**]

no { **permit** | **deny** } *ip-protocol* { *S_IPaddress mask* | **host** *S_IPaddress* | **any** } [*source-operator* [*S_port-numbers*]] [*TCP-flags*] [**vlan** *vlanID*] [**count**] [**fragment** | **non-fragment**]

Parameters

seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq** *seq-value*, the rule is added at the end of the list.
seq-value

Valid values range from 1 through 65535.

permit

Specifies rules to permit traffic.

deny

Specifies rules to deny traffic.

hard-drop

For bACLs, equivalent to deny.

ip-protocol

Indicates the type of IP packet you are filtering. The options are as follows:
<0-255>

Protocol number custom value from 0 through 255.

icmp

Internet Control Message Protocol

ip

Any IP protocol

tcp

(Supported only if the containing ACL is applied to incoming traffic) Transmission Control Protocol

udp

User Datagram Protocol

S_IPaddress

Specifies a source address for which you want to filter the subnet.

mask

Defines a mask, whose effect is to specify a subnet that includes the source address that you specified. For options to specify the mask, see the Usage Guidelines.

host

Specifies a source address.

S_IPaddress

The source address.

any

Specifies all source addresses.

source-operator

If you specified **tcp** or **udp** *ip-protocol*, the following optional operators are available:

eq

The policy applies to the TCP or UDP port name or number you enter after **eq.**

gt

The policy applies to TCP or UDP port numbers equal to or greater than the port number or the numeric equivalent of the port name you enter after **gt.**

lt

The policy applies to TCP or UDP port numbers that are equal to or less than the port number or the numeric equivalent of the port name you enter after **lt.**

neq

The policy applies to all TCP or UDP port numbers except the port number or port name you enter after **neq.**

range

The policy applies to all TCP or UDP port numbers that are between the first TCP or UDP port name or number and the second one you enter following the **range** keyword. The range includes the port names or numbers you enter. For example, to apply the policy to all ports between and including 23 (Telnet) and 53 (DNS), enter the following: range 23 53 (two values separated by a space). The first port number in the range must be lower than the last number in the range.

S_port-numbers

(Valid only when *ip-protocol* is UDP or TCP) Specifies one or more source or destination port numbers.

vlan *vlanID*

Specifies a VLAN interface to which the ACL is bound.

TCP-flags

If you specify **tcp** *ip-protocol*, one or more of the following flags are available:

ack

Filters packets for which the **ack** (acknowledge) flag is set.

fin

Filters packets for which the **fin** (finish) flag is set.

rst

Filters packets for which the **rst** (reset) flag is set.

sync

Filters packets for which the **syn** (synchronize) flag is set.

urg

Filters packets for which the **urg** (urgent) flag is set.

push

Filters packets for which the **psh** (push) flag is set.

count

Enables statistics for the rule.

log

Not supported for bACLs.

mirror

Not supported for bACLs.

copy-sflow

Not supported for bACLs.

fragment

Filter fragmented packets. This keyword and *non-fragment* keyword cannot be used together.

non-fragment

Filter non-fragmented packets. This keyword and *fragment* keyword cannot be used together.

Modes

ACL configuration mode

Usage Guidelines

This topic describes filtering rules in an extended IPv4 ACL intended for use as an IP broadcast ACL (bACL).

Broadcast ACLs are not supported on SLX 9150 or SLX 9250 devices.

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

You can specify a mask in either of the following ways:

- Wildcard mask format—for example, 0.0.0.255. The advantage of this format is that it enables you mask any bit, for example by specifying 0.255.0.255.
- Classless Interdomain Routing (CIDR) format—in which you specify the number of bits of the prefix. For example, appending /24 to an IPv4 address is equivalent to specifying 0.0.0.255 as wildcard mask format.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq** *seq-value*.
- If you do not know the rule number, type **no** followed by the full syntax without **seq** *seq-value*.

Filtering fragmented or non-fragmented packets is only supported on ingress ACLs. On the SLX 9540 and SLX 9640, fragment match is only supported on BGP FS profile. This ACL can also be used with RACL, PBR, and RL. Do not use Layer-4 matching along with fragment matching. Fragmented packets might not have Layer-4 information and most likely cause issues. ACL filtering of fragmented and non-fragmented packets is not supported on SLX 9150 and SLX 9250 devices.

Examples

The following example creates an IPv4 extended bACL, defines rules for it, and applies the bACL to an interface.

```
device# configure
device(config)# ip access-list extended bACL_ext_12
device(conf-ipacl-ext)# seq 5 deny tcp host 10.24.26.145 any eq 23
device(conf-ipacl-ext)# seq 7 deny tcp any any eq 80
device(conf-ipacl-ext)# seq 10 deny udp any any range 10 25
device(conf-ipacl-ext)# seq 15 permit tcp any any
device(conf-ipacl-ext)# exit
device(config)# interface ethernet 0/6
device(conf-if-eth-0/6)# ip subnet-broadcast-acl bACL_ext_12
```

The following example creates an IPv4 extended bACL, defines rules for it, and applies the bACL at device level.

```
device# configure
device(config)# ip access-list extended bACL_ext_22
device(conf-ipacl-ext)# seq 5 deny tcp host 10.24.26.145 any eq 23
device(conf-ipacl-ext)# seq 7 deny tcp any any eq 80
device(conf-ipacl-ext)# seq 10 deny udp any any range 10 25
device(conf-ipacl-ext)# seq 15 permit tcp any any
device(conf-ipacl-ext)# exit
device(config)# ip global-subnet-broadcast-acl bACL_ext_22
```

seq (rules in IPv4 standard ACLs)

Inserts filtering rules in IPv4 standard ACLs. Standard ACLs permit or deny traffic according to source address only.

Syntax

seq *seq-value* { **permit** | **deny** | **hard-drop** } { *S_IPaddress mask* | **host** *S_IPaddress* | **any** } [**count**] [**log**] [**copy-sflow**]

no seq *seq-value*

{ **permit** | **deny** | **hard-drop** } { *S_IPaddress mask* | **host** *S_IPaddress* | **any** } [**count**] [**log**] [**copy-sflow**]

no { **permit** | **deny** | **hard-drop** } { *S_IPaddress mask* | **host** *S_IPaddress* | **any** } [**count**] [**log**] [**copy-sflow**]

Parameters

seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq** *seq-value*, the rule is added at the end of the list.
seq-value

Valid values range from 1 through 65535.

permit

Specifies rules to permit traffic.

deny

Specifies rules to deny traffic.

hard-drop

Overrides the trap behavior for control frames. However, **hard-drop** does not override a **permit** for this address in a preceding rule.

S_IPaddress

Specifies a source address for which you want to filter the subnet.
mask

Defines a mask, whose effect is to specify a subnet that includes the source address that you specified. For options to specify the mask, see the Usage Guidelines.

host

Specifies a source address.
S_IPaddress

The source address.

any

Specifies all source addresses.

count

Enables statistics for the rule.

log

Enables inbound logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

copy-sflow

For incoming traffic, sends matching packets to the sFlow collector.

Modes

ACL configuration mode

Usage Guidelines

This command configures rules to permit or drop traffic based on source addresses. You can also enable counters, logging, and sFlow.

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

You can specify a mask in either of the following ways:

- Wildcard mask format—for example, 0.0.0.255. The advantage of this format is that it enables you mask any bit, for example by specifying 0.255.0.255.
- Classless Interdomain Routing (CIDR) format—in which you specify the number of bits of the prefix. For example, appending /24 to an IPv4 address is equivalent to specifying 0.0.0.255 as wildcard mask format.

Although in a standard-ACL rule you can specify both **log** and **copy-sflow**, only one of the two is processed, as follows:

- In a permit rule, only **copy-sflow** is processed.
- In a deny or hard-drop rule, only **log** is processed.

If you are defining rules for a QoS ACL, be aware of the following considerations for ACLs implemented under flow-based QoS. For details, refer to the *Extreme SLX-OS QoS and Traffic Management Configuration Guide*.

- Do not include the **count** keyword in ACLs intended for flow-based QoS implementation, because such ACLs automatically share a common counter.
- The **deny** keyword functions as a "pass-through": For a match, QoS action defined for that class is not applied.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq** *seq-value*.
- If you do not know the rule number, type **no** and then enter the full syntax without **seq** *seq-value*.

Examples

The following example shows how to create a IPv4 standard ACL, define rules for it, and apply the ACL to an interface:

```
device# configure
device(config)# ip access-list standard stdACL3
device(conf-ipacl-std)# seq 5 permit host 10.20.33.4
device(conf-ipacl-std)# seq 15 deny any
device(conf-ipacl-std)# exit
device(config)# interface ethernet 0/5
device(conf-if-eth-0/5)# ipv4 access-group stdACL3 in
```

seq (rules in IPv6 extended ACLs)

Inserts filtering rules in IPv6 extended ACLs.

Syntax

seq *seq-value* { **permit** | **deny** | **hard-drop** } *ip-protocol* { **any** | *S_IPaddress* **/** *prefix_len* | **host** *S_IPaddress* } [*source-operator* [*S_port-numbers*]] [*tcp/udp-flags*] [**vlan** *vlanID*] [**count**] [**log**] [**mirror**] [**copy-sflow**] [**connlimit** *connlimit-value*]

no seq *seq-value*

{ **permit** | **deny** | **hard-drop** } *ip-protocol* { **any** | *S_IPaddress* **/** *prefix_len* | **host** *S_IPaddress* } [*source-operator* [*S_port-numbers*]] [*tcp/udp-flags*] [**vlan** *vlanID*] [**count**] [**log**] [**mirror**] [**copy-sflow**] [**connlimit** *connlimit-value*]

no { **permit** | **deny** | **hard-drop** } *ip-protocol* { **any** | *S_IPaddress* **/** *prefix_len* | **host** *S_IPaddress* } [*source-operator* [*S_port-numbers*]] [*tcp/udp-flags*] [**vlan** *vlanID*] [**count**] [**log**] [**mirror**] [**copy-sflow**] [**connlimit** *connlimit-value*]

Parameters

seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq** *seq-value*, the rule is added at the end of the list.
seq-value

Valid values range from 1 through 65535.

permit

Specifies rules to permit traffic.

deny

Specifies rules to deny traffic.

hard-drop

Overrides the trap behavior for control frames. However, **hard-drop** does not override a **permit** for this address in a preceding rule.

ip-protocol

Indicates the type of IP packet you are filtering. The options are as follows:
<0-255>

Protocol number custom value from 0 through 255.

ipv6-icmp

Internet Control Message Protocol

ipv6

Any IP protocol

tcp

Transmission Control Protocol

udp

User Datagram Protocol

any

Specifies all source addresses.

S_IPaddress

Specifies a source address for which you want to filter the subnet. For options to abbreviate the address, see the Usage Guidelines.

prefix_len

Indicates how many of the high-order, contiguous bits of the address comprise the IPv6 prefix.

host

Specifies a source address.

S_IPaddress

The specific address. For options to abbreviate the address, see the Usage Guidelines.

source-operator

If you specified **tcp** or **udp** *ip-protocol*, the following optional operators are available:

eq

The policy applies to the TCP or UDP port name or number you enter after **eq.**

gt

The policy applies to TCP or UDP port numbers equal to or greater than the port number or the numeric equivalent of the port name you enter after **gt**.

lt

The policy applies to TCP or UDP port numbers that are equal to or less than the port number or the numeric equivalent of the port name you enter after **lt.**

neq

The policy applies to all TCP or UDP port numbers except the port number or port name you enter after **neq.**

range

The policy applies to all TCP or UDP port numbers that are between the first TCP or UDP port name or number and the second one you enter following the **range** keyword. The range includes the port names or numbers you enter. For example, to apply the policy to all ports between and including 23 (Telnet) and 53 (DNS), enter the following: range 23 53 (two values separated by a space). The first port number in the range must be lower than the last number in the range.

S_port-numbers

(Valid only when *ip-protocol* is UDP or TCP) Specify one or more port numbers.

drop-precedence-force *dp-value*

In **permit** rules applied to incoming traffic, forces drop precedence to a value of 0 through 2. On SLX 9540 or SLX 9640 devices, the **drop-precedence-force** keyword is supported only under the default, vxlan-ext, and bgp-flowspec TCAM profiles.

vlan *vlanID*

Specifies a VLAN interface to which the ACL is bound.

tcp/udp-flags

If you specify **tcp** or **udp** *ip-protocol*, one or more of the following flags are available:

ack

Filters packets for which the **ack** (acknowledge) flag is set.

fin

Filters packets for which the **fin** (finish) flag is set.

rst

Filters packets for which the **rst** (reset) flag is set.

sync

Filters packets for which the **syn** (synchronize) flag is set.

urg

Filters packets for which the **urg** (urgent) flag is set.

push

Filters packets for which the **psh** (push) flag is set.

count

Enables statistics for the rule.

log

Enables inbound logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

mirror

(Supported for rules in ACLs applied on physical interfaces to inbound traffic. Not supported for PBR, rACLs, or ACL-RL.) Mirrors packets matching the rule.

copy-sflow

For incoming traffic, sends matching packets to the sFlow collector.

connlimit connlimit-value

Number of connections allowed per IP address.

Modes

ACL configuration mode

Usage Guidelines

IPv6 extended ACLs permit or deny traffic according to source address, as well as other parameters.

An IPv6 ACL can only be applied to incoming traffic.

IPv6 filtering by destination address is not supported.

The order of the rules in an ACL is critical, because the first matching rule stops further processing. When you create rules, specify the sequence values to determine the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

You can abbreviate an IPv6 address by using one or more of the following rules:

- Remove one or more leading zeros from one or more groups of hexadecimal digits, usually for all or none of the leading zeros. (For example, convert the group 0042 to 42.)
- Omit consecutive sections of zeros, using a double colon (::) to denote the omitted sections. The double colon is used only once in any given address. The address would be indeterminate if the double colon were used multiple times. A double colon cannot be used to denote one omitted section of zeros. (For example, 2001:db8::1:2 is valid, but 2001:db8::1::2 or 2001:db8::1:1:1:1:1 is not permitted.)

Although in an extended-ACL rule you can include **log**, **mirror**, and **copy-sflow**, only one of the three is processed, as follows:

- In a permit rule, the order of precedence is **mirror** > **copy-sflow** > **log**.
- In a deny or hard-drop rule, the order of precedence is **log** > **copy-sflow** > **mirror**.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq** *seq-value*.
- If you do not know the rule number, type **no** followed by the full syntax except for **seq** *seq-value*.

Filtering fragmented or non-fragmented packets is only supported on ingress ACLs. For IPv6 frames, filtering is only supported if the fragment is the first extension header. Use protocol number *44* for fragmented extension header. ACL filtering of fragmented and non-fragmented packets is not supported on SLX 9150 and SLX 9250 devices.

Examples

The following example creates an IPv6 extended ACL, defines a rule for it, and applies the ACL to an interface.

```
device# configure
                        device(config)# ipv6 access-list extended ip_acl_1
                        device(conf-ip6acl-ext)# seq 10 deny ipv6 2001:2002:1234:1::/64
2001:1001:1234:1::/64 count
                        device(conf-ip6acl-ext)# exit
                        device(config)# interface ethernet 0/5
                        device(conf-if-eth-0/5)# ipv6 access-group ip_acl_1 in
```

The following example creates an IPv6 extended ACL, defines rules in the ACL, and applies it as a receive-path ACL (rACL).

```
device(config)# ipv6 access-list extended ipv6-receive-acl-example
device(conf-ip6acl-ext)# hard-drop tcp host 10::1 any count
device(conf-ip6acl-ext)# hard-drop udp any host 20::1 count
device(conf-ip6acl-ext)# permit tcp host 10::2 any eq telnet count
device(conf-ip6acl-ext)# permit tcp host 10::2 any eq bgp count
device(conf-ip6acl-ext)# hard-drop tcp host 10::3 host ff02::1 count

device(conf-ip6acl-ext)# exit
device(config)# ipv6 receive access-group ipv6-receive-acl-example
```

The following example creates an IPv6 extended ACL for permitting fragmented packets.

```
device(config)# ipv6 access-list extended ipv6-receive-acl-example
device(conf-ip6acl-ext)# seq 10 permit 44 any any count
```

seq (rules in IPv6 standard ACLs)

Inserts filtering rules in IPv6 standard ACLs. Standard ACLs permit or deny traffic according to source address only.

Syntax

seq *seq-value* { **deny** | **permit** | **hard-drop** } { **any** | **A:B:C:D:E:F:H:I /** **prefix_len** | **host** *S_IPaddress* } [**count**] [**log**] [**copy-sflow**]

no seq *seq-value*

{ **deny** | **permit** | **hard-drop** } { **any** | **A:B:C:D:E:F:H:I / prefix_len** | **host** *SIP_address* | *SIP_addressmask* } [**count**] [**log**] [**copy-sflow**]

no { **deny** | **permit** | **hard-drop** } { **any** | **A:B:C:D:E:F:H:I / prefix_len** | **host** *SIP_address* | *SIP_addressmask* } [**count**] [**log**] [**copy-sflow**]

Parameters

seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq** *seq-value*, the rule is added at the end of the list.
seq-value

Valid values range from 1 through 65535.

permit

Specifies rules to permit traffic.

deny

Specifies rules to deny traffic.

hard-drop

Overrides the trap behavior for control frames. However, **hard-drop** does not override a **permit** for this address in a preceding rule.

any

Specifies all source addresses.

S_IPaddress

Specify a source address for which you want to filter the subnet. For options to abbreviate the address, see the Usage Guidelines.
prefix_len

Indicates how many of the high-order, contiguous bits of the address comprise the IPv6 prefix.

host

Specifies a source address.
SIP_address

The source address. For options to abbreviate the address, see the Usage Guidelines.

count

Enables statistics for the rule.

log

Enables inbound logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

copy-sflow

For incoming traffic, sends matching packets to the sFlow collector..

Modes

ACL configuration mode

Usage Guidelines

This command configures rules to permit or drop traffic based on source addresses. You can also enable counters and either logging or sFlow collection.

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

An IPv6 ACL can only be applied to incoming traffic.

You can abbreviate an IPv6 address by using one or more of the following rules:

- Remove one or more leading zeros from one or more groups of hexadecimal digits; this is usually done to either all or none of the leading zeros. (For example, convert the group 0042 to 42.)
- Omit consecutive sections of zeros, using a double colon (::) to denote the omitted sections. The double colon may only be used once in any given address, as the address would be indeterminate if the double colon were used multiple times. A double colon may not be used to denote an omitted single section of zeros. (For example, 2001:db8::1:2 is valid, but 2001:db8::1::2 or 2001:db8::1:1:1:1:1:1 are not permitted.)

Although in a standard-ACL rule you can specify both **log** and **copy-sflow**, only one of the two is processed, as follows:

- In a permit rule, only **copy-sflow** is processed.
- In a deny or hard-drop rule, only **log** is processed.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq** *seq-value*.
- If you do not know the rule number, type **no** and then enter the full syntax without *seq-value*.

Filtering fragmented or non-fragmented packets is only supported on ingress ACLs. For IPv6 frames, filtering is only supported if the fragment is the first extension header. Use

protocol number *44* for fragmented extension header. ACL filtering of fragmented and non-fragmented packets is not supported on SLX 9150 and SLX 9250 devices.

Examples

The following example shows how to create an IPv6 standard ACL and define rules for it.

```
device# configure terminal
device(config)# ipv6 access-list standard ipv6-std-acl
device(conf-ip6acl-std)# seq 10 permit host 0:1::1
device(conf-ip6acl-std)# seq 20 deny 0:2::/64
device(conf-ip6acl-std)# seq 30 hard-drop any count
```

The following example creates an IPv6 standard ACL for permitting fragmented packets.

```
device(config)# ipv6 access-list standard ipv6-receive-acl-example
device(conf-ip6acl-std)# seq 10 permit 44 any any count
```

seq (rules in IPv4 standard bACLs)

Inserts filtering rules in IPv4 standard ACLs crafted as IP broadcast ACLs (bACLs).

Syntax

seq *seq-value* { **permit** | **deny** } { *S_IPaddress mask* | **host** *S_IPaddress* | **any** } [**count**] [**fragment** | **non-fragment**]

no seq *seq-value*

{ **permit** | **deny** } { *S_IPaddress mask* | **host** *S_IPaddress* | **any** } [**count**] [**fragment** | **non-fragment**]

no { **permit** | **deny** } { *S_IPaddress mask* | **host** *S_IPaddress* | **any** } [**count**] [**fragment** | **non-fragment**]

Parameters

seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq** *seq-value*, the rule is added at the end of the list.
seq-value

Valid values range from 1 through 65535.

permit

Specifies rules to permit traffic.

deny

Specifies rules to deny traffic.

hard-drop

For bACLs, equivalent to deny.

S_IPaddress

Specifies a source address for which you want to filter the subnet.
mask

Defines a mask, whose effect is to specify a subnet that includes the source address that you specified. For options to specify the mask, see the Usage Guidelines.

host

Specifies a source address.
S_IPaddress

The source address.

any

Specifies all source addresses.

count

Enables statistics for the rule.

log

Not supported for bACLs.

copy-sflow

Not supported for bACLs.

fragment

Filter fragmented packets. This keyword and *non-fragment* keyword cannot be used together.

non-fragment

Filter non-fragmented packets. This keyword and *fragment* keyword cannot be used together.

Modes

ACL configuration mode

Usage Guidelines

This topic describes filtering rules in a standard IPv4 ACL intended for use as an IP broadcast ACL (bACL).

Broadcast ACLs are not supported on SLX 9150 or SLX 9250 devices.

This command configures rules to permit or drop traffic based on source addresses. You can also enable counters.

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

You can specify a mask in either of the following ways:

- Wildcard mask format—for example, 0.0.0.255. The advantage of this format is that it enables you mask any bit, for example by specifying 0.255.0.255.
- Classless Interdomain Routing (CIDR) format—in which you specify the number of bits of the prefix. For example, appending /24 to an IPv4 address is equivalent to specifying 0.0.0.255 as wildcard mask format.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq** *seq-value*.
- If you do not know the rule number, type **no** and then enter the full syntax without **seq** *seq-value*.

Filtering fragmented or non-fragmented packets is only supported on ingress ACLs. On the SLX 9540 and SLX 9640, fragment match is only supported on BGP FS profile. This ACL can also be used with RACL, PBR, and RL. Do not use Layer-4 matching along with fragment matching. Fragmented packets might not have Layer-4 information and most likely cause issues. ACL filtering of fragmented and non-fragmented packets is not supported on SLX 9150 and SLX 9250 devices.

Examples

The following example creates an IPv4 standard bACL, defines rules for it, and applies the bACL to an interface.

```
device# configure
device(config)# ip access-list standard bACL_int_3
device(conf-ipacl-std)# seq 5 permit host 10.20.33.4
device(conf-ipacl-std)# seq 15 deny any
device(conf-ipacl-std)# exit
device(config)# interface ethernet 0/5
device(conf-if-eth-0/5)# ip subnet-broadcast-acl bACL_int_3
```

The following example shows how to create a IPv4 standard bACL, define rules for it, and apply the ACL at device level.

```
device# configure
device(config)# ip access-list standard bACL_glb_9
device(conf-ipacl-std)# seq 5 permit host 10.20.33.4
device(conf-ipacl-std)# seq 15 deny any
device(conf-ipacl-std)# exit
device(config)# ip global-subnet-broadcast-acl bACL_glb_9
```

seq (rules in MAC extended ACLs)

Inserts filtering rules in Layer 2 (MAC) extended access control lists (ACLs).

Syntax

[seq *seq-value* **] permit** { **any** | *SMAC-address mask* | **host** *SMAC-address* } { **any** | **host** *DMAC-address* | *DMAC-address mask* } [**known-unicast-only**] [**vlan** { **any** | *vlanID* }] [*custom-EtherType* | **arp** [**arp-guard**] | **cfm** | **ipv4** | **ipv6** | **mpls**] [**count**] [**log**] [**mirror**] [**copy-sflow**]

[seq *seq-value* **] permit** { **any** | *SMAC-address mask* | **host** *SMAC-address* } { **any** | **host** *DMAC-address* | *DMAC-address mask* } [**known-unicast-only**] [**vlan-tag-format** { **untagged vlan** *vlan-id* | **single-tagged vlan** { **any** | *vlan-id* [*vlan-id-mask*] } | **double-tagged outer-vlan** { **any** | *vlan-id* [*vlan-id-mask*] } **inner-vlan** { **any** | *vlan-id* [*vlan-id-mask*] }] [*custom-EtherType* | **arp** [**arp-guard**] | **cfm** | **ipv4** | **ipv6** | **mpls**] [**count**] [**log**] [**mirror**] [**copy-sflow**]

[seq *seq-value* **]** { **deny** | **hard-drop** } { **any** | *SMAC-address mask* | **host** *SMAC-address* } { **any** | **host** *DMAC-address* | *DMAC-address mask* } [**known-unicast-only**] [**vlan** { **any** | *vlanID* }] [*custom-EtherType* | **arp** [**arp-guard**] | **cfm** | **ipv4** | **ipv6** | **mpls**] [**count**] [**log**] [**mirror**] [**copy-sflow**]

[seq *seq-value* **]** { **deny** | **hard-drop** } { **any** | *SMAC-address mask* | **host** *SMAC-address* } { **any** | **host** *DMAC-address* | *DMAC-address mask* } [**known-unicast-only**] [**vlan-tag-format** { **untagged vlan** *vlan-id* | **single-tagged vlan** { **any** | *vlan-id* [*vlan-id-mask*] } | **double-tagged outer-vlan** { **any** | *vlan-id* [*vlan-id-mask*] } **inner-vlan** { **any** | *vlan-id* [*vlan-id-mask*] }] [*custom-EtherType* | **arp** [**arp-guard**] | **cfm** | **ipv4** | **ipv6** | **mpls**] [**count**] [**log**] [**mirror**] [**copy-sflow**]

no seq *seq-value*

no permit { **any** | *SMAC-address mask* | **host** *SMAC-address* } { **any** | **host** *DMAC-address* | *DMAC-address mask* } [**known-unicast-only**] [**vlan** { **any** | *vlanID* }] [*custom-EtherType* | **arp** [**arp-guard**] | **cfm** | **ipv4** | **ipv6** | **mpls**] [**count**] [**log**] [**mirror**] [**copy-sflow**]

no permit { **any** | *SMAC-address mask* | **host** *SMAC-address* } { **any** | **host** *DMAC-address* | *DMAC-address mask* } [**known-unicast-only**] [**vlan-tag-format** { **untagged vlan** *vlan-id* | **single-tagged vlan** { **any** | *vlan-id* [*vlan-id-mask*] } | **double-tagged outer-vlan** { **any** | *vlan-id* [*vlan-id-mask*] } **inner-vlan** { **any** | *vlan-id* [*vlan-id-mask*] }] [*custom-EtherType* | **arp** [**arp-guard**] | **cfm** | **ipv4** | **ipv6** | **mpls**] [**count**] [**log**] [**mirror**] [**copy-sflow**]

no { **deny** | **hard-drop** } { **any** | *SMAC-address mask* | **host** *SMAC-address* } { **any** | **host** *DMAC-address* | *DMAC-address mask* } [**known-unicast-only**] [**vlan** { **any** | *vlanID* }] [*custom-EtherType* | **arp** [**arp-**

guard] | **cfm** | **ipv4** | **ipv6** | **mpls**] [**count**] [**log**] [**mirror**] [**copy-sflow**]

no { **deny** | **hard-drop** } { **any** | *SMAC-address mask* | **host** *SMAC-address* } { **any** | **host** *DMAC-address* | *DMAC-address mask* } [**known-unicast-only**] [**vlan-tag-format** { **untagged vlan** *vlan-id* | **single-tagged vlan** { **any** | *vlan-id* [*vlan-id-mask*] } | **double-tagged outer-vlan** { **any** | *vlan-id* [*vlan-id-mask*] } **inner-vlan** { **any** | *vlan-id* [*vlan-id-mask*] }] [*custom-EtherType* | **arp** [**arp-guard**] | **cfm** | **ipv4** | **ipv6** | **mpls**] [**count**] [**log**] [**mirror**] [**copy-sflow**]

Parameters

seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq** *seq-value*, the rule is added at the end of the list.
seq-value

Valid values range from 1 through 65535.

permit

Specifies rules to permit traffic.

deny

Specifies rules to deny traffic.

hard-drop

Specifies rules to deny traffic.

any

Specifies any source MAC addresses.

SMAC-address

Specifies a source MAC address and a comparison mask.
mask

Specifies the mask using Fs and zeros. For example, to match on the first two bytes of the address aabb.ccdd.eeff, use the mask ffff.0000.0000. In this case, the clause matches all MAC addresses that contain "aabb" as the first two bytes and any values in the remaining bytes.

host *SMAC-address*

Specifies a source MAC address. Use the format HHHH.HHHH.HHHH.

any

Specifies any destination MAC addresses.

DMAC-address

Specifies a destination MAC address and a comparison mask.
mask

Specifies the mask using Fs and zeros. For example, to match on the first two bytes of the address aabb.ccdd.eeff, use the mask ffff.0000.0000. In this case, the clause matches all MAC addresses that contain "aabb" as the first two bytes and any values in the remaining bytes.

host *DMAC-address*

Specifies a destination MAC address. Use the format HHHH.HHHH.HHHH.

known-unicast-only

(is supported on the Extreme 8720, Extreme 8520, SLX 9250, and SLX 9150 devices only.) Specifies known unicast traffic only.

vlan

Specifies VLANs to which the ACL is bound.

any

Specifies any VLAN.

vlanID

Specifies a VLAN.

vlan-tag-format

Specifies **untagged**, **single-tagged**, or **double-tagged** VLAN traffic.

untagged

Specifies traffic with no VLAN tag.

vlan

Specifies a VLAN or any VLAN.

any

Specifies any VLAN.

vlanID

Specifies a VLAN or range of VLANs.

single-tagged

Specifies traffic with a single VLAN, a range of VLANs, or any VLAN.

vlan

Specifies a VLAN or any VLAN.

any

Specifies any VLAN.

vlanID [*vlan-id-mask*]

Specifies a VLAN or range of VLANs. Optionally, you can use a 12-bit hex value to specify a range of VLANs. For example, 0x0FFF specifies all VLANs for which the last 8 bits are 0.

double-tagged

(is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.) Specifies traffic with both an outer and an inner VLAN, a range of such VLANs, or any such VLAN.

outer-vlan

Specifies an outer VLAN, a range of outer VLANs, or any outer VLAN.

any

Specifies any outer VLAN.

vlanID [*vlan-id-mask*]

Specifies a outer VLAN or range of VLANs. Optionally, you can use a 12-bit hex value to specify a range of VLANs. For example, 0x0FFF specifies all VLANs for which the last 8 bits are 0.

inner-vlan-id

Specifies inner VLANs.

any

Specifies any inner VLAN.

vlanID [vlan-id-mask]

Specifies an inner VLAN or range of VLANs. Optionally, you can use a 12-bit hex value to specify a range of VLANs. For example, 0x0FFF specifies all VLANs for which the last 8 bits are 0.

custom-EtherType

Specifies a custom EtherType value for which to set the permit or deny conditions. Valid values range from 1536 through 65535.

arp

Specifies to permit or deny the ARP protocol (0x0806).

arp-guard

Enables ARP Guard.

cfm

Specifies to permit or deny the CFM protocol (0x8902).

ipv4

Specifies to permit or deny the IPv4 protocol (0x0800).

ipv6

Specifies to permit or deny the IPv6 protocol (0x86dd).

mpls

(is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.) Specifies to permit or deny the MPLS protocol (0x8847).

drop-precedence-force *dp-value*

In **permit** rules applied to incoming traffic, forces drop precedence to a value of 0 through 2. On is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices, the **drop-precedence-force** keyword is supported only under the default, vxlan-ext, and bgp-flowspec TCAM profiles.

count

Enables statistics for the rule.

log

Enables inbound logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

mirror

(Supported for rules in ACLs applied on physical interfaces to inbound traffic) Mirrors packets matching the rule.

copy-sflow

For incoming traffic, sends matching packets to the sFlow collector.

Modes

ACL configuration mode

Usage Guidelines

This command configures rules to permit or drop traffic based on source and destination MAC addresses and protocol type. You can also enable counters, logging, mirroring , and sending packets to the sFlow collector per rule.

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

The behavior of the **hard-drop** keyword varies with platform, as follows:

- (is supported on the Extreme 8720, Extreme 8520, SLX 9250, and SLX 9150 devices only.) Overrides the trap behavior for control frames and data frames such as echo request (ping). However, hard-drop does not override a permit for this address in a preceding rule.
- (is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.) Equivalent to the **deny** keyword.

Although in an extended-ACL rule you can include **log**, **mirror**, and **copy-sflow**, only one of the three is processed, as follows:

- In a permit rule, the order of precedence is **mirror** > **copy-sflow** > **log**.
- In a deny or hard-drop rule, the order of precedence is **log** > **copy-sflow** > **mirror**.

The following guidelines apply to rules that contain one of the **vlan-tag-format** options:

- Supported only when an ACL containing such rules is applied to physical or port-channel interfaces for ingress traffic. Ignored for ACLs applied to egress traffic and for ACLs applied to VLANs.
- (is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.) The **double-tagged** option is supported only for VPLS VLANs. The **untagged** and the **single-tagged** options are supported for all VLANs.
- An implicit LACP BPDU **permit** rule precedes the implicit **deny** rule. But to avoid port-channel interface flap for VPLS endpoints over dynamic LAGs, make sure that the LACP BPDUs do not match any of the configured **deny** rules.

To enable ARP Guard on an interface, you create and apply a MAC extended ACL with rules that contain the **arp** and **arp-guard** keywords. ARP Guard is supported on devices based on the is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq** *seq-value*.
- If you do not know the rule number, type **no** and then enter the full syntax without *seq-value*.

Examples

The following example creates a rule in a MAC extended ACL to deny IPv4 traffic from the source MAC address 0022.3333.4444 to the destination MAC address 0022.3333.5555 and enable packet counting.

```
device# configure terminal
device(config)# mac access-list extended ACL1
device(conf-macl-ext)# seq 100 deny 0022.3333.4444 0022.3333.5555 ipv4 count
```

The following example creates rule in a MAC extended ACL to filter permit traffic by VLAN tag types and enable packet counting.

```
device# configure terminal
device(config)# mac access-list extended ACL1
device(conf-macl-ext)# permit host 0001.0001.0001 any vlan-tag-format untagged vlan 100
count
device(conf-macl-ext)# permit host 0002.0002.0002 any vlan-tag-format single-tagged vlan
200 count
device(conf-macl-ext)# permit host 0003.0003.0003 any vlan-tag-format double-tagged outer-
vlan 300 inner-vlan-id 400 count
device(conf-macl-ext)# permit host 0001.0001.0004 any vlan-tag-format untagged vlan 100
0x0fff count
device(conf-macl-ext)# permit host 0003.0003.0005 any vlan-tag-format double-tagged outer-
vlan 300 0xfff inner-vlan-id 400 0x0fff count
device(conf-macl-ext)# permit host 0003.0003.0006 any vlan-tag-format double-tagged outer-
vlan any inner-vlan-id any count
```

The following example creates an MAC extended ACL with rules that enable ARP Guard and then applies it to the relevant interface.

```
device# configure terminal
device(config)# mac access-list extended arp_guard_enable_1
device(conf-macl-ext)# permit host 0014.2211.1111 any vlan 100 arp arp-guard
device(conf-macl-ext)# permit host 0014.2211.1112 any vlan 101 arp arp-guard
device(conf-macl-ext)# deny any any arp
device(conf-macl-ext)# permit any any
device(conf-macl-ext)# exit

device(conf)# interface ethernet 0/2
device(conf-if-eth-0/2)# switchport
device(conf-if-eth-0/2)# mac access-group arp_guard_enable_1 in
```

The following example deletes a rule from a MAC extended ACL.

```
device# configure terminal
device(config)# mac access-list extended ACL1
device(conf-macl-ext)# no seq 100
```

seq (rules in MAC standard ACLs)

Inserts filtering rules in Layer 2 (MAC) standard ACLs. Standard ACLs permit or deny traffic according to source address only.

Syntax

seq *seq-value* { **deny** | **permit** | **hard-drop** } { **any** | *SMAC_address mask* | **host** *SMAC_address* } [**count**] [**log**] [**copy-sflow**]

no seq *seq-value*

{ **deny** | **permit** | **hard-drop** } { **any** | *SMAC_address mask* | **host** *SMAC_address* } [**count**] [**log**] [**copy-sflow**]

no seq { **deny** | **permit** | **hard-drop** } { **any** | *SMAC_address mask* | **host** *SMAC_address* } [**count**] [**log**] [**copy-sflow**]

Parameters

seq

(Optional) Enables you to assign a sequence number to the rule. If you do not specify **seq** *seq-value*, the rule is added at the end of the list.
seq-value

Valid values range from 1 through 65535.

permit

Specifies rules to permit traffic.

deny

Specifies rules to deny traffic.

hard-drop

Specifies rules to deny traffic.

any

Specifies all source MAC addresses.

SMAC_address

Specifies a source MAC address and a comparison mask.
mask

Specify the mask using F's and zeros. For example, to match on the first two bytes of the address aabb.ccdd.eeff, use the mask ffff.0000.0000. In this case, the clause matches all MAC addresses that contain "aabb" as the first two bytes and any values in the remaining bytes.

host

Specifies a source MAC address.
SMAC_address

Use the format HHHH.HHHH.HHHH.

count

Enables statistics for the rule.

log

Enables inbound logging for the rule. In addition, the ACL log buffer must be enabled, using the **debug access-list-log buffer** command.

copy-sflow

For incoming traffic, sends matching packets to the sFlow collector.

Modes

ACL configuration mode

Usage Guidelines

This command configures rules to permit or drop traffic based on source MAC address.

The order of the rules in an ACL is critical, as the first matching rule stops further processing. When creating rules, specifying sequence values determines the order of rule processing. If you do not specify a sequence value, the rule is added to the end of the list.

The **hard-drop** keyword is equivalent to the **deny** keyword.

Although in a standard-ACL rule you can specify both **log** and **copy-sflow**, only one of the two is processed, as follows:

- In a permit rule, only **copy-sflow** is processed.
- In a deny or hard-drop rule, only **log** is processed.

To delete a rule from an ACL, do the relevant of the following:

- If you know the rule number, enter **no seq** *seq-value*.
- If you do not know the rule number, type **no** and then enter the full syntax, without **seq** *seq-value*.

Examples

The following command creates statistic-enabled rules in a MAC standard ACL.

```
device# configure terminal
device(config)# mac access-list standard ACL1
device(conf-macl-std)# seq 100 deny host 0022.3333.4444 count
device(conf-macl-std)# seq 110 permit host 0011.3333.5555 count
```

The following command deletes a rule in a MAC standard ACL, by specifying the **seq** number.

```
device# configure terminal
device(config)# mac access-list standard ACL1
device(conf-macl-std)# no seq 100
```

service password-encryption

Enables a global password encryption policy that overrides **username** encryption settings.

Syntax

service password-encryption

no service password-encryption

Command Default

Global password encryption policy is enabled.

Modes

Global configuration mode

Usage Guidelines

If global password encryption policy is enabled, it overrides **username** encryption settings.

To disable global password encryption policy, enter the **no** form of this command.

Even if global password encryption policy is disabled, the following **username** syntax does encrypt that user's password: **encryption-level 10**.

Examples

The following example enables global password encryption policy.

```
device# configure terminal
device(config)# service password-encryption
```

The following example disables global password encryption policy.

```
device# configure terminal
device(config)# no service password-encryption
```

service-policy (control plane)

Binds a policy map as a service policy for receive ACL (RACL) IPv4 and IPv6 inbound traffic to the control plane.

Syntax

service-policy in *policy-mapname*

no service-policy in

Command Default

No service policy is created.

Parameters

policy-mapname

Name of the policy map.

Modes

Control-plane configuration mode

Usage Guidelines

The policy map must be configured before you can apply it (refer to the description of the **policy-map** command).

The **no** form of this command removes the service-policy map from the control plane.

Examples

The following example applies a policy map as a service policy to the control plane.

```
device# configure terminal
device(config)# control-plane
device(conf-control-plane)# service-policy in policymap1
```

The following example removes a policy map from the control plane.

```
device# configure terminal
device(config)# control-plane
device(conf-control-plane)# no service-policy in
```

service-policy (interface)

Binds a policy map as a service policy to an interface.

Syntax

service-policy in | **out** *policy-mapname*

no service-policy in | **out**

Command Default

No service policy is created.

Parameters

in

Binds policy map to inbound traffic.

out

Binds policy map to outbound traffic.

policy-mapname

Name of the policy map.

Modes

Interface, Port Channel, and VE subtype configuration mode

Usage Guidelines

This command applies a policy-map containing a class-map with specific Policer parameters and match critters to a device interface. The policy map must be configured before you can apply it (refer to the description of the **policy-map** command).

The **no** form of this command removes the service policy.

Examples

To create a service policy for outbound traffic on a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 2/8
device(conf-if-eth-2/8)# service-policy out policymap1
```

To remove a service policy for outbound traffic from a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 2/8
```

```
device(conf-if-eth-2/8)# no service-policy out
```

To remove a service-policy for inbound traffic on a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 2/8
device(conf-if-eth-2/8)# no service-policy in
```

This example configures IPV4 ACL based **ingress** rate-limiting on a VE interface. The **show** command displays the current configuration for the interface.

```
SLX(config)# int ve 100
SLX(config-if-Ve-100)#
SLX(config-if-Ve-100)# service-policy in policy-map_1
SLX(config-if-Ve-100)#

SLX# show running-config interface Ve 100
interface Ve 100
service-policy in policy-map_1
ip address 10.0.0.2/24
no shutdown
!
SLX#
```

This example configures IPV4 ACL based **egress** rate-limiting on a VE interface. The **show** command displays the current configuration for the interface.

```
SLX(config)# int ve 100
SLX(config-if-Ve-100)#
SLX(config-if-Ve-100)# service-policy out policy-map_1
SLX(config-if-Ve-100)#

SLX# show running-config interface Ve 100
interface Ve 100
service-policy out policy-map_1
ip address 10.0.0.2/24
no shutdown
!
SLX#
```

The following is the configuration for the Policy map used in the above two (2) examples.

```
ip access-list extended ipv4acl
    seq 100 permit ip 10.10.10.10 255.255.255.0 10.10.10.20 255.255.255.0

    class-map class-map_1
        match access-group ipv4acl

    policy-map policy-map_1
        class class-map_1
        Police cir 3000000 eir 300000000
```

session

Configures an LDP session for the neighbor-based filtering of inbound or outbound FECs, You can also configure an authentication key for the LDP session.

Syntax

session *remote-ip-addr* { **filter-fec-in** | **filter-fec-out***prefix-list* } | { **key** *string* }

no session *remote-ip-addr* { **filter-fec-in** | **filter-fec-out** } | { **key** }

Command Default

None

Parameters

remote-ip-addr

Specifies the IP address of the LDP peer.

filter-fec-in

Applies neighbor-based LDP FEC filtering on inbound FECs.

filter-fec-out

Applies neighbor-based LDP FEC filtering on outbound FECs.

prefix-list

Specifies the prefix list for the neighbor to which the filter is applied to allow or prevent the advertisement of FECs.

key *string*

Configures an authentication key on the LDP session. The LDP session can be to an adjacent peer (basic discovery) or to the targeted peer (extended discovery).The string variable specifies a text string of up to 80 characters used for authentication between LDP peers. It must be configured on both peers.

Modes

MPLS LDP configuration mode

Usage Guidelines

Use the **no** form of the command to remove the neighbor-based FEC filtering or authentication key from the LDP session.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures LDP to prevent the advertisement of FEC 10.40.40.0/24 through the list-out prefix list and allow all others FECs to neighbor 10.12.12.12.

```
device# configure terminal
device(config)# ip prefix-list list-out deny 10.40.40.0/24
device(config)# ip prefix-list list-out permit 0.0.0.0/0 ge 32
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# session 10.12.12.12 filter-fec-out list-out
```

set extcommunity

Sets an extended BGP community attribute in a route-map instance.

Syntax

set extcommunity { **rt** *extcommunity value* | **soo** *extcommunity value* }

no set extcommunity

Command Default

No extended BGP community attribute is set.

Parameters

rt

Specifies the route target (RT) extended community attribute.

soo

Specifies the site of origin (SOO) extended community attribute.

extcommunity value

Specifies the value. The value can be one of the following:
ASN:nn—autonomous-system-number:network-number

Autonomous system (AS) number and network number.

IPAddress:nn—ip-address:network-number

IP address and network number.

Modes

Route-map configuration mode.

Usage Guidelines

Enter **no set extcommunity** to delete an extended community set statement from the configuration file.

Examples

The following example sets the route target to extended community attribute 1:1 for routes that are permitted by the route map.

```
device# configure terminal
device(config)# route-map extComRmap permit 10
device(config-route-map-sendExtComRmap/permit/10)# set extcommunity rt 1:1
```

The following example sets the site of origin to extended community attribute 2:2 for routes that are permitted by the route map.

```
device# configure terminal
device(config)# ip community-list extended 1 permit 123:2
device(config)# route-map extComRmap permit 10
device(config-route-map-sendExtComRmap/permit/10)# set extcommunity soo 2:2
```

set interface

Specifies an egress interface for a route-map.

Syntax

set interface { **ethernet** *slot* **/** *port* | **null0** | **port-channel** *number* }

no set interface { **ethernet** *slot* **/** *port* | **null0** | **port-channel** *number* }

Parameters

ethernet *slot* **/** *port*

Specifies an Ethernet interface. If the device does not have linecards, specify `0`.

null0

Specifies the Null0 interface, dropping the packet.

port-channel *number*

Specifies a port-channel interface.

Modes

Route-map configuration mode

Usage Guidelines

The order of the set statements in a route-map is critical: In general, a match followed by a valid **set interface** statement stops further processing. However a **set interface NULL0** statement is always processed last.

The maximum number of **set interface** statements supported in a stanza is 128.

To delete a **set interface** statement from a route map, enter the no form of this command.

set ip dscp

Configures a Differentiated Services Code Point (DSCP) value for a route-map rule.

Syntax

set ip dscp *dscp-value*

no set ip dscp *dscp-value*

Command Default

A DSCP value is not configured.

Parameters

dscp-value

DSCP value. The valid range is from 0 through 63.

Modes

Route-map configuration mode

Usage Guidelines

The **no** form of the command removes the configuration.

Examples

The following example shows how to set a DSCP value of 23 for rule number 4 under a route map named rm.

```
device# configure terminal
device(config)# route-map rm permit 4
device(config-route-map-rm/permit/4)# set ip dscp 23
```

set ip interface null0

Drops traffic when the null 0 statement becomes the active setting as determined by the route-hop selection process for IPv4 policy-based routing.

Syntax

set ip interface null0

no set ip interface null0

Modes

Route-map configuration mode

Usage Guidelines

If none of the configured next-hops or interfaces are up, this command drops the traffic.

The **no** form of this command removes the configuration.

Examples

The following example configures the next hop as NULL0 interface, dropping the packet instead of forwarding it.

```
device(config)# route-map test-route permit 99
device(config-route-map-test-route/permit/99)# set ip interface null0
```

set ip mirror

Configures an IPv4 mirroring destination for a Border Gateway Protocol flow specification (BGP flowspec) route-map rule.

Syntax

set ip mirror *ip-address*

no set ip mirror *ip-address*

Command Default

A mirroring destination is not configured.

Parameters

ip-address

Specifies the mirroring destination in IPv4 address format.

Modes

Route-map configuration mode

Usage Guidelines

To mirror to multiple destinations, you can configure multiple mirror destination addresses.

When mirroring is configured under a BGP flowspec rule, mirror destinations are advertised to BGP neighbors but are not installed in the hardware.

The **no** form of the command removes the configuration.

Examples

The following example shows how to configure two mirroring destination addresses for IPv4 packets for a BGP flowspec sequence number 4 under a route map named rm.

```
device# configure terminal
device(config)# route-map rm permit 4
device(config-route-map-rm/permit/4)# set ip mirror 10.2.3.4
device(config-route-map-rm/permit/4)# set ip mirror 10.6.7.8
```

set ip next-hop

Sets the IPv4 address of the redirect next hop in a route-map instance.

Syntax

set ip next-hop { *ip-address* | **peer-address** }

set ip [**global** | **vrf** *vrf-name*] **next-hop** *ip-address*

no set ip next-hop *ip-address*

Parameters

global

Specifies that the specified next-hop address is to be resolved from the global routing table.

vrf *vrf-name*

Specifies using a VRF routing table to resolve the specified next-hop address.

ip-address

Specifies, in IPv4 address format, the next hop to which to route the packet. The next hop need not be directly connected or reachable.

peer-address

Specifies, when configured, that the next hop is set to the neighbor peering address.

Modes

Route-map configuration mode

Usage Guidelines

The *global* and *vrf* options are not supported for BGP flowspec route maps.

When a route map applies to BGP flowspec, you can redirect traffic to multiple destinations by configuring multiple **set ip next-hop** statements in a single route-map instance. However, when the redirect next-hop holder is NLRI, only the first-configured next-hop IP address is advertised.

When the *peer-address* keyword is used when defining an inbound route map of a BGP peer, then the next hop of the matching route will be set to the neighbor peer address. Similarly, when the *peer-address* keyword is used when defining an outbound route map of a BGP peer, then the next hop of the outbound route map will be configured with the peer address of the local router.

The **no** form of this command removes the configuration.

Examples

The following example configures an IPv4 address as the next hop to which traffic that matches a match statement in the route map must be redirected.

```
SLX(config)# route-map test-route permit 99
SLX(config-route-map-test-route/permit/99)# set ip next-hop 192.168.3.1
```

The following example shows the configuration of the *peer-address* parameter when defining the next hop.

```
SLX (config)# route-map test-route permit 99
SLX (config-route-map-test-route/permit/99)# set ip next-hop peer-address
```

set ipv6 interface null0

Drops traffic when the null 0 statement becomes the active setting as determined by the route-hop selection process for IPv6 policy-based routing.

Syntax

set ipv6 interface null0

no set ipv6 interface null0

Modes

Route-map configuration mode

Usage Guidelines

If none of the configured next-hops or interfaces are up, this command drops the traffic.

The **no** form of this command removes the configuration.

Examples

The following example configures the next hop as NULL0 interface to send the traffic to the null interface, thus dropping the packet instead of forwarding it.:

```
device(config)# route-map test-route permit 99
device(config-route-map-test-route/permit/99)# set ipv6 interface null0
```

set ipv6 next-hop

Sets the IPv6 address of the next hop in a route-map instance.

Syntax

set ipv6 next-hop { *ipv6-address* | **peer-address** }

set ipv6 [**global** | **vrf** *vrf-name*] **next-hop** *ipv6-address*

no set ipv6 next-hop *ipv6-address*

Parameters

ipv6-address

IPv6 address of the next hop.

global

Specifies that the next specified hop address is to be resolved from the global routing table.

vrf *vrf-name*

Specifies from which VRF routing table the specified next hop address will be resolved.

ipv6-address

Specifies, in IPv6 address format, the next hop to which to route the packet. The next hop need not be directly connected or reachable.

peer-address

Specifies, when configured, that the next hop is set to the neighbor peering address.

Modes

Route-map configuration mode

Usage Guidelines

When the *peer-address* keyword is used when defining an inbound route map of a BGP peer, then the next hop of the matching route will be set to the neighbor peer address. Similarly, when the *peer-address* keyword is used when defining an outbound route map of a BGP peer, then the next hop of the outbound route map will be configured with the peer address of the local router.

The **no** form of this command removes the configuration.

Examples

The following example configures IPv6 address as the next hop to which the traffic that matches a match statement in the route map must be routed.

```
device(config)# route-map test-route permit 99
device(config-route-map-test-route/permit/99)# set ipv6 next-hop
2001:db8:0:0:0:ff00:42:8329
```

The following example shows the configuration of the *peer-address* parameter when defining the next hop.

```
SLX (config)# route-map test-route permit 99
SLX (config-route-map-test-route/permit/99)# set ipv6 next-hop peer-address
```

set large-community

Advertises routes with BGP Large Community attributes.

Syntax

set large-community { *ADMIN:OPER1:OPER2* } [**additive**]

no set large-community

Command Default

No large community is set.

Parameters

ADMIN

A four-octet namespace identifier for a BGP Large-Communities Global Administrator.

OPER1

A four-octet operator-defined value for BGP Large-Communities Local Data Part 1.

OPER2

A four-octet operator-defined value for BGP Large-Communities Local Data Part 2.

additive

Appends updates to existing attributes. See the Usage Guidelines.

Modes

Route map configuration mode.

Usage Guidelines

The maximum number of BGP Large Community values that can be configured in a route-map instance (per sequence number) is 32.

By default, this command replaces the BGP Large Community in the routes to which it is applied.

Use the **no** form of this command to remove a large-community list.

Examples

The following example sets a large-community list in a route-map instance.

```
device# configure terminal
device(config)# route-map myroutes permit 10
device(config-route-map-myroutes/permit/10)# set large-community 64497:1:528
```

The following example sets a large-community list in a route-map instance and appends updates to existing attributes.

```
device# configure terminal
device(config)# route-map myroutes permit 10
device(config-route-map-myroutes/permit/10)# set large-community 64497:1:528 additive
```

set large-community-list delete

Deletes BGP Large Community attributes specified in the access list from the route update.

Syntax

set large-community-list *name* **delete**

no set large-community-list *name* **delete**

Command Default

No large community access list is set.

Parameters

name

Name of a large community access list. Range is from 1 through 32 ASCII characters.

Modes

Route-map configuration mode

Usage Guidelines

Use the **no** form of this command to undelete BGP Large Community attributes specified in the access list from the route update.

Examples

The following example sets a community list for deletion in a route-map instance.

```
device# configure terminal
device(config)# route-map myroutes permit 10
device(config-route-map-myroutes/permit/10)# set large-community-list
mylargecommunitylist delete
```

set police cir

Configures a comitted information rate (CIR) value for a Border Gateway Protocol flow specification (BGP flowspec) route-map rule.

Syntax

set police cir *cir-value*

no set police cir

Command Default

A CIR value is not configured.

Parameters

cir-value

CIR value. Valid values are 0 (drop) and from 22000 through 300000000000 bits per second. When the *cir-value* is set to a value in the range from 1 through 21999, matched data traffic is dropped.

Modes

Route-map configuration mode.

Usage Guidelines

The **no** form of the command removes the configuration.

Examples

The following example shows how to set a CIR value to 1000 for BGP flowspec sequence number 4 under a route map named rm.

```
device# configure terminal
device(config)# route-map rm permit 4
device(config-route-map-rm/permit/4)# set police cir 1000
```

set sflow

Enables traffic sampling for a Border Gateway Protocol flow specification (BGP flowspec) route-map rule.

Syntax

set sflow

no set sflow

Command Default

Traffic sampling is disabled.

Modes

Route-map configuration mode.

Usage Guidelines

The **no** form of the command restores the default configuration.

Examples

The following example shows how enable traffic sampling for sequence number 4 under a route map named rm.

```
device# configure terminal
device(config)# route-map rm permit 4
device(config-route-map-rm/permit/4)# set sflow
```

set traffic-action continue

Sets traffic processing to continue (that is, to apply any subsequent traffic-filtering rules) after matching a route-map rule.

Syntax

set traffic-action continue

no set traffic-action continue

Command Default

By default, traffic evaluation stops after matching a rule.

Modes

Route-map configuration mode

Usage Guidelines

The **set traffic-action continue** command sets the traffic action to continue to evaluate traffic against subsequent filtering rules as defined by the ordering procedure. When **set traffic-action continue** is not configured, traffic evaluation stops after matching a rule.

The **no** form of the command restores the default configuration; that is, traffic evaluation stops after matching a rule.

Examples

The following example shows how to set the traffic action to **continue** for sequence number 4 in a route map named rm.

```
device# configure terminal
device(config)# route-map rm permit 4
device(config-route-map-rm/permit/4)# set traffic-action continue
```

set-debug

Enables debug configurations for Intermediate System-to-Intermediate System (IS-IS).

Syntax

set-debug nsr

no set-debug nsr

Command Default

Disabled.

Parameters

nsr

Specifies nonstop routing (NSR) debugs.

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example enables NSR debug configurations for IS-IS.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# set-debug nsr
```

The following example disables NSR debug configurations for IS-IS.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no set-debug nsr
```

set-overload-bit

Configures a device to signal other devices not to use it as an intermediate hop in their shortest path first (SPF) calculations if the resources of the intermediate system are overloaded and preventing the IS from properly performing Intermediate System-to-Intermediate System (IS-IS) routing.

Syntax

set-overload-bit

set-overload-bit on-startup *value*

set-overload-bit on-startup wait-for-bgp [*max-bgp-wait-time*]

no set-overload-bit

no set-overload-bit on-startup *interval*

no set-overload-bit on-startup wait-for-bgp [*max-bgp-wait-time*]

Command Default

A device automatically sets the overload on in its Link State PDUs (LSPs) to other intermediate systems if an overload condition occurs.

Parameters

on-startup

Sets the overload bit when the system starts up. The overload bit remains set for the number of seconds configured or until Border Gateway Protocol (BGP) has converged, depending on the subsequent argument or keyword specified.

interval

Specifies the number of seconds the overload bit remains set when the system starts up. Valid values range from 5 through 86400 seconds (24 hours).

wait-for-bgp

Specifies that the overload bit is set when the system starts up and remains set until BGP has converged.

max-bgp-wait-time

Specifies the maximum time in seconds that IS-IS waits for BGP convergence to complete. When the configured time interval is exceeded without BGP convergence, IS-IS exits the overload state. Valid values range from 5 seconds through 86400 seconds (24 hours). The default is 600 seconds (10 minutes).

Modes

IS-IS router configuration mode

Usage Guidelines

The **no** form of the command removes the configured overload state.

Examples

The following example sets the overload bit to on with immediate effect.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# set-overload-bit
```

The following example configures the device to set the overload bit on in all its IS-IS LSPs sent to other ISs during the first five seconds following a successful software reload. After the five seconds expire, the device resets the overload bit to off in all its IS-IS LSPs.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# set-overload-bit on-startup 60
```

The following example specifies that the overload bit is set upon system startup and remains set until BGP has converged and specifies that the device that 86400 seconds is the maximum time that IS-IS will wait for BGP convergence to complete.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# set-overload-bit on-startup wait-for-bgp 86400
```

sflow agent-address

Configures the sFlow agent-ID address.

Syntax

sflow agent-address { **ipv4** | **ipv6** [**ethernet** *slot/plot* | **loopback** *loopback-number* | **management** *mgmt-id* | **ve** *ve-inteface*] }

no sflow agent-address

Command Default

By default the sflow agent address is not configured.

Parameters

ipv4

Specifies an agent-address configuration for IPv4 collectors.

ipv6

Specifies an agent-address configuration for IPv6 collectors.

ethernet *slot/plot*

Specifies an Ethernet slot and port. The only supported slot value on the fixed form factor SLX devices is 0.

loopback *loopback-number*

Specifies a loopback interface. Valid values range from 1 through 255.

management *mgmt-id*

Specifies the management interface. The only supported value is **0**.

ve *ve-inteface*

Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to remove the sFlow agent address configuration.

Examples

The following example configures the sFlow agent-address globally. That is, it applies to all IPv4 collectors.

```
device# configure terminal
device(config)# sflow agent-address ipv4 ethernet 0/5
```

sflow collector

Configures the forwarding of sFLow datagrams to collectors.

Syntax

sflow collector { *IPv4address* | *IPv6address* } [**use-vrf** *vrf-name*]

no sflow collector { *IPv4address* | *IPv6address* } [**use-vrf** *vrf-name*]

Parameters

IPv4address

Specifies an IPv4 address in dotted-decimal format for the collector.

IPv6address

Specifies an IPv6 address for the collector.

use-vrf *vrf-name*

Specifies a VRF through which to connect to the collector. See the Usage Guidelines.

Modes

Global configuration mode

Usage Guidelines

You can only specify up to five sFlow collectors; this includes all VRFs.

Use the no form of this command to reset the specified collector address to a null value.

By default, all management services are enabled on the management VRF ("mgmt-vrf") and the default VRF ("default-vrf").

Examples

To specify the sFlow collectors for an IPv4 address with the default port on the management VRF:

```
device# configure terminal
device(config)# sflow collector 192.10.138.176
```

To specify the sFlow collectors for an IPv4 address with a nondefault port on a user-specified VRF:

```
device# configure terminal
device(config)# sflow collector 192.10.138.176 50 use-vrf myvrf
```

To specify the sFlow collectors for an IPv6 address with a nondefault port on the management VRF:

```
device# configure terminal
device(config)# sflow collector 3ff3:1900:4545:3:200:f8ff:fe21:67cf:6343 50
```

sflow enable

Enables sFlow. sFlow can be configured globally or on an interface.

Syntax

sflow enable

no sflow enable

Command Default

sFlow is disabled on the system.

Modes

Global Configuration Mode, Interface Mode

Usage Guidelines

The **no** form of this command disables sFlow. When this command is run on an interface, it disables sFlow on that interface.

Examples

The following example configures sFlow globally.

```
SLX# configure terminal
SLX (config)# sflow enable

2023/01/10-05:58:04.702198 , [SFLO-1001], 5826, DCE, INFO, GESpine2, sFlow is enabled
globally.

SLX (config)#
```

The following example configures sFlow on an interface.

```
SLX# configure terminal
SLX (config)# interface ethernet 0/25:2
SLX (conf-if-eth-0/25:2)# sflow enable

2023/01/10-07:08:03.093271 , [SFLO-1002], 5830, DCE, INFO, GESpine2, sFlow is enabled
     for interface Ethernet 0/25:2.

SLX (conf-if-eth-0/25:2)#
```

sflow polling-interval (global version)

Configures the polling interval globally.

Syntax

sflow polling-interval *interval_value*

no sflow polling-interval

Parameters

interval_value

Specifies a value in seconds to set the polling interval. Valid values range from 1 through 65535 seconds.

Command Default

The default is 20.

Modes

Global configuration mode

Usage Guidelines

The interval is the maximum number of seconds between successive samples of counters to be sent to the collector.

The **no** form of this command restores the default value.

Examples

To set the polling interval to 135 seconds:

```
device# configure terminal
device(config)# sflow polling-interval 135
```

sflow sample-rate

For sFlow, sets the number of packets that are skipped before the next sample is taken.

Syntax

sflow sample-rate *samplerate*

no sflow sample-rate

Command Default

The default value is 2048 packets for all platforms.

Parameters

samplerate

Specifies the sampling rate value in number of packets. Valid value are

- 1 - 16000000 - for SLX 9740 and Extreme 8820
- 1 - 100000 - for all other platforms

Modes

Global Configuration Mode, Interface Mode

Usage Guidelines

Sample-rate is the average number of packets skipped before the next sample is taken.

The **no** form of this command restores the default sampling rate.

Note

For the SLX 9740 and Extreme 8820 devices, the configurable sample rate value is 1-16000000.

For all other platforms, the configurable sample rate value is 1-100000.

Examples

This example shows how to change the sampling rate to 4096:

```
SLX# configure terminal
SLX (config) # sflow sample-rate 4096
SLX (config)#
```

This example shows how to configure sampling rate to 4096 on to an specific ethernet interface.

```
SLX# configure terminal
SLX (config) #
SLX (config)# interface ethernet 0/25:2
```

```
SLX (conf-if-eth-0/25:2)# sflow sample-rate 4096
SLX (conf-if-eth-0/25:2)#
```

sflow update-destination-mac

Updates the destination MAC address in the sFlow samples collected for analysis. This information can then be used for making peering decisions and correcting peering decisions.

Syntax

sflow update-destination-mac

no sflow update-destination-mac

Command Default

Update destination MAC is disabled by default.

Modes

Global Configuration Mode

Usage Guidelines

This feature is supported in all devices. It is also supported on all VRFs (default, management, and user vrf).

Updating destination MAC is only applicable for *Routed* packets.

sFlow must be enabled globally and at specific interface level before this command is executed.

The **no** form of this command disables updating the destination MAC address in sFlow samples for routed packets.

Examples

The following example enables sFlow Update Destination MAC globally.

```
SLX# configure terminal
SLX (config)# sflow update-destination-mac

2023/12/19-10:05:26.557334 , [SFLO-1021], 39217, DCE, INFO, DUT-3, Updating of
destination MAC in
    sFlow samples for routed packets is enabled globally.

SLX (config)#
```

The following example disables sFlow Update Destination MAC globally.

```
SLX# configure terminal
SLX (config)# no sflow update-destination-mac

2023/12/19-10:05:07.225059 , [SFLO-1022], 39216, DCE, INFO, DUT-3, Updating of
destination MAC in sFlow samples for routed packets is disabled globally.
```

```
SLX (config)#
```

sflow update-dst-mac(global version)

When enabled, the destination MAC address in *sFlow* sample is updated with the MAC address of the next hop through which the destination IP address is reachable.

Syntax

sflow update-dst-mac

no sflow update-dst-mac

Command Default

sFlow is disabled on the system.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command disables updating the destination MAC in sFlow sample for routed packets.

The **show running-config sflow** command will display the feature if enabled.

Examples

To enable updating the MAC address of the next hop in the destination MAC of the sFlow sample.

```
device#
device# sflow update-dst-mac
```

To disable updating the MAC address of the next hop in the destination MAC of the sFlow sample.

```
device#
device# no sflow update-dst-mac
```

sflow source-interface

Specifies to pick the IPv4 or IPv6 address of either the Ethernet, Virtual Ethernet (ve), management, or loopback interface as the source of sFlow packets.

Syntax

sflow source-interface { **ethernet** *slot/port* | **loopback** *loopback_num* | **management** *mgmt-id* | **ve** *ve_interface* }

no sflow source-interface

Command Default

By default, sFlow uses the management port IP address as the source IP.

Parameters

ethernet *slot/port*

Specifies an Ethernet slot and port. The only supported slot value on the fixed form factor SLX devices is **0**.

loopback *loopback_num*

Specifies a loopback interface. Valid values range from 1 through 255.

management *mgmt-id*

Specifies the management interface. The only supported value is 0.

ve *ve-interface-number*

Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command is available after the source type has been specified.

- The sFlow source IP (source interface) configurations are not applicable to sFlow collectors that are reachable through the management port unless the specified source interface falls in the management VRF.
- The **show sflow** command displays the source interface field only when it is configured.

Examples

To specify the Ethernet address as the source of sFlow packets:

```
device# config
device(config)# sflow source-interface ethernet 0/1
```

To specify the loopback interface as the source of sFlow packets:

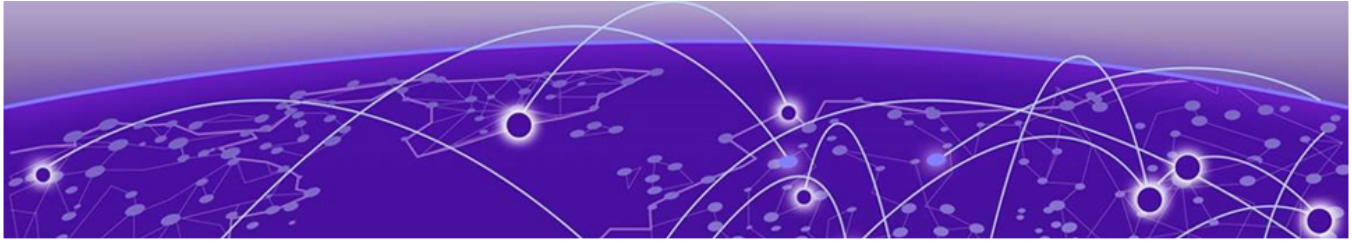
```
device(config)# sflow source-interface loopback 42
```

To confirm the above configuration:

```
device(config)# do show running-config sflow
sflow enable
sflow source-interface loopback 42
```

To disable the above configuration and revert to the default:

```
device(config)# no sflow source-interface
device(config)# do show running-config sflow
sflow enable
```



Show A through Show I

show access-list on page 1671
show access-list overlay transit on page 1675
show access-list overlay type vxlan acl-name on page 1676
show access-list-log buffer on page 1677
show access-list-log buffer config on page 1679
show arp on page 1680
show arp access-list on page 1683
show bfd on page 1684
show bfd neighbors on page 1686
show bfd neighbors application on page 1688
show bfd neighbors dest-ip on page 1690
show bfd neighbors details on page 1692
show bfd neighbors interface on page 1695
show bgp evpn ethernet-segment on page 1697
show bgp evpn evid on page 1698
show bgp evpn vni on page 1699
show bgp evpn interface tunnel on page 1700
show bgp evpn l2route on page 1702
show bgp evpn l2route next-hop on page 1705
show bgp evpn l2route unreachable on page 1706
show bgp evpn l3vni on page 1707
show bgp evpn neighbors on page 1710
show bgp evpn neighbors advertised-routes on page 1712
show bgp evpn neighbors routes on page 1714
show bgp evpn routes on page 1716
show bgp evpn routes best on page 1717
show bgp evpn routes detail on page 1719
show bgp evpn routes local on page 1720
show bgp evpn routes next-hop on page 1723
show bgp evpn routes no-best on page 1725
show bgp evpn routes not-installed-best on page 1727
show bgp evpn routes rd on page 1729
show bgp evpn routes rd type on page 1730
show bgp evpn routes type on page 1733

show bgp evpn routes type igmp-join-sync on page 1741
show bgp evpn routes type igmp-leave-sync on page 1742
show bgp evpn routes unreachable on page 1743
show bgp evpn summary on page 1744
show bgp ip flowspec on page 1745
show bgp ip flowspec neighbors on page 1747
show bgp ip neighbor ipv6 on page 1749
show bgp ip summary ipv6 on page 1752
show ip/ipv6 bgp peer-dampened on page 1753
show bmc config-history on page 1755
show bmc interface management status on page 1757
show bmc interface management ip on page 1758
show bmc password-status on page 1759
show bmc status on page 1760
show bridge-domain on page 1762
show capabilities on page 1768
show cee maps default on page 1769
show cert-util sshkey on page 1770
show cfm on page 1771
show cfm y1731 action-profile on page 1773
show cfm y1731 client-signal-fail on page 1774
show cfm y1731 delay-measurement on page 1775
show cfm y1731 synthetic-loss-measurement on page 1777
show cfm y1731 test-profile on page 1779
show chassis on page 1780
show cipherset on page 1782
show cli on page 1783
show clock on page 1784
show cluster on page 1785
show cluster track on page 1790
show config-drift-track on page 1791
show copy-support status on page 1792
show core-isolation track on page 1793
show crypto ca on page 1794
show crypto key on page 1795
show debug all on page 1796
show debug arp packet on page 1797
show debug dhcp packet on page 1799
show debug dhcp packet buffer on page 1800
show debug ip bgp all on page 1802
show debug ip igmp on page 1803
show debug ip ospf internal lsp-shortcuts on page 1804

show debug ip ospf all on page 1805
show debug ipv6 pim on page 1806
show debug lacp on page 1807
show debug lldp on page 1808
show debug spanning-tree on page 1809
show debug vrrp on page 1810
show defaults threshold on page 1811
show dot1x on page 1814
show environment fan on page 1817
show environment history on page 1818
show environment power on page 1820
show environment sensor on page 1824
show environment temp on page 1825
show erp on page 1828
show erp statistics on page 1829
show event-handler activations on page 1830
show file on page 1831
show firmware peripheral cpld on page 1833
show firmware peripheral fpga on page 1835
show firmwaredownloadhistory on page 1836
show firmwaredownloadstatus on page 1837
show grubversion on page 1839
show hardware media-database on page 1840
show hardware profile on page 1842
show hardware smt on page 1850
show history on page 1851
show http server status on page 1852
show hw route-info on page 1853
show interface on page 1855
show interface stats brief on page 1860
show interface stats detail on page 1862
show interface stats utilization-watermark on page 1865
show interface status on page 1868
show inventory on page 1869
show ip arp inspection on page 1870
show ip arp inspection interfaces on page 1872
show ip arp suppression-cache on page 1874
show ip arp suppression-statistics on page 1875
show ip arp suppression-status on page 1877
show ip bgp on page 1879
show ip bgp attribute-entries on page 1880
show ip bgp dampened-paths on page 1881

show ip bgp filtered-routes on page 1882
show ip bgp flap-statistics on page 1883
show ip bgp neighbors on page 1885
show ip bgp neighbors advertised-routes on page 1888
show ip bgp neighbors flap-statistics on page 1889
show ip bgp neighbors last-packet-with-error on page 1890
show ip bgp neighbors received on page 1892
show ip bgp neighbors received-routes on page 1893
show ip bgp neighbors rib-out-routes on page 1894
show ip bgp neighbors routes on page 1895
show ip bgp neighbors routes-summary on page 1897
show ip bgp peer-group on page 1898
show ip bgp routes on page 1899
show ip bgp routes community on page 1902
show ip bgp routes large-community on page 1903
show ip bgp routes large-community access-list on page 1905
show ip bgp routes large-community reg-expression on page 1906
show ip bgp rpki details on page 1907
show ip bgp rpki server summary on page 1908
show ip bgp rpki table on page 1909
show ip bgp summary on page 1910
show ip bgp vpnv4 routes large-community on page 1912
show ip bgp vpnv4 routes large-community access-list on page 1913
show ip bgp vpnv4 routes large-community reg-expression on page 1914
show ip bgp vpnv6 routes large-community on page 1915
show ip bgp vpnv6 routes large-community access-list on page 1916
show ip bgp vpn6 routes large-community reg-expression on page 1917
show ip dhcp relay address on page 1918
show ip dhcp relay gateway on page 1920
show ip dhcp relay statistics on page 1921
show ip dhcp snooping on page 1922
show ip flowspec rules on page 1924
show ip igmp groups on page 1928
show ip igmp interface on page 1929
show ip igmp snooping on page 1930
show ip igmp ssm-map on page 1932
show ip igmp statistics bridge-domain on page 1933
show ip igmp statistics interface on page 1934
show ip igmp statistics vlan on page 1935
show ip interface on page 1936
show ip multicast snooping on page 1939
show ip ospf on page 1940

show ip ospf area on page 1941
show ip ospf border-routers on page 1943
show ip ospf config on page 1944
show ip ospf database on page 1945
show ip ospf filtered-lsa area on page 1948
show ip ospf interface on page 1949
show ip ospf lsp-shortcuts on page 1951
show ip ospf neighbor on page 1952
show ip ospf redistribute route on page 1953
show ip ospf routes on page 1954
show ip ospf summary on page 1956
show ip ospf traffic on page 1958
show ip ospf virtual link on page 1959
show ip ospf virtual neighbor on page 1960
show ip pim bsr on page 1961
show ip pim interface on page 1964
show ip pim mcache on page 1965
show ip pim mdt on page 1966
show ip pim neighbor on page 1969
show ip pim rp-candidate on page 1971
show ip pim rp-hash on page 1973
show ip pim rp-map on page 1974
show ip pim rp-set on page 1975
show ip pim rpf on page 1977
show ip pim traffic on page 1978
show ip route on page 1981
show ip source guard binding entries on page 1985
show ip subnet-rate-limit stats on page 1986
show ipv6 bgp on page 1987
show ipv6 bgp attribute-entries on page 1988
show ipv6 bgp dampened-paths on page 1989
show ipv6 bgp filtered-routes on page 1990
show ipv6 bgp flap-statistics on page 1991
show ipv6 bgp neighbors on page 1993
show ipv6 bgp neighbors advertised-routes on page 1995
show ipv6 bgp neighbors flap-statistics on page 1997
show ipv6 bgp neighbors last-packet-with-error on page 1998
show ipv6 bgp neighbors received on page 2000
show ipv6 bgp neighbors received-routes on page 2001
show ipv6 bgp neighbors rib-out-routes on page 2002
show ipv6 bgp neighbors routes on page 2004
show ipv6 bgp neighbors routes-summary on page 2006

show ipv6 bgp peer-group on page 2010
show ipv6 bgp routes on page 2011
show ipv6 bgp routes community on page 2014
show ipv6 bgp routes large-community on page 2015
show ipv6 bgp routes large-community access-list on page 2016
show ipv6 bgp routes large-community reg-expression on page 2017
show ipv6 bgp summary on page 2018
show ipv6 counters interface on page 2020
show ipv6 dhcp relay address interface on page 2021
show ipv6 dhcp relay delegated-prefixes on page 2022
show ipv6 dhcp relay prefix-delegation-information on page 2024
show ipv6 dhcp relay statistics on page 2025
show ipv6 interface on page 2027
show ipv6 mld groups on page 2029
show ipv6 mld snooping on page 2031
show ipv6 mld snooping mrouter on page 2032
show ipv6 mld statistics on page 2033
show ipv6 multicast snooping on page 2035
show ipv6 multicast snooping mcache on page 2036
show ipv6 nd on page 2037
show ipv6 nd suppression-cache on page 2039
show ipv6 nd suppression-statistics on page 2041
show ipv6 nd suppression-status on page 2042
show ipv6 neighbor on page 2044
show ipv6 ospf on page 2047
show ipv6 ospf area on page 2048
show ipv6 ospf database on page 2049
show ipv6 ospf interface on page 2052
show ipv6 ospf memory on page 2053
show ipv6 ospf neighbor on page 2055
show ipv6 ospf redistribute route on page 2057
show ipv6 ospf routes on page 2058
show ipv6 ospf spf on page 2059
show ipv6 ospf summary on page 2060
show ipv6 ospf virtual-links on page 2062
show ipv6 ospf virtual-neighbor on page 2063
show ipv6 pim anycast-rp on page 2064
show ipv6 pim bsr on page 2065
show ipv6 pim group on page 2066
show ipv6 pim interface on page 2067
show ipv6 pim mcache on page 2069
show ipv6 pim neighbor on page 2070

show ipv6 pim rp-candidate on page 2072
show ipv6 pim rp-hash on page 2073
show ipv6 pim rp-map on page 2074
show ipv6 pim rp-set on page 2075
show ipv6 pim rpf on page 2076
show ipv6 pim settings on page 2077
show ipv6 pim traffic on page 2078
show ipv6 prefix-list on page 2079
show ipv6 route on page 2080
show ipv6 static route on page 2082
show ipv6 vrrp on page 2083
show isis on page 2088
show isis config on page 2093
show isis counts on page 2094
show isis database on page 2098
show isis hostname on page 2102
show isis interface on page 2103
show isis neighbors on page 2109
show isis routes on page 2113
show isis spf-log on page 2115
show isis traffic on page 2119
show selinux status on page 2120
show system internal bgp evpn nhid on page 2122
show mac-address-table on page 2123
show ip arp suppression-cache on page 2124

show access-list

Displays ACL information for an ACL type and inbound and outbound directions. You can show information for a specific ACL or only for that ACL on a specific interface. You can also display information for all ACLs bound to an interface.

Syntax

show access-list { **ip** | **ipv6** | **mac** }

show access-list { **ip** | **ipv6** | **mac** } *acl-name* { **in** | **out** }

show access-list interface { **ethernet** *slot* **/** *port* | **port-channel** *index* | **ve** *vlan_id* | **vlan** *vlan_id* } { **in** | **out** }

show access-list interface management *mgmt-id* **in**

show access-list mac *acl-name* **interface** { **ethernet** *slot* **/** *port* | **port-channel** *index* | **vlan** *vlan_id* } { **in** | **out** }

show access-list { **ip** | **ipv6** } *acl-name* **interface** { **ethernet** *slot* **/** *port* | **port-channel** *index* | **ve** *vlan_id* } { **in** | **out** }

show access-list { **ip** | **ipv6** } *acl-name* **interface management** *mgmt-id* **in**

show access-list global-subnet-broadcast ip *acl-name*

show access-list subnet-broadcast ip [*acl-name*[**interface** { **ethernet** *slot* **/** *port* | **ve** *vlan-id* }]]

show access-list receive { **ip** | **ipv6** } *acl-name*

Parameters

ip

Specifies the IPv4 Layer 3 network protocol.

ipv6

Specifies the IPv6 Layer 3 network protocol.

mac

Specifies the medium access control (MAC) Layer 2 network protocol.

in

Specifies the incoming binding direction.

out

Specifies the outgoing binding direction.

acl-name

Specifies the ACL name.

interface

Filters by interface.

ethernet

Specifies a physical Ethernet interface.

slot

Specifies a valid slot number. For devices that do not support line cards, specify **0**.

port

Specifies a valid port number.

port-channel *index*

Specifies a port-channel interface.

ve *vlan_id*

Specifies a virtual Ethernet (VE) interface.

vlan *vlan_id*

Specifies a VLAN interface.

management *mgmt-id*

Specifies the management interface. The only supported value is 0.

global-subnet-broadcast ip

Specifies an IP broadcast ACL (bACL) applied at the device level.

subnet-broadcast ip

Specifies an IP broadcast ACL (bACL) applied at the physical-interface or VE level.

receive

Specifies an ACL that applies to device receive-path traffic.

Modes

Privileged EXEC mode

Usage Guidelines

You can show information for a specified ACL or only for that ACL on a specified interface. You can also display information for all ACLs bound to a specified physical interface, port-channel, VLAN or VE.

The command also displays information for receive-path ACLs.

Output

The **show access-list** command displays the following information:

Output field	Description
Active	The rule is active and implements the configured action.
Partial	The rule is partially programmed, with the configured action implemented in some cases. This is typically seen for logical interfaces like VLAN, which span multiple hardware resources.

Output field	Description
In progress	The rule is currently being programmed into the hardware.
Inactive	The rule is inactive and is not programmed in the hardware. This is typically seen when the hardware resources limit is reached.

Examples

The following example displays the names of IPv4 ACLs applied to the device, interfaces to which they are applied, and the incoming/outgoing direction.

```
device# show access-list ip
Interface Ve 171
   Inbound access-list is not set
   Outbound access-list is IPV4_ACL_000 (From User)
Interface Ethernet 1/2
   Inbound switched access-list is IP_ACL_STD_EXAMPLE (From User)
   Outbound access-list is IP_ACL_EXT_EXAMPLE (From User)
```

The following example displays all interfaces on which an IPv4 ACL is applied in the outgoing direction.

```
device# show access-list ip IPV4_ACL_000 out
ip access-list IPV4_ACL_000 on Ve 171 at Egress (From User)
    seq 10 deny ip host 0.0.0.0 host 10.0.0.0 (Active)
```

The following example displays all interfaces on which an IPv6 ACL is applied in the incoming direction.

```
device# show access-list ipv6 distList in
ipv6 access-list distList on Ethernet 1/4 at Ingress (From User)
    seq 10 deny 2001:125:132:35::/64 (Active)
    seq 20 deny 2001:54:131::/64 (Active)
    seq 30 deny 2001:5409:2004::/64 (Active)
    seq 40 permit any (Active)
```

The following example displays all ACLs applied on a specified interface in the incoming direction.

```
device# show access-list interface ethernet 1/4 in
ipv6 access-list ipv6-std-acl on Ethernet 1/4 at Ingress (From User)
    seq 10 permit host 0:1::1 (Active)
    seq 20 deny 0:2::/64 (Active)
    seq 30 hard-drop any count (Active)
```

The following example displays IPv6 receive-path ACL information.

```
device# show access-list receive ipv6 ipv6_1
ip access-list extended ipv6_1
    seq 10 permit ipv6 any any count (Active)
```

This example displays permit and deny rules configured for control plane protection.

```
device# show access-list receive ip ip-ssh
ip access-list extended ip-ssh
    seq 5 deny tcp any 14.14.14.14 0.0.0.0 eq 22 count (Active)
    seq 10 permit tcp 10.10.10.10 0.0.0.255 any eq 22 count (Active)
    seq 20 permit tcp 11.11.11.11 0.0.0.255 any eq 22 count (Active)
    seq 100 deny tcp any any eq 22 count (Active)
```

The following example displays an ACL definition that supports filtering non-fragmented packets.

```
device# show access-list interface ethernet 0/7 in
ip access-list new_acl on Ethernet 0/7 at Ingress (From User)
    seq 10 permit ip any any non-fragment count (Active)
```

The following example displays an ACL definition that supports filtering fragmented packets.

```
device# show access-list int eth 0/8 in
ip access-list test on Ethernet 0/8 at Ingress (From User)
seq 10 permit ip any any fragment (Active)
```

The following example displays an ACL definition that supports flow based ingress miroring.

```
device# show access-list int eth 0/2 in
ip access-list mac1 on Ethernet 0/2 at Ingress (From User)
    seq 10 permit any host 1111.2222.3333 count mirror (Active)
    seq 20 permit host 4444.5555.6666 any count (Active)
```

The following example displays an ACL definition that supports flow based egress miroring.

```
device# show access-list int eth 0/1 out
ip access-list mac1 on Ethernet 0/1 at Egress (From User)
    seq 10 permit any host 1111.2222.3333 count mirror (Active)
    seq 20 permit host 4444.5555.6666 any count (Active)
```

show access-list overlay transit

Displays which overlay ACL is applied to a specific overlay transit.

Syntax

show access-list overlay transit *overlay-transit-name*

Parameters

overlay-transit-name

Specifies the name of the overlay transit.

Modes

Privileged EXEC mode

Usage Guidelines

Overlay ACLs are not supported on SLX 9150 or SLX 9250 devices.

Examples

```
device# show access-list overlay transit tr_name
Overlay Transit Global Binding
  Inbound access-list is abc_ext (From User)
  Outbound access-list is not set
```

show access-list overlay type vxlan acl-name

Displays the rules defined in a specific overlay VXLAN ACL and any overlay transit to which it is applied.

Syntax

show access-list overlay type vxlan acl-name *acl-name*

Parameters

acl-name

Specifies an overlay VXLAN ACL name.

Modes

Privileged EXEC mode

Usage Guidelines

Overlay ACLs are not supported on SLX 9150 or SLX 9250 devices.

Examples

The following example is an overlay VXLAN ACL applied to an overlay transit.

```
device# show access-list overlay type vxlan acl-name abc_ext
Number of Rules: 4
seq 1000 permit  dst-vtep-ip-host 200.1.1.1 src-vtep-ip-host 150.1.1.1 vni 1 vni-mask 0
redirect Ethernet 2/65 sflow count 44024774(pkts)/52829728800(bytes)
seq 1010 permit  dst-vtep-ip-host 200.1.1.2 src-vtep-ip-host 150.1.1.2 vni 2 vni-mask 0
redirect Ethernet 2/19 sflow count 44024773(pkts)/52829727600(bytes)
seq 1020 permit  dst-vtep-ip-host 200.1.1.3 src-vtep-ip-host 150.1.1.3 vni 3 vni-mask 0
redirect Ethernet 2/43 sflow count 0(pkts)/0(bytes)
seq 1030 permit  dst-vtep-ip-host 200.1.1.4 src-vtep-ip-host 150.1.1.4 vni 4 vni-mask 0
redirect Ethernet 2/67 sflow count 0(pkts)/0(bytes)
Transit : transit_name
```

show access-list-log buffer

Displays the contents of the log buffer for all ACLs, or for a specified interface.

Syntax

show access-list-log buffer [**interface** { **ethernet** *slot* **/** *port* | **port-channel** *index* }]

Parameters

interface

Filters by interface.

ethernet

Specifies a physical Ethernet interface.

slot

Specifies a valid slot number. For devices that do not support line cards, specify **0**.

port

Specifies a valid port number.

port-channel *index*

Specifies a port-channel interface.

Modes

Privileged EXEC mode

Output

The **show access-list log buffer** command displays the following information:

Output field	Description
Frames Logged on interface	Accumulated number of packets matching ACL rules applied to the interface
Ethernet Src, Dst; Internet proto, Src, Dst	Information for matched buffered packets for the specified source and destination addresses

Examples

Sample terminal output:

```
device# show access-list-log buffer
Frames Logged on interface 0/2 :
--------------------------------
Frame Received Time : Fri Dec 9 3:8:48 2011
Ethernet,       Src : (00:34:56:78:0a:ab), Dst: (00:12:ab:54:67:da)
  Ethtype           : 0x8100
  Vlan tag type     : 0x800
```

```
  VlanID              : 0x1
Internet proto, Src : 192.85.1.2, Dst: 192.0.0.1
  Interface           :
  Type of service     : 0
  Length              : 110
  Identification      : 0
  Fragmentation       : 00 00
  TTL                 : 255
  protocol            : 253
  Checksum            : 39 3a
  Payload type        :
packet(s) repeated  : 30
Ingress Deny Logged
-------------------------------------------------------------------------
```

show access-list-log buffer config

Displays the configuration of the ACL buffer.

Syntax

show access-list-log buffer config

Modes

Privileged EXEC mode

Output

The **show access-list log buffer config** command displays the following information:

Output field	Description
ACL Logging is	Displays "enabled" or "disabled".
Buffer exists	Displays interfaces buffered.
Buffer type is	Displays "circular" or "linear".

Examples

The following example displays the configuration of the ACL buffer.

```
device# show access-list-log buffer config
ACL Logging is enabled
Buffer exists for interface Eth 2/11
Buffer type is Circular and size is 1000
```

show arp

Displays the Address Resolution Protocol (ARP) entries.

Syntax

show arp { **ethernet** *slot* **/** *port* | **ve** *ve-id* } [**vrf** *name*]

show arp ip *ip-address* [**vrf** *name*]

show arp [**dynamic** | **static**] [**summary**] [**vrf** *name*]

Parameters

ethernet

Specifies a physical Ethernet interface.

slot

Specifies a valid slot number. For devices that do not support line cards, specify **0**.

port

Specifies a valid port number.

ve *ve-id*

Specifies a virtual Ethernet (VE) interface.

vrf *name*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

ip *ip-address*

Specifies a next-hop IP address.

dynamic

Displays all the dynamic ARP entries in the ARP table.

static

Displays all the static ARP entries in the ARP table.

summary

Displays a summary of the ARP table.

Modes

Privileged EXEC mode

Output

The **show arp** command displays the following information:

Output field	Description
Address	Displays the IP address.
Mac-address	Displays the MAC address or "UnResolved".
L3 Interface	Displays the physical or VE interface.
L2 Interface	Displays the Layer 2 interface. Supported values: • (Physical interface): "Eth *slot* **/** *port* " • (Port-channel): "Po" • (VxLAN): "Tu" • "PW": VPLS Pseudo-wire • "UnResolved"
Age	In hh:mm:ss format, displays the time since the most recent renewal of a dynamic entry. For a static entry, displays "Never".
Vlan / BD	Displays the VLAN or the BD for the ARP entry. VLANs are indicated with a (V) and BDs with (B)
Type	Displays the ARP type. Supported values: • Dynamic • Static • MCT/EVPN: MCT peer ARPS or entries learned through the BGP-EVPN control plane • MCT/EVPN Sticky: MCT peer ARPs or entries learned through the BGP-EVPN control plane—with the "sticky" attribute (static or MY-IP at the originator). • LeakArp: An ARP entry leaked from another VRF. • PreArp: ARP triggered by other than the data traffic, for example, by the static route.

Examples

The following example displays the output of the basic **show arp** command.

```
 SLX# show arp

Total Entries in VRF default-vrf : 7911

Address        Mac-address     L3 Interface  L2 Interface            Vlan/BD    Age       Type
-------------------------------------------------------------------------------------------------------
-
133.1.1.2      0010.9400.0068  Ve 21         Eth 0/11                21 (V)     Never     Static
133.1.1.2      0010.9400.0069  Ve 2          Po 100                  2 (V)      00:17:58  Dynamic
133.1.5.2      0010.9400.006c  Ve 6          Po 100                  6 (V)      Never     Mct
133.9.1.2      0010.9400.0099  Ve 10         Tu 32769 (60.1.1.1)     10 (V)     Never     Mct-Sticky
133.8.249.2    0010.9400.0860  Ve 2042       Tu 32771 (17.17.17.17)  2042 (V)   Never     Bgp-Evpn
133.9.252.2    0010.9400.0862  Ve 1049       Tu 32771 (17.17.17.17)  1049 (V)   Never     Bgp-Evpn-
Sticky
133.100.1.2    0010.9400.001a  Ve 212        Eth 0/12                219 (B)    Never     Static
133.111.1.2    0010.9400.001b  Ve 199        Eth 0/1.5264            188 (B)    00:1:36   Dynamic
```

```
133.121.5.2    0010.9400.001c  Ve 189        Po 100                  163 (B)    Never     Mct
133.19.1.2     0010.9400.001d  Ve 111        Tu 32769 (60.1.1.1)     100 (B)    Never     Mct-Sticky
133.204.249.2  0010.9400.081e  Ve 2034       Tu 32771 (17.17.17.17)  2049 (B)   Never     Bgp-Evpn
133.192.252.2  0010.9400.081f  Ve 1299       Tu 32771 (17.17.17.17)  101 (B)    Never     Bgp-Evpn-
Sticky

SLX#
```

The following example displays the output of the **show arp summary** option.

```
device# show arp summary
Static Entries                    : 1
Dynamic Entries                   : 6
Leaked Entries                    : 2
Pre-arp Entries                   : 1
Remote (MCT/EVPN) Entries         : 0
Remote (MCT/EVPN) Sticky Entries  : 14
Total Entries                     : 24
```

show arp access-list

Displays one or all Address Resolution Protocol (ARP) access control lists (ACLs) available on a device, including permit statements.

Syntax

show arp access-list [*acl-name*]

Parameters

acl-name

Specifies the name of an ARP ACL defined on the device.

Modes

Privileged EXEC mode

Examples

The following example displays the name and permit statements of an ARP ACL named "list1".

```
device# show arp access-list list1
ARP access list list1
     permit ip host 192.85.1.2 mac host 0010.9400.0002
     permit ip host 192.85.1.3 mac host 0010.9400.0003 log
     permit ip host 196.2.1.2 mac host 0020.3200.0008
```

The following example displays the name and permit statements of all ARP ACLs.

```
device# show arp access-list
ARP access list list1
     permit ip host 192.85.1.2 mac host 0010.9400.0002
     permit ip host 192.85.1.3 mac host 0010.9400.0003 log
     permit ip host 196.2.1.2 mac host 0020.3200.0008
ARP access list list2
     permit ip host 20.20.20.1 mac host 0011.9400.0001 log
     permit ip host 30.30.30.1 mac host 0011.9400.0002
```

show bfd

Displays Bidirectional Forwarding Detection (BFD) information.

Syntax

show bfd

Modes

Privileged EXEC mode

Output

The **show bfd** command displays the following information:

Output field	Description
BFD State	Specifies whether BFD is enabled or disabled on the device.
Version	Specifies the version of the BFD protocol operating on the device.
Supported Protocols	Specifies the protocols that are registered for the particular session.
Current	The number of hardware and software BFD sessions operating on the device.
Max Allowed	The maximum number of BFD sessions that are allowed on the device. The maximum number of sessions supported on a device is 250.
Max Exceeded Count	The number of times the request to set up a BFD session was declined because it would have resulted in exceeding the maximum number of BFD sessions allowed on the device.
Port	The port on which BFD is enabled. Entry for a port is displayed only if it has at least one session on that interface.
MinTx	The interval in milliseconds during which the device sends a BFD message from this port to its peer.
MinRx	The interval in milliseconds during which the device receives a BFD message from its peer on this port.

Output field	Description
Mult	The number of times that the device waits for the MinRx time on this port before determining that its peer device is nonoperational.
Sessions	The number of BFD sessions originating on this port.

Examples

The following example displays typical information.

```
device# show bfd
  BFD State: ENABLED, Version: 1
  Supported Protocols: static-ip, ospf6, ospf, bgp

  All Sessions: Current HW : 0 Current SW : 0 Max Allowed: 250 Max Exceeded Count: 0

  Port            MinTx       MinRx       Mult Sessions
  ====            =====       =====       ==== ========
  ve2             100         100         3    1
```

show bfd neighbors

Displays Bidirectional Forwarding Detection (BFD) neighbor information.

Syntax

show bfd neighbors [**vrf** *vrfname* [**details**]]

Parameters

vrf *vrfname*

Specifies the name of a nondefault VRF instance.

details

Displays detailed neighbor information.

Modes

Privileged EXEC mode

Usage Guidelines

Output

The **show bfd neighbors** command displays the following information:

Output field	Description
OurAddr	Specifies the source IP address of the interface on which this BFD session is running.
NeighAddr	The IPv4 or IPv6 address of the remote neighbor.
State	The current state of the BFD session: • UP • DOWN • A.DOWN - The administrative down state. • INIT - The initialization state. • UNKNOWN - The current state is unknown.
Int	Specifies the interface on which the BFD session is running.

Examples

The following example shows sample output from the **show bfd neighbors** command.

```
device# show bfd neighbors

Flags: * indicates State is inconsistent across the cluster
```

```
OurAddr      NeighAddr   State      Int
=======      =========   =====      ===
7.7.7.1      7.7.7.2     UP         Eth 0/1/2
```

show bfd neighbors application

Displays Bidirectional Forwarding Detection (BFD) neighbor session information.

Syntax

show bfd neighbors application { **bgp** | **isis** | **ospf** | **ospf6** | **static-ip**}

Parameters

bgp

Specifies Border Gateway Protocol (BGP) sessions.

isis

Specifies Intermediate System to Intermediate System (IS-IS) sessions.

ospf

Specifies Open Shortest Path First (OSPF) sessions.

ospf6

Specifies Open Shortest Path First version 3 (OSPFv3) sessions.

static-ip

Specifies static IPv4 and IPv6 sessions.

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Output

The **show bfd neighbors application** command displays the following information:

Output field	Description
OurAddr	Specifies the source IP address of the interface on which this BFD session is running.
NeighAddr	The IPv4 or IPv6 address of the remote neighbor.

Output field	Description
State	The current state of the BFD session: • UP • DOWN • A.DOWN - The administrative down state. • INIT - The initialization state. • UNKNOWN - The current state is unknown.
Int	Specifies the interface on which the BFD session is running.

Examples

The following example shows sample output when the **ospf** keyword is used.

```
device# show bfd neighbors application ospf

Flags: * indicates State is inconsistent across the cluster
OurAddr     NeighAddr   State     Int
=======     =========   =====     ===
7.7.7.1     7.7.7.2     UP        Eth 0/1/2

Local    State: UP  Diag: 0  Demand mode: 0 Poll: 0
Received State: UP  Diag: 0  Demand mode: 0 Poll: 0 Final: 0
Local    MinTxInt(ms): 1000   MinRxInt(ms): 1000   Multiplier: 5
Received MinTxInt(ms): 1000   MinRxInt(ms): 1000   Multiplier: 5
  Rx Count: 3806   Tx Count: 4308
  LD/RD: 10001/10001   Heard from Remote: Y
Current Registered Protocols: ospf
Uptime: 0 day 0 hour 0 min 0 sec 0 msec
```

show bfd neighbors dest-ip

Displays Bidirectional Forwarding Detection (BFD) neighbor information about destination devices.

Syntax

show bfd neighbors dest-ip { *ip-address* | *ipv6-address* } [**details**]

show bfd neighbors dest-ip { *ip-address* | *ipv6-address* } **interface** { **ethernet** *slot/port* | **loopback** *number* | **port-channel** *number* | **ve** *ve-interface-number* }

Parameters

ip-address

Specifies the IP address of the destination device.

ipv6-address

Specifies the IPv6 address of the destination device.

details

Displays detailed neighbor information about the destination device.

interface

Displays BFD neighbor interface information.

ethernet *slot/port*

Specifies an Ethernet slot and port.

loopback *number*

Specifies a loopback interface. Valid values range from 1 through 255.

port-channel *number*

Specifies a port-channel interface.

ve *ve-interface-number*

Specifies a virtual Ethernet (VE) interface.

Modes

Privileged EXEC mode

Output

The **show bfd neighbors dest-ip** command displays the following information:

Output field	Description
OurAddr	Specifies the source IP address of the interface on which this BFD session is running.
NeighAddr	The IPv4 or IPv6 address of the remote neighbor.
State	The current state of the BFD session: • UP • DOWN • A.DOWN - The administrative down state. • INIT - The initialization state. • UNKNOWN - The current state is unknown.
Int	Specifies the interface on which the BFD session is running.

Examples

The following example shows sample output from the **show bfd neighbors dest-ip** command when the **details** keyword is used.

```
device# show bfd neighbors dest-ip 5.1.0.1 details
Flags: * indicates State is inconsistent across the cluster
OurAddr                                 NeighAddr
State     Int
=======                                 =========
=====     ===
5.1.0.2                                 5.1.0.1
UP        ve6

  Local    State: UP            Diag: 0              Demand mode: 0    Poll: 0
  Received State: UP            Diag: 0              Demand mode: 0    Poll: 0    Final: 1
  Local    MinTxInt(ms): 200    MinRxInt(ms): 200    Multiplier: 3
  Received MinTxInt(ms): 200    MinRxInt(ms): 200    Multiplier: 3
  Rx Count: 129722              Tx Count: 4
  LD/RD:          3/62          Heard from Remote: Y
  Current Registered Protocols: bgp
  Uptime: 0 day 5 hour 24 min 17 sec 424 msec
```

show bfd neighbors details

Displays details about Bidirectional Forwarding Detection (BFD) neighbors.

Syntax

show bfd neighbors details

Modes

Privileged EXEC mode

Output

The **show bfd neighbors details** command displays the following information:

Output field	Description
OurAddr	Specifies the source IP address of the interface on which this BFD session is running.
NeighAddr	Specifies the IPv4 address of the remote neighbor.
State	Specifies the current state of the BFD session: • UP • DOWN • A.DOWN - The administrative down state. • INIT - The initialization state. • UNKNOWN - The current state is unknown.
Int	Specifies the interface on which the BFD session is running.
Local:	
State	State of the local device.
Diag	Value of the diagnostic field in the BFD control message as used by the device in the last message sent.
Demand mode	Value of the demand in the BFD control message as used by the device in the last message received.
Poll	Value of the poll in the BFD control message as used by the device in the last message sent or received.
Received	
State	State of the remote device.

Output field	Description
Diag	Value of the diagnostic field in the BFD control message as used by the device in the last message received.
Demand mode	Value of the demand in the BFD control message as used by the device in the last message received.
Poll	Value of the poll in the BFD control message as used by the device in the last message received.
Final	Value of the final bit in the BFD control message as used by the device in the last message received.
Local	The local device
MinTxInt(ms)	The interval in milliseconds between which the device will send a BFD message from this local neighbor port to its peer.
MinRxInt(ms)	The interval in milliseconds that the neighbor device waits to receive a BFD message from its peer on this local port.
Multiplier	The number of times that the neighbor device will wait for the MinRxInterval time on this port before it determines that its peer device is nonoperational.
Received	Remote Device
MinTxInt(ms)	The interval in milliseconds between which the device will send a BFD message from the remote neighbor port to its peer.
MinRxInt(ms)	The interval in milliseconds that the neighbor device waits to receive a BFD message from its peer on this remote port.
Multiplier	The number of times that the remote neighbor device will wait for the MinRxInterval time on this port before it determines that its peer device is nonoperational.
Rx Count	Total number of BFD control messages received from the remote peer.
Tx Count	Total number of BFD control messages sent to the remote peer.
LD/RD	Local and remote discriminator.
Heard from Remote	Indicates the packets received from the BFD neighbor.

Output field	Description
Current Registered Protocols	Specifies the protocols that are registered for the particular session.
Uptime	The amount of time the BFD session has been in the up state.

This example shows typical output for the command.

```
device# show bfd neighbors details
Flags: * indicates State is inconsistent across the cluster
OurAddr                                 NeighAddr
State     Int
=======                                 =========
=====     ===
121.5.0.1                               121.5.0.2
UP        ve256

  Local    State: UP            Diag: 0              Demand mode: 0    Poll: 0
  Received State: UP            Diag: 0              Demand mode: 0    Poll: 0    Final:
0
  Local    MinTxInt(ms): 100    MinRxInt(ms): 100    Multiplier: 3
  Received MinTxInt(ms): 100    MinRxInt(ms): 100    Multiplier: 3
  Rx Count: 0                   Tx Count: 0
  LD/RD:          1/1           Heard from Remote: Y
  Current Registered Protocols: static-ip
  Uptime: 0 day 0 hour 15 min 31 sec 981 msec

  Session type : Hardware
OurAddr                                 NeighAddr
State     Int
=======                                 =========
=====     ===
121.6.0.1                               121.6.0.2
UP        ve257

  Local    State: UP            Diag: 0              Demand mode: 0    Poll: 0
  Received State: UP            Diag: 0              Demand mode: 0    Poll: 0    Final:
0
  Local    MinTxInt(ms): 100    MinRxInt(ms): 100    Multiplier: 3
  Received MinTxInt(ms): 100    MinRxInt(ms): 100    Multiplier: 3
  Rx Count: 0                   Tx Count: 0
  LD/RD:          3/3           Heard from Remote: Y
  Current Registered Protocols: static-ip
  Uptime: 0 day 0 hour 15 min 31 sec 981 msec

  Session type : Software
```

show bfd neighbors interface

Displays Bidirectional Forwarding Detection (BFD) neighbor information about specified interfaces.

Syntax

```
show bfd neighbors interface { ethernet slot/port | loopback number
   | tunnel number | port-channel number | ve ve-interface-number }
   [ details ]
```

Parameters

ethernet *slot/port*

Specifies an Ethernet slot and port.

loopback *number*

Specifies a loopback interface. Valid values range from 1 through 255.

tunnel *number*

Specifies a tunnel interface. Valid values range from 1 through 100000.

port-channel *number*

Specifies a port-channel interface.

ve *ve-interface-number*

Specifies a virtual Ethernet (VE) interface.

details

Specifies detailed information.

Modes

Privileged EXEC mode

Output

The **show bfd neighbors interface** command displays the following information:

Output field	Description
OurAddr	Specifies the source IP address of the interface on which this BFD session is running.
NeighAddr	The IPv4 or IPv6 address of the remote neighbor.

Output field	Description
State	The current state of the BFD session: • UP • DOWN • A.DOWN - The administrative down state. • INIT - The initialization state. • UNKNOWN - The current state is unknown.
Int	Specifies the interface on which the BFD session is running.

Examples

The following example shows BFD neighbor information with details about a specific VE interface.

```
device# show bfd neighbors interface ve 6 details
Flags: * indicates State is inconsistent across the cluster
OurAddr                                 NeighAddr
State     Int
=======                                 =========
=====     ===
5.1.0.2                                 5.1.0.1
UP        ve6

  Local    State: UP            Diag: 0              Demand mode: 0    Poll: 0
  Received State: UP            Diag: 0              Demand mode: 0    Poll: 0    Final: 1
  Local    MinTxInt(ms): 200    MinRxInt(ms): 200    Multiplier: 3
  Received MinTxInt(ms): 200    MinRxInt(ms): 200    Multiplier: 3
  Rx Count: 129409              Tx Count: 4
  LD/RD:          3/62          Heard from Remote: Y
  Current Registered Protocols: bgp
  Uptime: 0 day 5 hour 23 min 30 sec 427 msec
```

show bgp evpn ethernet-segment

Displays the Ethernet Segment information for the multi-homed client. When the *esi* parameter is provided, displays information for that ESI.

Syntax

show bgp evpn ethernet-segment { **esi** *es-id* }

Parameters

esi *es-id*

Use this option to query for ESI information for a particular ESI value.

Modes

EXEC mode

Output

The displays the following information:

Output field	Description
ESI	The unique ethernet segment identifier.
Interface	The interface on which the ethernet segment is deployed.
Interface State	The state of the interface, can be either *Up* or *down*.
Load balancing Mode	The type of load balancing applied to the interface.
List of MH Nodes	The list of MH nodes.
DF Vlans	The VLANs for the Designated Forwarder.
DF BD	The broadcast domain for the Designated Forwarders.
AC-influenced-DF-election	The status of the AC influenced DF Election setting.

Examples

The following example displays the ethernet segment information for all interfaces on the multi-homed client.

```
sw#show bgp evpn ethernet-segment
ESI : 00.112233445566778899
Interface : po4
Interface state : Up
Load balancing Mode : Active-Active
AC-influenced-DF-election : Enabled
List of MH Nodes : 1.1.1.1 2.2.2.2
DF Vlans : 100 102 104 106 108 110
DF BD :  50 52 54 56 58 60
```

show bgp evpn evid

Displays BGP EVPN information for a specific EV Id.

Syntax

show bgp evpn evid evid *<evid-value>*]

Parameters

evid *<evid-value>*

Specifies the EVPN ID to display information for. Specify a value in the range of 1-12288.

Modes

Privileged EXEC mode

Examples

The following example shows the details for a specific BGP EVPN.

```
SLX_mh1_peer_2# show bgp evpn evid 62
EVID                   : 62
VLAN/BD                : 62
VNI                      : 62
Extended                 : Yes
Is L3VNI                 : No
VRF ID                   : 1
L2S redistribution       : Disabled
ARP & ND redistribution  : Enabled
ARP subscription         : Disabled
ND  subscription         : Disabled
SVI MAC                  : 0000.0000.0000
SLX_mh1_peer_2#
```

show bgp evpn vni

Displays the BGP EVPN information for a specific virtual network identifiers (VNI).

Syntax

show bgp evpn vni *<vni-number>*

Parameters

vni *<vni-number>*

The VNI number. Provide a value in the range of 1-16777215.

Modes

Privileged EXEC mode

Examples

The following example shows information for a specific VNI.

```
SLX_mh1_peer_2# show bgp evpn vni 61
EVID                    : 61
VLAN/BD                 : 61
VNI                     : 61
Extended                : Yes
Is L3VNI                : No
VRF ID                  : 1
L2S redistribution      : Disabled
ARP & ND redistribution : Enabled
ARP subscription        : Disabled
ND  subscription        : Disabled
SVI MAC                 : 0000.0000.0000
SLX_mh1_peer_2#
```

show bgp evpn interface tunnel

This command displays information about the EVPN Tunnel interface.

Syntax

show bgp evpn interface tunnel [*<ip-address>* | **dynamic-discovered**]

Parameters

dynamic-discovered

Displays information for dynamically discovered tunnels.

<ip-address>

Displays information for the tunnel specified by this IP address.

Modes

Privileged EXEC mode

Examples

The following example displays information about BGP EVPN Tunnels

```
SLX_Leaf-1A# show bgp evpn interface tunnel
VTEP ID         : 1
VRF  ID         : 1
VTEP Source IP  : 172.31.254.217
-------------------------------------------------------------------------------------
  IfIndex        Dest IP             Status    Type    MAC Learning on Tunnel (BGP EVPN)
-------------------------------------------------------------------------------------
0x7c008003       172.31.254.179      Up        DYNAMIC      YES
0x7c008004       172.31.254.145      Up        DYNAMIC      YES
0x7c008005       172.31.254.204      Up        DYNAMIC      YES
0x7c008006       172.31.254.114      Up        DYNAMIC      YES
SLX_Leaf-1A#
```

The following example shows the output for the *dynamic-discovered* parameter.

```
SLX_Leaf-1A# show bgp evpn interface tunnel dynamic-discovered
VTEP ID         : 1
VRF  ID         : 1
VTEP Source IP  : 172.31.254.217
-------------------------------------------------------------------------------------
IfIndex        Dest IP             Status    Type    MAC Learning on Tunnel (BGP EVPN)
-------------------------------------------------------------------------------------
0x7c008003       172.31.254.179      Up        DYNAMIC      YES
0x7c008004       172.31.254.145      Up        DYNAMIC      YES
0x7c008005       172.31.254.204      Up        DYNAMIC      YES
0x7c008006       172.31.254.114      Up        DYNAMIC      YES
SLX_Leaf-1A#
```

The following example shows the output for a specific tunnel.

```
SLX_Leaf-1A# show bgp evpn interface tunnel 172.31.254.179
VTEP ID         : 1
VRF  ID         : 1
```

```
VTEP Source IP  : 172.31.254.217
-------------------------------------------------------------------------------------------
IfIndex        Dest IP             Status    Type    MAC Learning on Tunnel (BGP EVPN)
-------------------------------------------------------------------------------------------
0x7c008003       172.31.254.179      Up        DYNAMIC      YES
SLX_Leaf-1A#
```

show bgp evpn l2route

Displays BGP EVPN Layer 2 route information in the MAC VRF table.

Syntax

show bgp evpn l2route type { **arp** |**igmp-join-sync** | **igmp-leave-sync** | **inclusive-multicast** | **mac** | **nd**}

Parameters

type { **arp** |**igmp-join-sync** | **igmp-leave-sync** | **inclusive-multicast** | **mac** | **nd**}

Specifies the type of route.

Modes

Privileged EXEC mode

Examples

The following example shows routes in the VPN table.

```
device# show bgp evpn l2route
Total number of BGP EVPN Routes : 5
Status codes: s suppressed, d damped, h history, * valid, > best, i internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network            Next Hop        MED        LocPrf     Weight Path
Route Distinguisher: 3.3.100.3:1
*>  IMR:[50][IPv4:3.3.100.3]
                       0.0.0.0         0          100        0      ?
*>i IMR:[50][IPv4:4.4.100.4]
                       4.4.100.4       0          100        0      ?
*>i IMR:[50][IPv4:5.5.100.5]
                       5.5.100.5       0          100        0      ?
*>  MAC:[50][0000.0300.0050]
                       0.0.0.0         0          100        0      ?
*>i MAC:[50][0000.0400.0050]
                       4.4.100.4       0          100        0      ?
```

The following example displays details for inclusive-multicast routes. In this example, the EVPN instance is configured with route-targets configured automatically.

```
device# show bgp evpn l2route type inclusive-multicast detail
Total number of BGP EVPN IMR Routes : 3
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
Route Distinguisher: 3.3.100.3:1
1       Prefix: IMR:[50][IPv4:3.3.100.3],  Status: BL,  Age: 0h8m46s
         NEXT_HOP: 0.0.0.0, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: ExtCom:03:0c:00:00:00:00:00:08
```

```
            PMSI Attribute Flags: 0x00000000  Label-Stack: 0x00000032 Tunnel-Type:
0x00000006 Tunnel-IP: 3.3.100.3
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            L2_vni: 50
            RD: 3.3.100.3:1
2       Prefix: IMR:[50][IPv4:4.4.100.4],  Status: BI,  Age: 0h2m43s
         NEXT_HOP: 4.4.100.4, Learned from Peer: 4.4.100.4 (100)
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: ExtCom:03:0c:00:00:00:00:00:08 RT 25600:838860816 RT
100:50
            PMSI Attribute Flags: 0x00000000  Label-Stack: 0x00000032 Tunnel-Type:
0x00000006 Tunnel-IP: 4.4.100.4
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            L2_vni: 50
            RD: 3.3.100.3:1
3       Prefix: IMR:[50][IPv4:5.5.100.5],  Status: BI,  Age: 0h2m37s
         NEXT_HOP: 5.5.100.5, Learned from Peer: 5.5.100.5 (100)
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: ExtCom:03:0c:00:00:00:00:00:08 RT 25600:838860816 RT
100:50
            PMSI Attribute Flags: 0x00000000  Label-Stack: 0x00000032 Tunnel-Type:
0x00000006 Tunnel-IP: 5.5.100.5
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            L2_vni: 50
            RD: 3.3.100.3:1
```

The following example displays details for inclusive-multicast routes. In this example, the EVPN instance is configured with route-targets configured explicitly.

```
device# show bgp evpn l2route type inclusive-multicast detail
Total number of BGP EVPN IMR Routes : 2
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
Route Distinguisher: 3.3.100.3:1
1       Prefix: IMR:[50][IPv4:3.3.100.3],  Status: BL,  Age: 0h4m17s
         NEXT_HOP: 0.0.0.0, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: ExtCom:03:0c:00:00:00:00:00:08
            PMSI Attribute Flags: 0x00000000  Label-Stack: 0x00000032 Tunnel-Type:
0x00000006 Tunnel-IP: 3.3.100.3
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            L2_vni: 50
            RD: 3.3.100.3:1
2       Prefix: IMR:[50][IPv4:4.4.100.4],  Status: BI,  Age: 0h3m31s
         NEXT_HOP: 4.4.100.4, Learned from Peer: 4.4.100.4 (100)
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: ExtCom:03:0c:00:00:00:00:00:08 RT 50:1
            PMSI Attribute Flags: 0x00000000  Label-Stack: 0x00000032 Tunnel-Type:
0x00000006 Tunnel-IP: 4.4.100.4
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            L2_vni: 50
            RD: 3.3.100.3:1
```

The following example displays details for MAC routes. **BI** indicates that the route is "Best" and "Installed." This ensures that it is downloaded into the system.

```
device# show bgp evpn l2route type mac detail
Total number of BGP EVPN MAC Routes : 1
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
Route Distinguisher: 01:00:04:03:02:01:01:00
1       Prefix: MAC:[100][1111.2222.3333],  Status: BI,  Age: 0h6m17s
         NEXT_HOP: 10.20.30.40, Learned from Peer: 10.0.0.2 (100)
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: ExtCom:03:0c:00:00:00:00:08:00 RT 25600:1677721600
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            L2_vni: 100
            ESI : 00.000000000000000000
            RD: 01:00:04:03:02:01:01:00
```

show bgp evpn l2route next-hop

Displays information for BGP EVPN Layer 2 routes received from the specified next-hop.

Syntax

show bgp evpn l2route next-hop { *ipv4-address* | *ipv6-address* } **type** { **igmp-join-sync** | **igmp-leave-sync** | **inclusive-multicast**}

Parameters

ipv4-address

Specifies an IPv4 address.

ipv6-address

Specifies an IPv6 address.

type

Specifies the type of route.

igmp-join-sync

Specifies Join Sync routes.

igmp-leave-sync

Specifies Leave Sync routes.

inclusive-multicast

Specifies Leave Sync routes.

Modes

Privileged EXEC mode

Examples

This example displays inclusive multicast information received from 2.2.2.2.

```
device# show bgp evpn l2route next-hop 2.2.2.2 type inclusive-multicast
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix             Next Hop        MED        LocPrf     Weight Status
1      IMR:[2][IPv4:2.2.2.2]
                          2.2.2.2         0          100        0      BL
         AS_PATH:
         L2 Label: 2
```

show bgp evpn l2route unreachable

Displays route information about BGP EVPN Layer 2 routes whose destinations are unreachable through any path in the BGP EVPN route table.

Syntax

show bgp evpn l2route unreachable type { **igmp-join-sync** | **igmp-leave-sync**}

Parameters

type

Specifies the type of route.

igmp-join-sync

Specifies Join Sync routes.

igmp-leave-sync

Specifies Leave Sync routes.

Modes

Privileged EXEC mode

This example shows bgp evpn l2route unreachable.

```
SLX-MH1# show bgp evpn l2route unreachable
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix             Next Hop        MED        LocPrf     Weight RPKI State Status
1      IMR:[101][IPv4:2.2.2.2]
                          2.2.2.2          none      100        0      E
         AS_PATH: 200 100
         L2 Label: 101
2      IMR:[102][IPv4:2.2.2.2]
                          2.2.2.2          none      100        0      E
         AS_PATH: 200 100
         L2 Label: 102
3      ESR:[01.609c9f.871e00.000100][IPv4:2.2.2.2]
                          2.2.2.2          none      100        0      E
         AS_PATH: 200 100
```

show bgp evpn l3vni

Displays BGP EVPN information for Layer 3 virtual network identifiers (VNIs).

Syntax

show bgp evpn l3 vni { **all-vrfs** | **vrf** *name* }

Parameters

all-vrfs

Specifies all VRFs.

vrf *name*

Specifies the name of the VRF instance.

Modes

Privileged EXEC mode

Examples

The following example shows Layer 3 VNI information for all VRFs.

```
device# show bgp evpn l3vni all-vrfs

------------------------------------------------------------------------
   L3VNI Prefix Origination Conditions for vrf (2)
------------------------------------------------------------------------
Address Family under BGP : True
RD Configured            : True
L3 VNI Configured        : True
VLAN VNI Mapping exists  : True
Router mac Exists        : True
L3 VNI  Link UP          : True
Source VTEP              : 0x06000006
L3VNI Active             : Active


------------------------------------------------------------------------
   L3VNI Prefix Import Conditions for vrf (2)
------------------------------------------------------------------------
Address Family under BGP : True
L3 VNI Configured        : True
VLAN VNI Mapping exists  : True
Router mac Exists        : True
L3VNI Active             : Active


------------------------------------------------------------------------
   L3VNI Prefix Origination Conditions for vrf (3)
------------------------------------------------------------------------
Address Family under BGP : True
RD Configured            : True
L3 VNI Configured        : True
VLAN VNI Mapping exists  : True
```

```
Router mac Exists        : True
L3 VNI  Link UP          : True
Source VTEP              : 0x06000006
L3VNI Active             : Active


-------------------------------------------------------------------------
   L3VNI Prefix Import Conditions for vrf (3)
-------------------------------------------------------------------------
Address Family under BGP : True
L3 VNI Configured        : True
VLAN VNI Mapping exists  : True
Router mac Exists        : True
L3VNI Active             : Active


-------------------------------------------------------------------------
   L3VNI Prefix Origination Conditions for vrf (4)
-------------------------------------------------------------------------
Address Family under BGP : True
RD Configured            : True
L3 VNI Configured        : True
VLAN VNI Mapping exists  : True
Router mac Exists        : True
L3 VNI  Link UP          : True
Source VTEP              : 0x06000006
L3VNI Active             : Active


-------------------------------------------------------------------------
   L3VNI Prefix Import Conditions for vrf (4)
-------------------------------------------------------------------------
Address Family under BGP : True
L3 VNI Configured        : True
VLAN VNI Mapping exists  : True
Router mac Exists        : True
L3VNI Active             : Active


-------------------------------------------------------------------------
   L3VNI Prefix Origination Conditions for vrf (5)
-------------------------------------------------------------------------
Address Family under BGP : True
RD Configured            : True
L3 VNI Configured        : True
VLAN VNI Mapping exists  : True
Router mac Exists        : True
L3 VNI  Link UP          : True
Source VTEP              : 0x06000006
L3VNI Active             : Active


-------------------------------------------------------------------------
   L3VNI Prefix Import Conditions for vrf (5)
-------------------------------------------------------------------------
Address Family under BGP : True
L3 VNI Configured        : True
VLAN VNI Mapping exists  : True
Router mac Exists        : True
L3VNI Active             : Active
```

The following example shows Layer 3 VNI information for a specified VRF.

```
device# show bgp evpn l3vni vrf red

------------------------------------------------------------------------
   L3VNI Prefix Origination Conditions for vrf (red)
------------------------------------------------------------------------
Address Family under BGP : True
RD Configured            : True
IRB I/F Configured        : True (0x48000064)
IRB I/F Status            : False
IRB EVID Conigured        : True (100)
Router mac Exists        : True
Source VTEP              : 40.40.40.1
VTEP Active              : Active
IPv4 L3VNI Active             : Active
IPv6 L3VNI Active             : Inactive


------------------------------------------------------------------------
   L3VNI Prefix Import Conditions for vrf (red)
------------------------------------------------------------------------
Address Family under BGP : True
IRB I/F Configured       : True (0x48000064)
IRB EVID Configured      : True (100)
Router mac Exists        : True
IPv4 L3VNI Active             : Active
IPv6 L3VNI Active             : Inactive
```

show bgp evpn neighbors

Displays configuration information for BGP EVPN neighbors of the device.

Syntax

show bgp evpn neighbors [*ip-addr* | *ipv6-addr* | **routes-summary**]

Parameters

ip-addr

Specifies the IPv4 address of a neighbor.

ipv6-addr

Specifies the IPv6 address of a neighbor.

routes-summary

Displays routes received, routes accepted, number of routes advertised by peer, and so on.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to view configuration information and statistics for BGP EVPN neighbors of the device. Output shows all configured parameters for the neighbors.

Examples

The following example shows sample output from the `show bgp evpn neighbors` command.

```
device# show bgp evpn neighbors
Total number of BGP Neighbors: 1
    '+': Data in InQueue '>': Data in OutQueue '-': Clearing
    '*': Update Policy 'c': Group change 'p': Group change Pending
    'r': Restarting 's': Stale '^': Up before Restart '<': EOR waiting

1   IP Address: 20.0.0.2, AS: 100 (IBGP), RouterID: 2.2.2.2, VRF: default-vrf
    State: ESTABLISHED, Time: 0h0m13s, KeepAliveTime: 60, HoldTime: 180
       KeepAliveTimer Expire in 38 seconds, HoldTimer Expire in 171 seconds
    Minimal Route Advertisement Interval: 0 seconds
       RefreshCapability: Received
       GracefulRestartCapability: Sent
           Restart Time 120 sec, Restart bit 0
           afi/safi 25/70, Forwarding bit 0
    Address Family : L2VPN EVPN
       SendExtendedCommunity: yes
    Messages:    Open        Update      KeepAlive   Notification   Refresh-Req
       Sent    : 7           9           5           0              0
       Received: 2           5           5           1              0
```

```
    Last Update Time: NLRI              Withdraw                NLRI
Withdraw
                  Tx: 0h0m12s           ---                 Rx: 0h0m12s             ---
    Last Connection Reset Reason:Rcv Notification
    Notification Sent:     Unspecified
    Notification Received: Cease/Administrative Reset
    Neighbor NLRI Negotiation:
      Peer Negotiated IPV4  unicast  capability
      Peer Negotiated L2VPN EVPN address family
      Peer configured for IPV4 unicast  Routes
      Peer configured for L2VPN EVPN address family
    Neighbor ipv6 MPLS Label Capability Negotiation:
    Neighbor AS4 Capability Negotiation:
    Outbound Policy Group:
       ID: 2, Use Count: 1
       Byte Sent:   804, Received: 607
       Local host:  20.0.0.1, Local  Port: 8015
       Remote host: 20.0.0.2, Remote Port: 179
    Maintenance Mode : Disabled
    G-Shut: Disabled
```

show bgp evpn neighbors advertised-routes

Displays information about the routes that the device has advertised to the specified neighbor during the current BGP EVPN session.

Syntax

show bgp evpn neighbors { *ip address* | *ipv6 address* } **advertised-routes** [**detail** |**type** [**arp** |**auto-discovery | ethernet-segment |igmp-join-sync | igmp-leave-sync** |**inclusive-multicast | ipv4-prefix | ipv6-prefix | mac | nd**]]

Parameters

ip address

Specifies the IPv4 address of a neighbor.

ipv6 address

Specifies the IPv6 address of a neighbor.

type

Specifies the type of route.

detail

Specifies that detailed information be shown for the designated route type.

arp

Specifies Address Resolution Protocol routes.

auto-discovery

Specifies automatically discovered routes.

ethernet-segment

Specifies Ethernet Segment (ES) routes.

igmp-join-sync

Specifies Join Sync routes.

igmp-leave-sync

Specifies Leave Sync routes.

inclusive-multicast

Specifies inclusive multicast routes.

ipv4-prefix

Specifies IPv4 prefix routes.

ipv6-prefix

Specifies IPv6 prefix routes.

mac

Specifies MAC routes.

nd

Specifies Neighbor Discovery routes.

Modes

Privileged EXEC mode

Examples

The following example shows output for the **show bgp evpn neighbors advertised-routes detail** command.

```
device# show bgp evpn neighbors 20.0.0.2 advertised-routes detail
There are 4 routes advertised to neighbor 20.0.0.2
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
1       Prefix: IP4Prefix:[0][2.1.1.0/24],  Status: BL,  Age: 0h5m11s
         NEXT_HOP: 1.1.1.1, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: RT 2:2 RT 03:0d:00:00:00:00:00:00 RT 100:1073741826 RT
06:03:60:9c:9f:de:0f:15 RT 03:0c:00:00:00:00:00:08
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 1,  Admin distance 0
            L3 Label: 2 (EVI)
            RD: 1:1
            As-magic: 17
2       Prefix: MAC:[0][609c.9fde.0f15],  Status: BL,  Age: 0h5m12s
         NEXT_HOP: 1.1.1.1, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: RT 100:268435458 RT 100:2 RT 06:00:01:00:00:00:00:00 RT
03:0d:00:00:00:00:00:00 RT 100:1073741826 RT 03:0c:00:00:00:00:00:08
            Mac Mobility Sticky: True
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 1,  Admin distance 0
            L2 Label: 2 (EVI)
            ESI : 00.0000000000000000000
            RD: 1.1.1.1:32770
            As-magic: 16
```

show bgp evpn neighbors routes

Displays routes of specified types received from designated BGP EVPN neighbors, for example, best BGP EVPN routes to their destination.

Syntax

show bgp evpn neighbors { *ip address* | *ipv6 address* } **routes** [*type*] | **best** [*type*] | **detail** [*type*] | **not-installed-best** [*type*] | **unreachable** [*type*]]

Parameters

type

Specifies the type of route.

auto-discovery

Specifies automatically discovered routes.

ethernet-segment

Specifies Ethernet Segments (ES) routes.

inclusive-multicast

Specifies inclusive multicast routes.

mac

Specifies MAC routes.

igmp-join-sync

Specifies Join Sync routes.

igmp-leave-sync

Specifies Leave Sync routes.

Modes

Privileged EXEC mode

Examples

The following example shows output for the **show bgp evpn neighbors routes best** command.

```
device# show bgp evpn neighbors 20.0.0.2 routes best
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix              Next Hop        MED        LocPrf     Weight Status
1      IMR:[0][IPv4:2.2.2.2]
                           2.2.2.2         0          100        0      BI
         AS_PATH:
         L2 Label: 2 (VNI)
2      ARP:[0][609c.9fde.1215]:[IPv4:2.1.1.1]
                           2.2.2.2         0          100        0      BI
```

```
          AS_PATH:
             L2 Label: 2 L3 Label: 0 (VNI)
          ESI : 00.000000000000000000
3       ARP:[0][609c.9fde.1215]:[IPv4:102.1.1.1]
                             2.2.2.2         0          100        0      BI
          AS_PATH:
             L2 Label: 2 L3 Label: 0 (VNI)
          ESI : 00.000000000000000000
4       MAC:[0][609c.9fde.1215]
                             2.2.2.2         0          100        0      BI
          AS_PATH:
          L2 Label: 2 (VNI)
          ESI : 00.000000000000000000
```

show bgp evpn routes

Displays EVPN routes in the VPN table. Routes are imported into the MAC VRF table if those routes are imported.

Syntax

show bgp evpn routes

Modes

Privileged EXEC mode

Examples

The following example shows routes in the VPN table.

```
device# show bgp evpn routes
Total number of BGP EVPN Routes : 5
Status codes: s suppressed, d damped, h history, * valid, > best, i internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network            Next Hop        MED        LocPrf     Weight Path
Route Distinguisher: 3.3.100.3:32818
*>  IMR:[0][IPv4:3.3.100.3]
                         3.3.100.3       0          100        0      ?
*>  MAC:[0][0000.0300.0050]
                         3.3.100.3       0          100        0      ?
Route Distinguisher: 4.4.100.4:32818
*>i IMR:[0][IPv4:4.4.100.4]
                         4.4.100.4       0          100        0      ?
*>i MAC:[0][0000.0400.0050]
                         4.4.100.4       0          100        0      ?
Route Distinguisher: 5.5.100.5:32818
*>i IMR:[0][IPv4:5.5.100.5]
                         5.5.100.5       0          100        0      ?
```

show bgp evpn routes best

Displays information for BGP EVPN routes that were selected as best routes.

Syntax

show bgp evpn routes best

show bgp evpn routes best [**type** { **auto-discovery** | **ethernet-segment** | **inclusive-multicast** | **ipv4-prefix** | **ipv6-prefix** | **mac** |**igmp-join-sync** | **igmp-leave-sync** }]

Parameters

type

Specifies the type of route.

auto-discovery

Specifies automatically discovered routes.

ethernet-segment

Specifies Ethernet Segments (ES) routes.

inclusive-multicast

Specifies inclusive multicast routes.

ipv4-prefix

Specifies IPv4 prefix routes.

ipv6-prefix

Specifies IPv6 prefix routes.

mac

Specifies MAC routes.

igmp-join-sync

Specifies Join Sync routes.

igmp-leave-sync

Specifies Leave Sync routes.

Modes

Privileged EXEC mode

Examples

The following example shows output for the **show bgp evpn routes best** command.

```
device# show bgp evpn neighbors 20.0.0.2 routes best
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
```

```
       Prefix             Next Hop        MED        LocPrf     Weight Status
1      IMR:[0][IPv4:2.2.2.2]
                          2.2.2.2         0          100        0      BI
         AS_PATH:
         L2 Label: 2 (VNI)
2      ARP:[0][609c.9fde.1215]:[IPv4:2.1.1.1]
                          2.2.2.2         0          100        0      BI
         AS_PATH:
            L2 Label: 2 L3 Label: 0 (VNI)
         ESI : 00.000000000000000000
3      ARP:[0][609c.9fde.1215]:[IPv4:102.1.1.1]
                          2.2.2.2         0          100        0      BI
         AS_PATH:
            L2 Label: 2 L3 Label: 0 (VNI)
         ESI : 00.000000000000000000
4      MAC:[0][609c.9fde.1215]
                          2.2.2.2         0          100        0      BI
         AS_PATH:
         L2 Label: 2 (VNI)
         ESI : 00.000000000000000000
```

show bgp evpn routes detail

Displays detailed BGP EVPN route information.

Syntax

show bgp evpn routes detail

Modes

Privileged EXEC mode

Examples

The following example shows output for the **show bgp evpn routes detail** command.

```
device# show bgp evpn routes detail
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
1       Prefix: IMR:[0][IPv4:2.2.2.2],  Status: BI,  Age: 0h9m34s
         NEXT_HOP: 2.2.2.2, Learned from Peer: 20.0.0.2 (100)
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: RT 100:268435458 RT 100:2 RT 100:1073741826 RT
03:0c:00:00:00:00:00:08
            PMSI Attribute Flags: 0x00000000  Label-Stack: 2 Tunnel-Type: 6 Tunnel-IP:
2.2.2.2
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            L2 Label: 2 (VNI)
            RD: 2.2.2.2:32770
            As-magic: 20
2       Prefix: ARP:[0][609c.9fde.1215]:[IPv4:2.1.1.1],  Status: BI,  Age: 0h9m34s
         NEXT_HOP: 2.2.2.2, Learned from Peer: 20.0.0.2 (100)
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: RT 100:268435458 RT 100:2 RT 06:00:01:00:00:00:00:00 RT
100:1073741826 RT 03:0c:00:00:00:00:00:08
            Mac Mobility Sticky: True
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            L2 Label: 2 L3 Label: 0 (VNI)
            ESI : 00.000000000000000000
            RD: 2.2.2.2:32770
            As-magic: 22
3       Prefix: ARP:[0][609c.9fde.1215]:[IPv4:1
```

show bgp evpn routes local

Displays information about BGP EVPN local routes.

Syntax

```
show bgp evpn routes local

show bgp evpn routes local type [ arp |auto-discovery | ethernet-segment
    | igmp-join-sync | igmp-leave-sync |inclusive-multicast | ipv4-prefix
    | ipv6-prefix | mac | nd]
```

Parameters

type

Specifies the type of route.

arp

Specifies Address Resolution Protocol routes.

auto-discovery

Specifies automatically discovered routes.

ethernet-segment

Specifies Ethernet Segments (ES) routes.

igmp-join-sync

Specifies Join Sync routes.

igmp-leave-sync

Specifies Leave Sync routes.

inclusive-multicast

Specifies inclusive multicast routes.

ipv4-prefix

Specifies IPv4 prefix routes.

ipv6-prefix

Specifies IPv6 prefix routes.

mac

Specifies MAC routes.

nd

Specifies Neighbor Discovery routes.

Modes

Privileged EXEC mode

Examples

The following example shows output for the **show bgp evpn routes local** command.

```
device# show bgp evpn routes local
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
1       Prefix: IMR:[0][IPv4:1.1.1.1],  Status: BL,  Age: 0h15m0s
         NEXT_HOP: 0.0.0.0, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: RT 100:1073741826 RT 2:2 RT 06:03:60:9c:9f:de:0f:15
            Adj_RIB_out count: 1,  Admin distance 0
            L2 Label: 2 (EVI)
            RD: 1:1
            As-magic: 8
2       Prefix: IP4Prefix:[0][2.1.1.0/24],  Status: BL,  Age: 0h14m59s
         NEXT_HOP: 0.0.0.0, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: RT 2:2 RT 03:0d:00:00:00:00:00:00 RT 100:1073741826
            Default Extd Gw  Community: Received
            Adj_RIB_out count: 1,  Admin distance 0
            L3 Label: 2 (EVI)
            RD: 1:1
            As-magic: 12
3       Prefix: ARP:[0][609c.9fde.0f15]:[IPv4:2.1.1.1],  Status: BL,  Age: 0h14m59s
         NEXT_HOP: 0.0.0.0, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: RT 06:00:01:00:00:00:00:00 RT 100:1073741826 RT 2:2
            Mac Mobility Sticky: True
            Adj_RIB_out count: 1,  Admin distance 0
            L2 Label: 2 L3 Label: 2 (EVI)
            ESI : 00.000000000000000000
            RD: 1.1.1.1:32770
            As-magic: 13
4       Prefix: MAC:[0][609c.9fde.0f15],  Status: BL,  Age: 0h15m0s
         NEXT_HOP: 0.0.0.0, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: RT 06:00:01:00:00:00:00:00 RT 03:0d:00:00:00:00:00:00 RT
100:1073741826
            Mac Mobility Sticky: True
            Default Extd Gw  Community: Received
            Adj_RIB_out count: 1,  Admin distance 0
            L2 Label: 2 (EVI)
            ESI : 00.000000000000000000
            RD: 1.1.1.1:32770
            As-magic: 5
```

This example shows output for the **show bgp evpn routes local** command when the **type** and **mac** keywords are used.

```
device# show bgp evpn routes local type mac

Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
1       Prefix: MAC:[0][0000.abba.abba],  Status: BL,  Age: 1d9h36m12s
         NEXT_HOP: 109.0.0.109, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
```

```
         AS_PATH:
            Extended Community: ExtCom:06:00:01:00:00:00:00:00
ExtCom:03:0d:00:00:00:00:00:00 ExtCom:03:0c:00:00:00:00:00:08 RT 65009:22
            Mac Mobility Sticky: True
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 3,  Admin distance 0
            L2_vni: 22
            ESI : 00.000000000000000000
2       Prefix: MAC:[0][0000.abba.baba],  Status: BL,  Age: 1d9h36m12s
         NEXT_HOP: 109.0.0.109, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: ExtCom:06:00:01:00:00:00:00:00
ExtCom:03:0d:00:00:00:00:00:00 ExtCom:03:0c:00:00:00:00:00:08 RT 65009:22
            Mac Mobility Sticky: True
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 3,  Admin distance 0
            L2_vni: 22
            ESI : 00.000000000000000000
3       Prefix: MAC:[0][0027.f8fd.274b],  Status: BL,  Age: 1d9h36m32s
         NEXT_HOP: 109.0.0.109, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: ExtCom:06:00:01:00:00:00:00:00
ExtCom:03:0d:00:00:00:00:00:00 ExtCom:03:0c:00:00:00:00:00:08 RT 65009:22
            Mac Mobility Sticky: True
            Default Extd Gw  Community: Received
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            Adj_RIB_out count: 3,  Admin distance 0
            L2_vni: 22
            ESI : 00.000000000000000000
   …
```

show bgp evpn routes next-hop

Displays information for BGP EVPN routes received from the specified next-hop.

Syntax

show bgp evpn routes next-hop { *ipv4-address* | *ipv6-address* } **type** { **auto-discovery** | **ethernet-segment** | **inclusive-multicast** | **ipv4-prefix** | **ipv6-prefix** | **mac** | **igmp-join-sync** | **igmp-leave-sync** }

Parameters

ipv4-address

Specifies an IPv4 address.

ipv6-address

Specifies an IPv6 address.

type

Specifies the type of route.

auto-discovery

Specifies automatically discovered routes.

ethernet-segment

Specifies Ethernet Segments (ES) routes.

inclusive-multicast

Specifies inclusive multicast routes.

ipv4-prefix

Specifies IPv4 prefix routes.

ipv6-prefix

Specifies IPv6 prefix routes.

mac

Specifies MAC routes.

igmp-join-sync

Specifies Join Sync routes.

igmp-leave-sync

Specifies Leave Sync routes.

Modes

Privileged EXEC mode

This example shows bgp evpn routes next-hop

```
SLX-MH1# show bgp evpn routes next-hop ?
Possible completions:
  <A.B.C.D>    IP address
  <A:B::C:D>   IPV6 address
```

```
SLX-MH1# show bgp evpn routes next-hop 2.2.2.2 type auto-discovery
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
1         Prefix: AD:[01.609c9f871e00000100][4294967295],  Status: E,  Age: 0h28m34s
         NEXT_HOP: 2.2.2.2, Learned from Peer: 30.1.1.1 (200)
          LOCAL_PREF: 100,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 200 100
            Extended Community: RT 06:01:00:00:00:00:00:00 RT 100:101 RT 100:1073741926
RT 03:0c:00:00:00:00:00:08
            ESI Label Ext Community: 0     All-Active (0x00000000)
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            RD: 2.2.2.2:1
            As-magic: 25
2         Prefix: AD:[01.609c9f871e00000100][0],  Status: E,  Age: 0h28m34s
         NEXT_HOP: 2.2.2.2, Learned from Peer: 30.1.1.1 (200)
          LOCAL_PREF: 100,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 200 100
            Extended Community: RT 06:01:00:00:00:00:00:00 RT 100:101 RT
03:0c:00:00:00:00:00:08
            ESI Label Ext Community: 0     All-Active (0x00000000)
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            RD: 2.2.2.2:134
            As-magic: 22
3         Prefix: AD:[01.609c9f871e00000100][0],  Status: E,  Age: 0h28m34s
         NEXT_HOP: 2.2.2.2, Learned from Peer: 30.1.1.1 (200)
          LOCAL_PREF: 100,  MED: none,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 200 100
            Extended Community: RT 06:01:00:00:00:00:00:00 RT 100:1073741926 RT
03:0c:00:00:00:00:00:08
            ESI Label Ext Community: 0     All-Active (0x00000000)
            Extended Community: ExtCom: Tunnel Encapsulation (Type Vxlan)
            RD: 2.2.2.2:135
            As-magic: 23
```

show bgp evpn routes no-best

Displays information for BGP EVPN routes that were selected as not best routes.

Syntax

show bgp evpn routes no-best

show bgp evpn routes no-best [**type** { **auto-discovery** | **ethernet-segment** | **inclusive-multicast** | **ipv4-prefix** | **ipv6-prefix** | **mac** | **igmp-join-sync** | **igmp-leave-sync**}]

Parameters

type

Specifies the type of route.

auto-discovery

Specifies automatically discovered routes.

ethernet-segment

Specifies Ethernet Segments (ES) routes.

inclusive-multicast

Specifies inclusive multicast routes.

ipv4-prefix

Specifies IPv4 prefix routes.

ipv6-prefix

Specifies IPv6 prefix routes.

mac

Specifies MAC routes.

igmp-join-sync

Specifies Join Sync routes.

igmp-leave-sync

Specifies Leave Sync routes.

Modes

Privileged EXEC mode

Examples

The following example shows output for the **show bgp evpn routes no-best** command.

```
device# show bgp evpn routes no-best
```

```
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix             Next Hop        MED        LocPrf     Weight Status
1      IMR:[0][IPv4:57.0.0.57]
                          57.0.0.57        0          100        0      I
         AS_PATH: 65009 65002 65006
         L2_vni: 22
2      ARP:[0][0000.abba.baba]:[IPv4:2.22.1.254]
                          57.0.0.57        0          100        0      I
         AS_PATH: 65009 65002 65006
            L2_vni: 22 L3_vni: 0
         ESI : 00.000000000000000000
3      ND:[0][0000.abba.abba]:[IPv6:2:22:1::254]
                          57.0.0.57        0          100        0      I
         AS_PATH: 65009 65002 65006
            L2_vni: 22 L3_vni: 0
         ESI : 00.000000000000000000
4      ND:[0][0027.f8ca.76ba]:[IPv6:fe80::227:f8ff:feca:76ba]
                          57.0.0.57        0          100        0      I
         AS_PATH: 65009 65002 65006
            L2_vni: 22 L3_vni: 0
         ESI : 00.000000000000000000
5      MAC:[0][0000.abba.abba]
                          57.0.0.57        0          100        0      I
         AS_PATH: 65009 65002 65006
         L2_vni: 22
         ESI : 00.000000000000000000
6      MAC:[0][0000.abba.baba]
                          57.0.0.57        0          100        0      I
         AS_PATH: 65009 65002 65006
         L2_vni: 22
         ESI : 00.000000000000000000
…
```

This example shows bgp evpn routes no-best

```
SLX-MH1# show bgp evpn routes no-best
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix             Next Hop        MED        LocPrf     Weight RPKI State Status
1      AD:[01.609c9f871e00000100][4294967295]
                          2.2.2.2          none       100        0      E
         AS_PATH: 200 100
2      AD:[01.609c9f871e00000100][0]
                          2.2.2.2          none       100        0      E
         AS_PATH: 200 100
3      AD:[01.609c9f871e00000100][0]
                          2.2.2.2          none       100        0      E
         AS_PATH: 200 100
```

show bgp evpn routes not-installed-best

Displays information for BGP EVPN best routes that are not installed.

Syntax

show bgp evpn routes not-installed-best

show bgp evpn routes not-installed-best [**type** { **auto-discovery** | **ethernet-segment** | **inclusive-multicast** | **ipv4-prefix** | **ipv6-prefix** | **mac** | **igmp-join-sync** | **igmp-leave-sync** }]

Parameters

type

Specifies the type of route.

auto-discovery

Specifies automatically discovered routes.

ethernet-segment

Specifies Ethernet Segments (ES) routes.

inclusive-multicast

Specifies inclusive multicast routes.

ipv4-prefix

Specifies IPv4 prefix routes.

ipv6-prefix

Specifies IPv6 prefix routes.

mac

Specifies MAC routes.

igmp-join-sync

Specifies Join Sync routes.

igmp-leave-sync

Specifies Leave Sync routes.

Modes

Privileged EXEC mode

This example shows bgp evpn routes not-installed-best

```
B06_S1-113# show bgp evpn routes not-installed-best
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix             Next Hop        MED        LocPrf     Weight RPKI State Status
1      IMR:[0][IPv4:172.31.254.234]
                          172.31.254.234  0          100        0      bE
         AS_PATH: 4200003000
         L2 Label: 101 (VNI)
```

```
2      ARP:[0][0201.0101.0101]:[IPv4:172.17.101.254]
                          172.31.254.234  0          100        0      bE
         AS_PATH: 4200003000
            L2 Label: 101 L3 Label: 0 (VNI) Router Mac : 0000.0000.0000
         ESI : 00.000000000000000000
3      ND:[0][0201.0101.0102]:[IPv6:1e00:65::1]
                          172.31.254.234  0          100        0      bE
         AS_PATH: 4200003000
            L2 Label: 101 L3 Label: 0 (VNI) Router Mac : 0000.0000.0000
         ESI : 00.000000000000000000
4      ND:[0][887e.25d3.fe0b]:[IPv6:fe80::8a7e:25ff:fed3:fe0b]
                          172.31.254.234  0          100        0      bE
         AS_PATH: 4200003000
            L2 Label: 101 L3 Label: 0 (VNI) Router Mac : 0000.0000.0000
         ESI : 00.000000000000000000
```

show bgp evpn routes rd

Displays information for BGP EVPN routes with the specified route distinguisher (RD).

Syntax

show bgp evpn routes rd *ID*

Parameters

ID

VPM route distinguisher, in the form of ASN:nn or IP-address:nn.

Modes

Privileged EXEC mode

Examples

The following example shows output for the **show bgp evpn routes rd** command.

```
device# show bgp evpn routes rd 2.2.2.2:32770
Status codes: s suppressed, d damped, h history, * valid, > best, i internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network            Next Hop        MED        LocPrf     Weight Path
*>  IMR:[0][IPv4:2.2.2.2]
                          0.0.0.0         0          100        0      ?
*>  ARP:[0][609c.9fde.1215]:[IPv4:2.1.1.1]
                          0.0.0.0         0          100        0      ?
*>  ARP:[0][609c.9fde.1215]:[IPv4:102.1.1.1]
                          0.0.0.0         0          100        0      ?
*>  MAC:[0][609c.9fde.1215]
                          0.0.0.0         0          100        0      ?
```

show bgp evpn routes rd type

Displays information for BGP EVPN routes, filtered based on a specified route type, with the specified route distinguisher (RD).

Syntax

show bgp evpn routes rd *admin-value*:*arbitrary-value* **type** { **auto-discovery** | **ethernet-segment** | **inclusive-multicast** | **ipv4-prefix** | **ipv6-prefix** | **mac** } **detail**

show bgp evpn routes rd *admin-value*:*arbitrary-value* **type auto-discovery esi-value** *value* **ethernet-tag** *tag-id*

show bgp evpn routes rd *admin-value*:*arbitrary-value* **type ethernet-segment esi-value** *value* { **ipv4-address** *address* | **ipv6-address** *address* }

show bgp evpn routes rd *admin-value*:*arbitrary-value* **type inclusive-multicast ethernet-tag** *tag-id* **ipv4-address** *address* [**l2-vni** *number*]

show bgp evpn routes rd *admin-value*:*arbitrary-value* **type ipv4-prefix** *ip address/mask* **tag** *tag-id* [**l3vni** *value*]

show bgp evpn routes rd *admin-value*:*arbitrary-value* **type ipv6-prefix** *ipv6 address/mask* **tag** *tag-id* [**l3vni** *value*]

show bgp evpn routes rd *admin-value*:*arbitrary-value* **type mac** *mac address***ethernet-tag** *tag-id* [**l2-vni** *number*]

show bgp evpn routes rd *admin-value*:*arbitrary-value* **type** [**auto-discovery | igmp-join-sync | igmp-leave-sync**] [**detail**]

Parameters

admin-value

The administrative number assigned to the route. This can be a local ASN number or an IP address. The ASN number can be either a 2-byte number (from 0 through 65535) or a 4-byte number (from 0 through 4294967295).

arbitrary-value

An arbitrary number you choose. The range of valid values is from 0 through 65535 if the ASN is 2 byte, or from 0 through 4294967295 if the ASN is 4 byte.

type

Specifies a route type.

auto-discovery

Specifies automatically discovered routes.

ethernet-segment

Specifies Ethernet Segment (ES) information.

inclusive-multicast

Specifies inclusive multicast information.

ipv4-prefix

Specifies IPv4 prefix information information.

ipv6-prefix

Specifies IPv6 prefix information information.

mac

Specifies Media Access Control (MAC) information.

detail

Displays detailed information.

mac *mac address*

Specifies a MAC address. The valid format is HHHH.HHHH.HHHH.

ethernet-tag *tag-id*

Specifies an Ethenet tag. Valid values range from 1 through 4294967295.

l2-vni *number*

Specifies a layer 2 virtual network identifier (VNI). Valid values range from 1 through 16777215.

esi-value *value*

Specifies a 10 byte Ethernet Segment Identifier (ESI) value in the form of hexadecimal characters (HH.HH.HH.HH.HH.HH.HH.HH.HH.HH).

ipv4-address *address*

Specifies an IPv4 address.

ipv6-address *address*

Specifies an IPv6 address.

ip address/mask

Specifies an IPv4 address and mask.

ipv6 address/mask

Specifies an IPv6 address and mask.

tag *tag-id*

Specifies an Ethenet tag. Valid values range from 1 through 4294967295.

l3vni *value*

Specifies a Layer 3 virtual network identifier (VNIs). Valid values range from 1 through 6777215.

igmp-join-sync

Specifies Join Sync route information.

igmp-leave-sync

Specifies Leave Sync route information.

Modes

Privileged EXEC mode

Examples

The following example shows detailed inclusive multicast information for a BGP EVPN route with the RD 2.2.2.2:32770.

```
device# show bgp evpn routes rd 2.2.2.2:32770 type inclusive-multicast detail
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
1       Prefix: IMR:[0][IPv4:2.2.2.2],  Status: BL,  Age: 0h18m48s
         NEXT_HOP: 0.0.0.0, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community: RT 100:1073741826
            Adj_RIB_out count: 1,  Admin distance 0
            L2 Label: 2 (EVI)
            RD: 2.2.2.2:32770
            As-magic: 47
```

show bgp evpn routes type

Displays EVPN routes in the VPN table by type. Routes are imported into the MAC VRF table if those routes are imported.

Syntax

show bgp evpn routes type arp [*IPv4_address* | **mac** *MAC_address* | **brief** | **detail**]

show bgp evpn routes type auto-discovery [**brief** | **detail** | **esi-value**]

show bgp evpn routes type ethernet-segment [**brief** | **detail** | **esi-value** *ESI*]

show bgp evpn routes type inclusive-multicast [**brief** | **detail** | **ethernet-tag**]

show bgp evpn routes type ipv4-prefix [*IPv4_address/mask* | **brief** | **detail** | **l3-label**]

show bgp evpn routes type ipv6-prefix [*IPv6_address/mask* | **brief** | **detail** | **l3-label**]

show bgp evpn routes type mac [*MAC_address* | **brief** | **detail**]

show bgp evpn routes type nd [*IPv6_address* | **brief** | **detail**]

show bgp evpn routes type igmp-join-sync [**brief** | **detail**]

show bgp evpn routes type igmp-leave-sync [**brief** | **detail**]

Parameters

arp

Specifies ARP details.
IPv4_address

Specifies an IPv4 address in A.B.C.D format.

mac *MAC_address*

Specifies a MAC address in HHHH.HHHH.HHHH format.

brief

Specifies brief information.

detail

Specifies detailed information.

auto-discovery

Specifies auto-discovery details.
esi-value *ESI*

Specifies an Ethernet Segment Indicator in the following hexadecimal format: HH:HH:HH:HH:HH:HH:HH:HH:HH , HH.

ethernet-segment

Specifies Ethernet Segment details.

inclusive-multicast

Specifies inclusive multicast details.
ethernet-tag *tag*

Specifies an Ethernet tag ID. Range is from 0 through 4294967295.

ipv4-prefix *IPv4_address/mask*

Specifies an IPv4 prefix and mask length in A.B.C.D/L format.
l3-label *number*

Specifies a Layer 3 Virtual Network Identifier (VNI). Range is from 1 through 16777215.

ipv6-prefix *IPv6_address/mask*

Specifies an IPv6 prefix and mask length in A:B::C:D/L format.
l3-label *number*

Specifies a Layer 3 Virtual Network Identifier (VNI). Range is from 1 through 16777215.

mac *MAC_address*

Specifies a MAC address in HHHH.HHHH.HHHH format.

nd *IPv6_address*

Specifies a BGP Neighbor Discovery IPv6 address in A:B::C:D format.

igmp-join-sync

Specifies Join Sync route information.

igmp-leave-sync

Specifies Leave Sync route information.

Modes

Privileged EXEC mode

Examples

The following example displays information related to ARP routes.

```
device# show bgp evpn route type arp
Total number of BGP EVPN ARP Routes : 4 Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST
C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix             Next Hop        MED        LocPrf     Weight Status
Route Distinguisher: 40.40.100.50:32869
1      ARP:[0][0000.0a0a.0a0b]:[IPv4:10.10.10.11]
                          0.0.0.0         0          100        0      BL
         AS_PATH:
            L2 Label: 101 L3 Label: 100
         ESI : 00.00000000000000000
2      ARP:[0][609c.9f5a.4715]:[IPv4:15.143.15.1]
                          0.0.0.0         0          100        0      BL
         AS_PATH:
```

```
            L2 Label: 101 L3 Label: 100
          ESI : 00.00000000000000000
Route Distinguisher: 40.40.100.50:33769
3      ARP:[0][609c.9f5a.4715]:[IPv4:14.13.15.1]
                         0.0.0.0         0          100        0      BL
          AS_PATH:
             L2 Label: 1001 L3 Label: 100
          ESI : 00.00000000000000000
Route Distinguisher: 40.40.100.60:32869
4      ARP:[0][609c.9f5a.8d15]:[IPv4:6.6.2.5]
                         40.40.40.2      0          100        0      BE
          AS_PATH: 1000
             L2 Label: 101 L3 Label: 0
          ESI : 00.00000000000000000
```

The following example displays brief information related to IPv4 prefix routes.

```
device# show bgp evpn route type ipv4-prefix detail
Total number of BGP EVPN Ipv4Prefix Routes : 1
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
Route Distinguisher: 100:100
1         Prefix: IP4Prefix:[0][34.0.0.0/24],  Status: BL,  Age: 0h1m5s
          NEXT_HOP: 0.0.0.0, Learned from Peer: Local Router
           LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
          AS_PATH:
             Extended Community:
             RT 100:100
             RT 100:1073742024
             Default Gateway: Received
             Adj_RIB_out count: 1,  Admin distance 0
             L3 Label: 200 (EVI)
             RD: 100:100
             As-magic: 31
```

The following example displays information for inclusive multicast routes.

```
device# show bgp evpn routes type inclusive-multicast
Total number of BGP EVPN IMR Routes : 5
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
Route Distinguisher: 100:100
1         Prefix: IMR:[0][IPv4:2.2.2.2],  Status: BI,  Age: 0h1m21s
          NEXT_HOP: 2.2.2.2, Learned from Peer: 30.0.0.2 (100)
           LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
          AS_PATH:
             Extended Community:
             RT 100:268435656
             RT 100:200
             RT 100:1073742024
             RT 100:100
             PMSI Attribute Flags: 0x00000000  Label-Stack: 200 Tunnel-Type: 6 Tunnel-IP:
2.2.2.2
             Encapsulation Type: Vxlan
             L2 Label: 200 (VNI)
             RD: 100:100
             As-magic: 24
Route Distinguisher: 200:100
2         Prefix: IMR:[0][IPv4:1.1.1.1],  Status: BL,  Age: 0h1m21s
          NEXT_HOP: 0.0.0.0, Learned from Peer: Local Router
           LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
          AS_PATH:
```

```
            Extended Community:
            RT 100:1073742024
            RT 100:100
            Adj_RIB_out count: 1,  Admin distance 0
            L2 Label: 200 (EVI)
            RD: 200:100
            As-magic: 27
Route Distinguisher: 201:100
3         Prefix: IMR:[0][IPv4:1.1.1.1],  Status: BL,  Age: 0h1m50s
         NEXT_HOP: 0.0.0.0, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community:
            RT 100:1073742025
            RT 100:100
            Adj_RIB_out count: 1,  Admin distance 0
            L2 Label: 201 (EVI)
            RD: 201:100
            As-magic: 14
Route Distinguisher: 1.1.1.1:32868
4         Prefix: IMR:[0][IPv4:1.1.1.1],  Status: BL,  Age: 0h1m51s
         NEXT_HOP: 0.0.0.0, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community:
            RT 100:1073741924
            Adj_RIB_out count: 1,  Admin distance 0
            L2 Label: 100 (EVI)
            RD: 1.1.1.1:32868
            As-magic: 2
Route Distinguisher: 2.2.2.2:32868
5         Prefix: IMR:[0][IPv4:2.2.2.2],  Status: BI,  Age: 0h1m21s
         NEXT_HOP: 2.2.2.2, Learned from Peer: 30.0.0.2 (100)
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community:
            RT 100:268435556
            RT 100:100
            RT 100:1073741924
            PMSI Attribute Flags: 0x00000000  Label-Stack: 100 Tunnel-Type: 6 Tunnel-IP:
2.2.2.2
            Encapsulation Type: Vxlan
            L2 Label: 100 (VNI)
            RD: 2.2.2.2:32868
            As-magic: 23
```

The following example displays information for BGP EVPN MAC routes.

```
Peer1#  show bgp evpn route type mac detail
Total number of BGP EVPN MAC Routes : 3
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
Route Distinguisher: 1.1.1.1:32968
1         Prefix: MAC:[0][489b.d57e.c806],  Status: BL,  Age: 0h2m30s
         NEXT_HOP: 0.0.0.0, Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH:
            Extended Community:
            RT 100:1073742024
            Mac Mobility: Sticky Mac
            Default Gateway: Received
            Adj_RIB_out count: 1,  Admin distance 0
            L2 Label: 200 (EVI)
```

```
            ESI : 00.000000000000000000
            RD: 1.1.1.1:32968
            As-magic: 7
Route Distinguisher: 1.1.1.1:32969
2          Prefix: MAC:[0][489b.d57e.c806],  Status: BL,  Age: 0h2m30s
          NEXT_HOP: 0.0.0.0, Learned from Peer: Local Router
           LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
          AS_PATH:
            Extended Community:
            RT 100:1073742025
            Mac Mobility: Sticky Mac
            Default Gateway: Received
            Adj_RIB_out count: 1,  Admin distance 0
            L2 Label: 201 (EVI)
            ESI : 00.000000000000000000
            RD: 1.1.1.1:32969
            As-magic: 11
Route Distinguisher: 2.2.2.2:32968
3          Prefix: MAC:[0][489b.d57f.a406],  Status: BI,  Age: 0h2m1s
          NEXT_HOP: 2.2.2.2, Learned from Peer: 30.0.0.2 (100)
           LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
          AS_PATH:
            Extended Community:
            RT 100:268435656
            RT 100:200
            RT 100:1073742024
            Mac Mobility: Sticky Mac
            Default Gateway: Received
            Encapsulation Type: Vxlan
            L2 Label: 200 (VNI)
            ESI : 00.000000000000000000
            RD: 2.2.2.2:32968
            As-magic: 22
```

The following example displays information for BGP EVPN Auto Discovered routes.

```
Peer1#  show system internal bgp evpn route type auto-discovery

Total number of BGP EVPN AD Routes : 6
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
Route Distinguisher: 1.1.1.1:1
1          Prefix: AD:[01.609c9f871e00000100][4294967295],  Status: bE,  Age: 0h9m20s
          NEXT_HOP: 1.1.1.1, Learned from Peer: 30.1.1.2 (100)
           LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
          AS_PATH: 100
            Extended Community:
            RT 100:101
            RT 100:1073741926
            ESI Label Ext Community: 0  All-Active (0x00000000)
            Encapsulation Type: Vxlan
            Adj_RIB_out count: 2,  Admin distance 20
            RD: 1.1.1.1:1
          Received from: 30.1.1.2(100), AsPath_Addr: 0xc2f7ead3 Nh_Addr: 0xc2e81064
Nlri_Addr: 0xc2efea44
          route_is_vpn 1, Par_Nlri: 0x00000000 , Prev_Nlri: 0x00000000 Next_Nlri:
0x00000000 nlts 00000999 bc : 0
          evpn_label_info : t:3, e:2, 1:0 2:0 evid:12288 ESI : 12.01b8207f0000000029
  evpn node nne 1,nnr 0,aa 0,rp 0, dp 0,pp 0,rp 0, vp 0,d 0,nm 0,lsl 0,vpn 1,recap 0,dd
0,pi 0, gid 0, eviid 0,nhid 0,elts 00000000,nhid_node 00007f20
            As-magic: 29
Route Distinguisher: 1.1.1.1:134
2          Prefix: AD:[01.609c9f871e00000100][0],  Status: bE,  Age: 0h9m20s
```

```
         NEXT_HOP: 1.1.1.1, Learned from Peer: 30.1.1.2 (100)
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 100
            Extended Community:
            RT 100:101
            ESI Label Ext Community: 0  All-Active (0x00000000)
            Encapsulation Type: Vxlan
            Adj_RIB_out count: 2,  Admin distance 20
            RD: 1.1.1.1:134
         Received from: 30.1.1.2(100), AsPath_Addr: 0xc2f7e45b Nh_Addr: 0xc2e81064
Nlri_Addr: 0xc2efe494
         route_is_vpn 1, Par_Nlri: 0x00000000 , Prev_Nlri: 0x00000000 Next_Nlri:
0x00000000 nlts 00000999 bc : 0
         evpn_label_info : t:3, e:2, 1:101 2:0 evid:12288 ESI : 12.01b8207f0000a01301
  evpn node nne 1,nnr 0,aa 0,rp 0, dp 0,pp 0,rp 0, vp 0,d 0,nm 0,lsl 0,vpn 1,recap 0,dd
0,pi 0, gid 0, eviid 0,nhid 0,elts 00000000,nhid_node 00007f20
            As-magic: 26
Route Distinguisher: 1.1.1.1:135
3          Prefix: AD:[01.609c9f871e00000100][0],  Status: bE,  Age: 0h9m20s
         NEXT_HOP: 1.1.1.1, Learned from Peer: 30.1.1.2 (100)
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 100
            Extended Community:
            RT 100:1073741926
            ESI Label Ext Community: 0  All-Active (0x00000000)
            Encapsulation Type: Vxlan
            Adj_RIB_out count: 2,  Admin distance 20
            RD: 1.1.1.1:135
         Received from: 30.1.1.2(100), AsPath_Addr: 0xc2f7e935 Nh_Addr: 0xc2e81064
Nlri_Addr: 0xc2efe8d8
         route_is_vpn 1, Par_Nlri: 0x00000000 , Prev_Nlri: 0x00000000 Next_Nlri:
0x00000000 nlts 00000999 bc : 0
         evpn_label_info : t:3, e:2, 1:102 2:0 evid:12288 ESI : 12.01b8207f000000003e
  evpn node nne 1,nnr 0,aa 0,rp 0, dp 0,pp 0,rp 0, vp 0,d 0,nm 0,lsl 0,vpn 1,recap 0,dd
0,pi 0, gid 0, eviid 0,nhid 0,elts 00000000,nhid_node 00007f20
            As-magic: 27
Route Distinguisher: 2.2.2.2:1
4          Prefix: AD:[01.609c9f871e00000100][4294967295],  Status: bE,  Age: 0h9m20s
         NEXT_HOP: 2.2.2.2, Learned from Peer: 20.1.1.2 (100)
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 100
            Extended Community:
            RT 100:101
            RT 100:1073741926
            ESI Label Ext Community: 0  All-Active (0x00000000)
            Encapsulation Type: Vxlan
            Adj_RIB_out count: 2,  Admin distance 20
            RD: 2.2.2.2:1
         Received from: 20.1.1.2(100), AsPath_Addr: 0xc2f7e1ee Nh_Addr: 0xc2e7f85a
Nlri_Addr: 0xc2efe272
         route_is_vpn 1, Par_Nlri: 0x00000000 , Prev_Nlri: 0x00000000 Next_Nlri:
0x00000000 nlts 00000990 bc : 0
         evpn_label_info : t:3, e:2, 1:0 2:0 evid:12288 ESI : 12.01b8207f0000000029
  evpn node nne 1,nnr 0,aa 0,rp 0, dp 0,pp 0,rp 0, vp 0,d 0,nm 0,lsl 0,vpn 1,recap 0,dd
0,pi 0, gid 0, eviid 0,nhid 0,elts 00000000,nhid_node 00007f20
            As-magic: 21
Route Distinguisher: 2.2.2.2:134
5          Prefix: AD:[01.609c9f871e00000100][101],  Status: bE,  Age: 0h9m20s
         NEXT_HOP: 2.2.2.2, Learned from Peer: 20.1.1.2 (100)
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 100
            Extended Community:
            RT 100:101
            ESI Label Ext Community: 0  All-Active (0x00000000)
```

```
            Encapsulation Type: Vxlan
            Adj_RIB_out count: 2,  Admin distance 20
            RD: 2.2.2.2:134
         Received from: 20.1.1.2(100), AsPath_Addr: 0xc2f7ed40 Nh_Addr: 0xc2e7f85a
Nlri_Addr: 0xc2efec66
         route_is_vpn 1, Par_Nlri: 0x00000000 , Prev_Nlri: 0x00000000 Next_Nlri:
0x00000000 nlts 00000990 bc : 0
         evpn_label_info : t:3, e:2, 1:101 2:0 evid:12288 ESI : 12.01b8207f0000b81301
  evpn node nne 1,nnr 0,aa 0,rp 0, dp 0,pp 0,rp 0, vp 0,d 0,nm 0,lsl 0,vpn 1,recap 0,dd
0,pi 0, gid 0, eviid 0,nhid 0,elts 00000000,nhid_node 00007f20
            As-magic: 17
Route Distinguisher: 2.2.2.2:135
6         Prefix: AD:[01.609c9f871e00000100][102],  Status: bE,  Age: 0h9m20s
         NEXT_HOP: 2.2.2.2, Learned from Peer: 20.1.1.2 (100)
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 100
            Extended Community:
            RT 100:1073741926
            ESI Label Ext Community: 0  All-Active (0x00000000)
            Encapsulation Type: Vxlan
            Adj_RIB_out count: 2,  Admin distance 20
            RD: 2.2.2.2:135
         Received from: 20.1.1.2(100), AsPath_Addr: 0xc2f7e5f9 Nh_Addr: 0xc2e7f85a
Nlri_Addr: 0xc2efe600
         route_is_vpn 1, Par_Nlri: 0x00000000 , Prev_Nlri: 0x00000000 Next_Nlri:
0x00000000 nlts 00000990 bc : 0
         evpn_label_info : t:3, e:2, 1:102 2:0 evid:12288 ESI : 12.01b8207f000000003e
  evpn node nne 1,nnr 0,aa 0,rp 0, dp 0,pp 0,rp 0, vp 0,d 0,nm 0,lsl 0,vpn 1,recap 0,dd
0,pi 0, gid 0, eviid 0,nhid 0,elts 00000000,nhid_node 00007f20
            As-magic: 18
```

The following example displays information of BGP EVPN routes of the type *ethernet-segment*.

```
Peer1#  show system internal bgp evpn route type ethernet-segment
Total number of BGP EVPN Ethernet Segment Routes : 2
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
Route Distinguisher: 1.1.1.1:1
1         Prefix: ESR:[01.609c9f.871e00.000100][IPv4:1.1.1.1],  Status: bE,  Age: 0h16m21s
         NEXT_HOP: 1.1.1.1, Learned from Peer: 30.1.1.2 (100)
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 100
            Extended Community:
            DF Election Ext Community: AC-influenced-DF-election: Enabled
            ES Import RT: 06:02:60:9c:9f:87:1e:00
            Encapsulation Type: Vxlan
            Adj_RIB_out count: 2,  Admin distance 20
            RD: 1.1.1.1:1
         Received from: 30.1.1.2(100), AsPath_Addr: 0xc2f7ea04 Nh_Addr: 0xc2e81064
Nlri_Addr: 0xc2efe98e
         route_is_vpn 1, Par_Nlri: 0x00000000 , Prev_Nlri: 0x00000000 Next_Nlri:
0x00000000 nlts 00000999 bc : 0
         evpn_label_info : t:3, e:2, 1:65793 2:0 evid:12288 ESI : 12.01b8207f000000003e
  evpn node nne 1,nnr 0,aa 0,rp 0, dp 0,pp 0,rp 0, vp 0,d 0,nm 0,lsl 0,vpn 1,recap 0,dd
0,pi 0, gid 0, eviid 0,nhid 0,elts 00000000,nhid_node 00214e00
            As-magic: 28
Route Distinguisher: 2.2.2.2:1
2         Prefix: ESR:[01.609c9f.871e00.000100][IPv4:2.2.2.2],  Status: bE,  Age: 0h16m21s
         NEXT_HOP: 2.2.2.2, Learned from Peer: 20.1.1.2 (100)
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: incomplete,  Weight: 0
         AS_PATH: 100
            Extended Community:
```

```
            DF Election Ext Community: AC-influenced-DF-election: Enabled
            ES Import RT: 06:02:60:9c:9f:87:1e:00
            Encapsulation Type: Vxlan
            Adj_RIB_out count: 2,  Admin distance 20
            RD: 2.2.2.2:1
         Received from: 20.1.1.2(100), AsPath_Addr: 0xc2f7e6c8 Nh_Addr: 0xc2e7f85a
Nlri_Addr: 0xc2efe6b6
         route_is_vpn 1, Par_Nlri: 0x00000000 , Prev_Nlri: 0x00000000 Next_Nlri:
0x00000000 nlts 00000990 bc : 0
         evpn_label_info : t:3, e:2, 1:131586 2:0 evid:12288 ESI : 12.01b8207f0000000029
  evpn node nne 1,nnr 0,aa 0,rp 0, dp 0,pp 0,rp 0, vp 0,d 0,nm 0,lsl 0,vpn 1,recap 0,dd
0,pi 0, gid 0, eviid 0,nhid 0,elts 00000000,nhid_node f9001c00
            As-magic: 19
```

show bgp evpn routes type igmp-join-sync

Displays information for BGP EVPN routes to join IGMP sync.

Syntax

show bgp evpn routes type igmp-join-sync

show bgp evpn routes type igmp-join-sync brief

show bgp evpn routes type igmp-join-sync detail

Parameters

brief

Displays summary information.

detail

Displays detailed information.

Modes

Privileged EXEC mode

Examples

The following example shows routes to join IGMP sync:

```
Total number of BGP EVPN Igmp Join Sync Routes : 2
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix             Next Hop        MED        LocPrf     Weight Status
Route Distinguisher: 19.1.2.3:32868
1      IGMPJoinSyncPrefix4:[0](100.1.2.3,234.1.2.3):19.1.2.3 (esi 00.010203040506070809)
                           19.1.2.3        0          100        0      BI
         AS_PATH:
2      IGMPJoinSyncPrefix6:[0](2001::4,ff03::1):19.1.2.3 (esi 02.010203040506070809)
                           19.1.2.3        0          100        0      BI
         AS_PATH:
```

show bgp evpn routes type igmp-leave-sync

Displays BGP EVPN routes to leave IGMP sync.

Syntax

show bgp evpn routes type igmp-leave-sync

show bgp evpn routes type igmp-leave-sync brief

show bgp evpn routes type igmp-leave-sync detail

Parameters

brief

Displays summary information.

detail

Displays detailed information.

Modes

Privileged EXEC mode

Examples

The following example shows routes to leave IGMP sync:

```
Total number of BGP EVPN Igmp Leave Sync Routes :
2
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP
D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-
MULTIPATH
       S:SUPPRESSED F:FILTERED
s:STALE

       Prefix             Next Hop        MED        LocPrf     Weight
Status
Route Distinguisher:
19.1.2.3:32868

1      IGMPLeaveSyncPrefix4:[0](101.1.2.3,235.1.2.3):19.1.2.3 (esi
01.010203040506070809)
                          19.1.2.3        0          100        0
BI
         AS_PATH:
2      IGMPLeaveSyncPrefix6:[0](2002::5,ff04::3):19.1.2.3 (esi 03.010203040506070809)
                          19.1.2.3        0          100        0      BI
         AS_PATH:
```

show bgp evpn routes unreachable

Displays route information about BGP EVPN routes whose destinations are unreachable through any of the paths in the BGP EVPN route table.

Syntax

show bgp evpn routes unreachable [**type** { **igmp-join-sync** | **igmp-leave-sync** }]

Parameters

type

Specifies the type of route.

igmp-join-sync

Specifies Join Sync routes.

igmp-leave-sync

Specifies Leave Sync routes.

Modes

Privileged EXEC mode

This example shows the status of bgp evpn routes unreachable.

```
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix             Next Hop        MED        LocPrf     Weight RPKI State Status
1      IMR:[0][IPv4:172.31.254.234]
                          172.31.254.234  0          100        0      bE
         AS_PATH: 4200003000
         L2 Label: 101 (VNI)
2      ARP:[0][0201.0101.0101]:[IPv4:172.17.101.254]
                          172.31.254.234  0          100        0      bE
         AS_PATH: 4200003000
            L2 Label: 101 L3 Label: 0 (VNI) Router Mac : 0000.0000.0000
         ESI : 00.000000000000000000
3      ND:[0][0201.0101.0102]:[IPv6:1e00:65::1]
                          172.31.254.234  0          100        0      bE
         AS_PATH: 4200003000
            L2 Label: 101 L3 Label: 0 (VNI) Router Mac : 0000.0000.0000
         ESI : 00.000000000000000000
4      ND:[0][887e.25d3.fe0b]:[IPv6:fe80::8a7e:25ff:fed3:fe0b]
                          172.31.254.234  0          100        0      bE
         AS_PATH: 4200003000
            L2 Label: 101 L3 Label: 0 (VNI) Router Mac : 0000.0000.0000
         ESI : 00.000000000000000000
```

show bgp evpn summary

Displays the EVPN neighbors configured on the router, including how many routes have been received, sent, and filtered.

Syntax

show bgp evpn summary

Modes

Privileged EXEC mode

Examples

The following example displays summarized information for EVPN neighbors.

```
device# show bgp evpn summary
  BGP4 Summary
  Router ID: 3.3.100.3   Local AS Number: 100
  Confederation Identifier: not configured
  Confederation Peers:
  Maximum Number of IP ECMP Paths Supported for Load Sharing: 1
  Number of Neighbors Configured: 3, UP: 2
  Number of Routes Installed: 5, Uses 625 bytes
  Number of Routes Advertising to All Neighbors: 6 (2 entries), Uses 120 bytes
  Number of Attribute Entries Installed: 7, Uses 805 bytes
  '+': Data in InQueue '>': Data in OutQueue '-': Clearing
  '*': Update Policy 'c': Group change 'p': Group change Pending
  'r': Restarting 's': Stale '^': Up before Restart '<': EOR waiting
  Neighbor Address  AS#         State     Time     Rt:Accepted Filtered Sent     ToSend
  4.4.100.4         100         ESTAB     0h 4m49s    2        0        2        0
```

show bgp ip flowspec

Displays Border Gateway Protocol flow specification (BGP flowspec) configuration information.

Syntax

show bgp ip flowspec

show bgp ip flowspec attribute-entries

show bgp ip flowspec routes [*asn-number* | **age** | **best** | **detail** | **local** | **neighbor** | **no-best** | **not-installed-best** | **summary** | **vrf** *vrf-name*]

show bgp ip flowspec summary

Parameters

attribute-entries

Specifes the the display of AS-path attribute-entry information for BGP flowspec.

routes

Specifies the display of route configuration information for BGP flowspec.
asn-number

Displays route information starting from the specified autonomous system number (ASN). The range od from 1 through 4294967295.

age

Displays recently updated route information.

best

Displays information about routes that are selected as best routes.

detail

Displays detailed route information.

local

Displays information about selected local routes.

neighbor

Displays routes from BGP neighbors.

no-best

Displays information about routes that do not have a best path.

not-installed-best

Displays best routes that are not installed in the IP route table.

summary

Displays summary information for BGP flowspec routes.

vrf *vrf-name*

Displays route information for the specified VRF instance.

summary

Specifies the display of summary information for BGP flowspec.

Modes

Privileged EXEC mode

Usage Guidelines

For a flowspec route (which is a combination of all match components), specify the **detail** option to display all match components and traffic actions. When the **detail** option is not specified, traffic-action configuration information is not displayed and only a limited length of match component imformation is displayed for the route.

Examples

The following example shows output from the **show bgp ip flowspec routes** command.

```
device# show bgp ip flowspec routes

Total number of BGP Routes: 1
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Flowspec                                                              MED
LocPrf  Weight Status
1       Dst:91.92.93.0/24 Src:81.82.83.0/24 Protocol:!=56|=34 Port:>=500...      0
100     32768  BL
         AS_PATH:
```

The following example shows summary information for the **show bgp ip flowspec routes** command.

```
device# show bgp ip flowspec routes summary

  Total number of BGP routes (NLRIs) Installed       : 2
  Distinct BGP destination networks                  : 2
  Filtered bgp routes for soft reconfig              : 0
  Routes originated by this router                   : 0
  Routes selected as BEST routes                     : 2
  Routes Installed as BEST routes                    : 2
  BEST routes not installed in IP forwarding table   : 0
  Static routes not installed in IP forwarding table : 0
  Unreachable routes (no IGP route for NEXTHOP)      : 0
  IBGP routes selected as best routes                : 0
  EBGP routes selected as best routes                : 2
  BEST routes not valid for IP forwarding table      : 0
```

show bgp ip flowspec neighbors

Displays Border Gateway Protocol flow specification (BGP flowspec) neighbor configuration information.

Syntax

show bgp ip flowspec neighbors

show bgp ip flowspec neighbors *ip-address* **advertised-routes**

show bgp ip flowspec neighbors *ip-address* **rib-out-routes**

show bgp ip flowspec neighbors *ip-address* **routes** [**best** | **detail** | **not-installed-best** | **vrf** *vrf-name*

show bgp ip flowspec neighbors routes-summary

show bgp ip flowspec neighbors vrf *vrf-name* }

Parameters

ip-address

Specifes the IP address (in IPv4 format) of a BGP flowspec neighbor.

advertised-routes

Displays information about routes advertised to the neighbor.

rib-out-routes

Displays information about RIB-out routes for the neighbor.

routes

Causes the display of information about routes learned from the neighbor.

best

Displays information about routes that are selected as best routes.

detail

Displays detailed information about routes that are learned from the neighbor.

not-installed-best

Displays information about best routes that are not installed in the IP route table.

vrf *vrf-name*

Displays information about routes that are learned from the neighbor for the specified VRF instance.

routes-summary

Displays summary information for routes learned from a neighbor.

vrf *vrf-name*

Displays information for BGP flowspec neighbors for the specified VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

Examples

The following example displays detailed RIB-out route information for a BGP flowspec neighbor (10.61.61.1).

```
device# show bgp ip flowspec neighbors 10.61.61.1 rib-out-routes detail

      There are 1 RIB_out routes for neighbor 10.61.61.1
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
1    Flowspec: Dst:10.92.93.0/24 Src:10.82.83.0/24 Protocol:!=56|=34 Port:>=5000&<=6000
DPort:=76|<899 SPort:>89
          ICMP-type: =56 ICMP-code:!=4 TCP-flags:(match)(ACK&SYN) Pkt-length:!=788
DSCP:=45|=44
    Fragment:!(LF|FF)
         Status: BL,  Age: 0h20m19s
         Learned from Peer: Local Router
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: igp,  Weight: 32768
         AS_PATH:
            Extended Community:
            Flowspec Extended Community: Redirect IP NH(0x0800):(redirect)5.6.7.8
Redirect IP NH(0x0800):(mirror)7.8.9.3
                                        Traffic-rate:asn 666,rate 5625000 bytes/sec
                                        Traffic-remarking(DSCP):32 Traffic-
action:terminal-action,sample
            Adj_RIB_out count: 3,  Admin distance 1
```

show bgp ip neighbor ipv6

Displays configuration information and statistics for IPv6 neighbors that are configured under IPv4 address family.

Syntax

show bgp ip neigbor ipv6 { **all** | **last-packet-with-error** | **routes-summary** }

show bgp ip neighbor ipv6 *ipv6-addr* [**flap-statistics** | **last-packet-with-error** [**decode**] | **received prefix-filter**]

show bgp ip neighbor ipv6 *ipv6-addr* { **advertised-routes** | **received-routes** | **rib-out-routes** } [**detail**]

show bgp ip neighbor ipv6 *ipv6-addr* **routes** { **best** | **detail** [**best** | **not-installed-best** | **unreachable**] | **not-installed-best** | **unreachable** }

show bgp ip neighbor ipv6 *ipv6-addr* **routes-summary**

Parameters

advertised-routes

Specifies the display of information about routes advertised to the BGP4+ neighbor in the current session.

detail

Specifies the display of detailed information.

all

Specifies the display of information about all routes advertised to the BGP4+ neighbor in the current session.

flap-statistics

Specifies the display of route flap statistics for routes received from or sent to a BGP4+ neighbor.

last-packet-with-error

Specifies the display of information about the last packet that contained an error received from any device neighbor.

decode

Specifies decoding the packet.

received-routes

Specifies the display of route information received from BGP4 neighbors in the current session.

detail

Specifies the display of detailed information.

rib-out-routes

Specifies the display of information about BGP4 outbound RIB routes.

detail

Specifies the display of detailed information.

routes

best

Specifies the display of information about routes received from the neighbor that are the best BGP4+ routes to their destination.

detail

Specifies the display of detailed information.

best

Specifies the display of information about routes received from the neighbor that are the best BGP4+ routes to their destination.

not-installed-best

Specifies the display of information about routes received from the BGP4+ neighbor that are the best BGP4+ routes to their destination and that were not installed in the route table because the device received better routes from other sources.

unreachable

Specifies the display of information about routes that are unreachable because the device does not have a valid RIP, OSPF, or static route to the next hop.

Modes

Privileged EXEC mode

Examples

The following example shows configuration information and statistics for an IPv6 neighbor that is configured under an IPv4 address family.

```
show bgp ip neighbors ipv6 2000::1

  '+': Data in InQueue '>': Data in OutQueue '-': Clearing
  '*': Update Policy 'c': Group change 'p': Group change Pending
  'r': Restarting 's': Stale '^': Up before Restart '<': EOR waiting

1 IP Address: 2000::1 , AS: 1 (EBGP), RouterID: 10.1.1.1, VRF: default-vrf
  State: ESTABLISHED, Time: 0h0m50s, KeepAliveTime: 60, HoldTime: 180
  KeepAliveTimer Expire in 15 seconds, HoldTimer Expire in 144 seconds
  Minimal Route Advertisement Interval: 0 seconds
  RefreshCapability: Received

Messages:  Open  Update KeepAlive  Notification  Refresh-Req
Sent :       1     1      1          0             0
Received:    1     1      1          0             0

Last Update Time: NLRI  Withdraw NLRI Withdraw
Tx: 0h0m33s  ---  Rx: 0h0m35s  ---

Last Connection Reset Reason:Unknown
Notification Sent:     Unspecified
Notification Received: Unspecified
Neighbor NLRI Negotiation:
 Peer Negotiated IPV4 unicast capability
```

```
 Peer configured for IPV4 unicast Routes
Neighbor ipv6 MPLS Label Capability Negotiation:
Neighbor AS4 Capability Negotiation:
Outbound Policy Group:
 ID: 2, Use Count: 1
BFD:Disabled
 Byte Sent: 159, Received: 159
 Local host: 2000::2, Local Port: 179
 Remote host: 2000::1 , Remote Port: 8042
```

show bgp ip summary ipv6

Displays summary configuration information and statistics for IPv6 neighbors that are configured under IPv4 address family.

Syntax

show bgp ip summary ipv6

Modes

Privileged EXEC mode

Examples

The following example displays summary configuration information and statistics for IPv6 neighbors that are configured under an IPv4 address family.

```
device# show bgp ip summary ipv6

BGP4 Summary
Router ID: 10.1.1.1   Local AS Number: 1
Confederation Identifier: not configured
Confederation Peers:
Maximum Number of IP ECMP Paths Supported for Load Sharing: 1
Number of Neighbors Configured: 1, UP: 1
Number of Routes Installed: 0
Number of Routes Advertising to All Neighbors: 0 (0 entries)
Number of Attribute Entries Installed: 0

*Dynamically created based on a listen range command
Dynamically created neighbors: 0/100(max)
A: Auto Discovered Neighbors using LLDP
Auto Neighbors Count: 0
'+': Data in InQueue '>': Data in OutQueue '-': Clearing
'*': Update Policy 'c': Group change 'p': Group change Pending
'r': Restarting 's': Stale '^': Up before Restart '<': EOR waiting

Neighbor Address  AS#        State     Time     Rt:Accepted Filtered Sent ToSend
2000::2           2          ESTAB     0h0m0s     0           0       0    0
```

show ip/ipv6 bgp peer-dampened

Displays the list of dampened peers. Both IPv4 and IPv6 peers are shown. This command also shows the current values for the *Idle Hold*, *Idle Hold Timer*, and *Stability Interval* timer values.

Syntax

show { **ip** | **ipv6** } **bgp peer-dampened [detail]** [**all-vrfs** | **vrf** *vrf-name*]

Parameters

{ *ip* | *ipv6* }

The address family for which the peer dampening information is required.

all-vrfs

Show the peer dampening information for all VRFs.

vrf *vrf-name*

Show the peer dampening information for the VRF specified in the *vrf-name* parameter.

detail Show the peer dampening information in detail including delay-hold and penalty.

Modes

Global Executable Mode

Usage Guidelines

- The *Idle-hold-Timer* column of the output displays the time remaining to move to next state.
- The *Idle-hold* column of the output displays the time the neighbor will stay in the idle state.
- The *Stability-interval* column of the output displays the time the session must remain error-free to be considered stable.
- The *Delay-hold* column output displays the time assigned to the *Idle-hold-Timer* for the first peer-flap event received.
- The *Penalty* column of the output displays the time added to *Idle-hold-Timer* for the second and more peer-flap event received.

Examples

The following command example displays a list of all dampened BGP peers (IPv4) on all VRFs.

```
leaf-1# show ip bgp peer-dampened all-vrfs
------------------------------------------------------------------------------------
                VRF - default vrf
```

```
-------------------------------------------------------------------------------------
Total number of BGP Neighbors: 1
Neighbor    Idle-hold-Timer     Idle-Hold   Stability-interval
50.1.1.2       03                 15          30
```

The following command example displays a list of all dampened BGP peers (IPv6) on all VRFs.

```
leaf-1#  show ipv6 bgp peer-dampened all-vrfs
-------------------------------------------------------------------------------------
               VRF - default vrf
-------------------------------------------------------------------------------------
Total number of BGP Neighbors: 1
Neighbor        Idle-hold-Timer     Idle-Hold  Stability-interval
200:1:1:1:1::1     06                  15         30
```

The following example displays **show ip bgp peer-dampened detail all-vrfs**

```
leaf-1# show ip bgp peer-dampened detail all-vrfs
-------------------------------------------------------------------------
            VRF: default-vrf
-------------------------------------------------------------------------
Total number of BGP Neighbors:1
Neighbor     Idle-hold-Timer  Idle-Hold  Stability-interval  delay-hold  penalty
50.1.12           3          15           30         10      10
leaf-1#
```

The following example displays **show ipv6 bgp peer-dampened detail all-vrfs**

```
leaf-1# show ipv6 bgp peer-dampened detail all-vrfs
-------------------------------------------------------------------------
            VRF: default-vrf
-------------------------------------------------------------------------
Total number of BGP Neighbors:1
Neighbor      Idle-hold-Timer  Idle-Hold  Stability-interval  delay-hold  penalty
200.1.1.1.1::1    3           15        30         10      10
leaf-1#
```

show bmc config-history

Displays a log of all the configuration changes made to BMC using the command line interface. The last 40 entries are listed.

Syntax

show bmc config-history

Parameters

None

Modes

Privileged EXEC Mode

Usage Guidelines

None

Examples

The following example displays the output of the **show bmc config-history** command.

```
 SLX # show bmc config-history

================================
BMC config-history
================================
     1  Event: bmc_set_static_ipaddr IPv4 addressStart time: Mon Oct 28 14:49:02 2024  Duration:
3.4693e-05s    Status: Initiated
     2  Event: bmc_set_static_ipaddr netmaskStart time: Mon Oct 28 14:49:02 2024  Duration:
3.3913e-05s    Status: Initiated
     3  Event: bmc_set_static_ipaddr gatewayStart time: Mon Oct 28 14:49:02 2024  Duration:
4.1044e-05s    Status: Initiated
     4  Event: bmc_set_static_ipaddr Start time: Mon Oct 28 14:49:02 2024  Duration: 3.4622e-05s
Status: Initiated
     5  Event: bmc_set_static_ipaddr Start time: Mon Oct 28 14:49:02 2024  Duration: 3.3244e-05s
Status: Initiated
     6  Event: check10TimesBmcLanReadyStart time: Mon Oct 28 14:49:02 2024  Duration: 3.306e-05s
Status: Initiated
     7  Event: check10TimesBmcLanReadyStart time: Mon Oct 28 14:49:03 2024  Duration: 7.6561e-05s
Status: Success
     8  Event: bmc_set_static_ipaddr IPSrc StaticStart time: Mon Oct 28 14:49:03 2024  Duration:
3.5352e-05s    Status: Initiated
     9  Event: bmc_set_static_ipaddr IPv4 addressStart time: Mon Oct 28 14:49:03 2024  Duration:
3.3281e-05s    Status: Initiated
    10  Event: setBmcLanAddrCmd      Start time: Mon Oct 28 14:49:03 2024  Duration: 3.2997e-05s
Status: Initiated
    11  Event: setBmcLanAddrCmd      Start time: Mon Oct 28 14:49:12 2024  Duration: 9.4659e-05s
Status: Success
    12  Event: check10TimesBmcLanReadyStart time: Mon Oct 28 14:49:12 2024  Duration: 3.4097e-05s
Status: Initiated
    13  Event: check10TimesBmcLanReadyStart time: Mon Oct 28 14:49:48 2024  Duration: 9.9227e-05s
```

```
Status: Success
    14  Event: bmc_set_static_ipaddr IPv4 addressStart time: Mon Oct 28 14:49:48 2024  Duration:
3.3211e-05s    Status: Success
    15  Event: bmc_set_static_ipaddr netmaskStart time: Mon Oct 28 14:49:48 2024  Duration:
3.6361e-05s    Status: Initiated
    16  Event: bmc_set_static_ipaddr gatewayStart time: Mon Oct 28 14:49:48 2024  Duration:
4.3865e-05s    Status: Initiated
    17  Event: setBmcLanAddrCmd      Start time: Mon Oct 28 14:49:48 2024  Duration: 3.5976e-05s
Status: Initiated
    18  Event: setBmcLanAddrCmd      Start time: Mon Oct 28 14:50:01 2024  Duration: 0.000100956s
Status: Success
    19  Event: check10TimesBmcLanReadyStart time: Mon Oct 28 14:50:01 2024  Duration: 3.675e-05s
Status: Initiated
    20  Event: check10TimesBmcLanReadyStart time: Mon Oct 28 14:50:37 2024  Duration: 0.000102784s
Status: Success
    21  Event: bmc_set_static_ipaddr gatewayStart time: Mon Oct 28 14:50:37 2024  Duration:
3.3318e-05s    Status: Success
    22  Event: bmc_set_static_ipaddr Start time: Mon Oct 28 14:50:37 2024  Duration: 3.4294e-05s
Status: Initiated
    23  Event: bmc_set_static_ipaddr Start time: Mon Oct 28 15:13:04 2024  Duration: 0.000252519s
Status: Initiated
    24  Event: check10TimesBmcLanReadyStart time: Mon Oct 28 15:13:04 2024  Duration: 3.8538e-05s
Status: Initiated
    25  Event: check10TimesBmcLanReadyStart time: Mon Oct 28 15:13:04 2024  Duration: 8.617e-05s
Status: Success
    26  Event: bmc_set_static_ipaddr IPSrc StaticStart time: Mon Oct 28 15:13:04 2024  Duration:
3.5873e-05s    Status: Initiated
    27  Event: bmc_set_static_ipaddr IPv4 addressStart time: Mon Oct 28 15:13:04 2024  Duration:
3.6586e-05s    Status: Initiated
    28  Event: setBmcLanAddrCmd      Start time: Mon Oct 28 15:13:04 2024  Duration: 5.0485e-05s
Status: Initiated
    29  Event: setBmcLanAddrCmd      Start time: Mon Oct 28 15:13:19 2024  Duration: 0.000101873s
Status: Success
    30  Event: check10TimesBmcLanReadyStart time: Mon Oct 28 15:13:19 2024  Duration: 3.4795e-05s
Status: Initiated
    31  Event: check10TimesBmcLanReadyStart time: Mon Oct 28 15:13:56 2024  Duration: 9.9378e-05s
Status: Success
    32  Event: bmc_set_static_ipaddr IPv4 addressStart time: Mon Oct 28 15:13:56 2024  Duration:
3.3801e-05s    Status: Success
    33  Event: bmc_set_static_ipaddr netmaskStart time: Mon Oct 28 15:13:56 2024  Duration:
3.5064e-05s    Status: Initiated
    34  Event: bmc_set_static_ipaddr gatewayStart time: Mon Oct 28 15:13:56 2024  Duration:
3.3555e-05s    Status: Initiated
    35  Event: setBmcLanAddrCmd      Start time: Mon Oct 28 15:13:56 2024  Duration: 3.559e-05s
Status: Initiated
    36  Event: setBmcLanAddrCmd      Start time: Mon Oct 28 15:14:29 2024  Duration: 0.000100428s
Status: Failed
    37  Event: check10TimesBmcLanReadyStart time: Mon Oct 28 15:14:29 2024  Duration: 3.4931e-05s
Status: Initiated
    38  Event: check10TimesBmcLanReadyStart time: Mon Oct 28 15:15:05 2024  Duration: 8.1208e-05s
Status: Success
    39  Event: bmc_set_static_ipaddr gatewayStart time: Mon Oct 28 15:15:05 2024  Duration:
3.347e-05s    Status: Success
    40  Event: bmc_set_static_ipaddr Start time: Mon Oct 28 15:15:05 2024  Duration: 3.3878e-05s
Status: Initiated
```

show bmc interface management status

Shows the current status of the selected BMC Management Interface.

Syntax

show bmc interface management *interface-number* **status**

Parameters

interface-number

The BMC Management Interface ID. Only interface ID 0 is supported.

Modes

Privileged EXEC Mode

Usage Guidelines

Displays the status of the SOHO port connected to BMC.

This command requires about 15 seconds to refresh after a **shutdown** or **no shutdown** command is run on the BMC Management Interface. Till this time BMC might report incorrect status.

Examples

The following example shows the output of the command when the interface is enabled.

```
SLX # show bmc interface management 0 status
Status: Enabled
```

The following example shows the output of the command when the interface is not accessible.

```
SLX # show bmc interface management 0 status
Status: Disabled
```

show bmc interface management ip

Displays the configured IP for the selected BMC Management Interface.

Syntax

show bmc interface management *interface-number* **ip**

Parameters

interface-number

Displays the configured IPv4 address information for the selected management interface. Only interface with ID 0 is supported.

Modes

Privileged EXEC Mode

Usage Guidelines

None

Examples

This example shows the default configuration for the BMC Management Interface.

```
SLX # show bmc interface management 0 status
Status: Disabled
SLX # show bmc interface management 0 ip
 IP Address Source  : Static Address
 IP Address         : 192.168.11.1
 Subnet Mask        : 255.255.255.0
 MAC Addres         : 00:04:96:b8:41:b8
 Default Gateway IP : 0.0.0.0
```

This example shows the manually configured IPv4 address for the BMC Management Interface.

```
SLX # show bmc interface management 0 ip
IP Address Source       : Static Address
IP Address              : 10.20.111.155
Subnet Mask             : 255.255.240.0
MAC Address             : 88:7e:25:d3:40:05
Default Gateway IP      : 10.20.96.1
```

This example shows the configuration when the BMC Management Interface IPv4 address is assigned by an external DHCP server.

```
SLX # show bmc interface management 0 ip
IP Address Source       : DHCP Address
IP Address              : 10.20.111.155
Subnet Mask             : 255.255.240.0
MAC Address             : 88:7e:25:d3:40:05
Default Gateway IP      : 10.20.96.1
```

show bmc password-status

Displays the status of the password being set for the specific BMC User ID.

Syntax

show bmc password-status *bmc-user-id*

Parameters

bmc-user-id

The user ID.

Modes

Privileged EXEC Mode

Usage Guidelines

None

Examples

The following is the command output when the password is not set for a specific user ID.

```
SLX # show bmc password-status 1
pending
```

The following is the command output when the password is set for a specific user ID.

```
SLX # show bmc password-status 1
set
```

The following is the command output when the BMC User ID cannot be found.

```
SLX # show bmc password-status 1
user-id is not found.
```

show bmc status

Displays the current BMC firmware version and network configurations.

Syntax

show bmc status

Parameters

None

Modes

Privileged EXEC Mode

Usage Guidelines

When the IP source `ipsrc` is changed between *dhcp* and *static*, the modified LAN configuration takes few seconds to get applied. This is a known BMC behavior.

The command will not display any output if a BMC configuration is in progress. It is recommended to try the same command after some time.

Examples

The following example shows the output of the `show bmc status` command.

```
SLX# show bmc status

Firmware Revision : 3.20

LAN configurations
Set in Progress          : Set Complete
Auth Type Support        : MD2 MD5 PASSWORD
Auth Type Enable         : Callback : MD2 MD5 PASSWORD
                         : User     : MD2 MD5 PASSWORD
                         : Operator : MD2 MD5 PASSWORD
                         : Admin    : MD2 MD5 PASSWORD
                         : OEM      :
IP Address Source        : DHCP Address
IP Address               : 10.20.111.155
Subnet Mask              : 255.255.240.0
MAC Address              : 88:7e:25:d3:40:05
SNMP Community String    : Quanta
IP Header                : TTL=0x40 Flags=0x40 Precedence=0x00 TOS=0x10
BMC ARP Control          : ARP Responses Enabled, Gratuitous ARP
Disabled
Gratituous ARP Intrvl    : 0.0 seconds
Default Gateway IP       : 10.20.96.1
Default Gateway MAC      : 00:00:00:00:00:00
Backup Gateway IP        : 0.0.0.0
Backup Gateway MAC       : 00:00:00:00:00:00
802.1q VLAN ID           : Disabled
802.1q VLAN Priority     : 0
```

```
RMCP+ Cipher Suites      : 0,1,2,3,6,7,8,11,12,15,16,17
Cipher Suite Priv Max    : XaaaaaaaaaaaXXX
                         : X=Cipher Suite Unused
                         : c=CALLBACK
                         : u=USER
                         : o=OPERATOR
                         : a=ADMIN
                         : O=OEM
Bad Password Threshold   : 0
Invalid password disable : no
Attempt Count Reset Int. : 0
User Lockout Interval    : 0
LAN status (on SOHO)     : enabled
SLX#
```

The following example shows the output of the `show bmc status` command when a LAN configuration on the BMC is in progress.

```
SLX# show bmc status
Firmware Revision : 3.20
LAN configurations Configuration still in progress. Try again after few seconds.
SLX#
```

show bridge-domain

Displays information about bridge domains.

Syntax

show bridge-domain [*bd-id* [**logical-interface**]]

show bridge-domain brief [**p2mp** | **p2p**]

show bridge-domain interface { **ethernet** *slot/port* | **port-channel** *number* }

show bridge-domain vc-peer

Parameters

bd-id

Specifies the bridge-domain identifier.

logical-interface

Causes the display of the ifindex and operational information for logical interfaces configured under the bridge domain.

brief

Causes the display of summary bridge-domain information.

p2mp

Causes the display of multipoint service information.

p2p

Causes the display of multi-point cross-connect service information.

interface

Displays a list of bridge-domain logical interfaces that are associated with a physical interface.

ethernet *slot/port*

Specifies an Ethernet interface in slot/port format. For devices that do not support linecards, specify **0** for the slot.

port-channel *number*

Specifies a port-channel interface number.

vc-peer

Causes the display of summary virtual connection (VC) peer information for the bridge domain.

Modes

Privileged EXEC mode.

Output

The following table describes elements of information displayed in output from the **show bridge-domain** command:

Output field	Description
Assigned LSPs	Assigned label-switched paths.
AC LIF Count	Number of attachment circuit (AC) logical interfaces in the bridge-domain.
bpdu-drop-enable	Indicates whether dropping Layer 2 (L2) bridge protocol data units (BPDUs) is enabled (TRUE) or disabled (FALSE) for the bridge domain.
BDID	Bridge domain identifier.
Bridge-domain Type	Bridge-domain type. Type can be multipoint service (MP) or multi-point cross-connect (P2P).
Cos Enabled	Indicates whether Cost of Service (CoS) is enabled (True) or disabled (False) for a peer device in the bridge domain.
Load-balance	Indicates whether load balancing is enabled (True) or disabled (False) for a peer device in the bridge domain.
Local switching	Indicates whether local switching is enabled (TRUE) or disabled (FALSE) for the bridge domain.
Local VC lbl	Local virtual connection label (for the pseudowire that corresponds with the peer).
Local MTU	Local maximum transmission unit configuration (for the pseudowire that corresponds with the peer).
Local VC-Type	Local virtual connection mode configuration (for the pseudowire that corresponds with the peer).
Macs Dynamically learned	MAC addresses learned dynamically from traffic on the interface part of the bridge domain.
Macs statically configured	Number of MAC addresses configured statically over interfaces associated with the bridge domain.
MCT Enabled	Whether the bridge domain is configured under the MCT cluster. If it is, the field displays TRUE. Otherwise, the field displays FALSE.
Number of configured end-points	Number of endpoints that are configured for the bridge domain.
Number of Active end-points	Number of endpoints that are active in the bridge domain.
PW-profile	Pseudowire profile that is associated the bridge domain.
Remote VC lbl	Remote virtual connection label (for the pseudowire that corresponds with the peer).
Remote VC MTU	Remote maximum transmission unit configuration (for the pseudowire that corresponds with the peer).
Remote VC-Type	Remote virtual connection mode configuration (for the pseudowire that corresponds with the peer).

Output field	Description
Total number of VC peers	Number of remote VPLS provider-edge (PE) devices that this node is peered with. (This is the same as the number of remote VPLS peers.)
Total VPLS peers	Number of remote VPLS provider-edge (PE) devices that this node is peered with.
Tunnel cnt	The number of MPLS tunnels that are selected by the pseudowire (corresponding to the peer).
VC id	Virtual connection identifier.
VE if-indx	Routing interface (virtual switching interface) index.
VFI LIF Count:	Number of virtual forwarding interfaces (VFI) in the bridge-domain.

Examples

The following example shows the information displayed by the **show bridge-domain** command.

```
device# show bridge-domain

Total Number of bridge-domains: 3
Number of bridge-domains: 3

Bridge-domain 1
-------------------------------
Bridge-domain Type: mp , VC-ID: 5, MCT Enabled: TRUE
Number of configured end-points:  5 , Number of Active end-points: 4
VE if-indx: 1207959555, Local switching: TRUE, bpdu-drop-enable:TRUE
PW-profile: 1, mac-limit: 128000
Number of Mac's learned:90000,     Static-mac count: 10,
VLAN: 100, Tagged ports: 2(2 up), Un-tagged ports: 0 (0 up)
Tagged ports: Eth 0/2/6, eth 0/2/8
Un-tagged ports:

Total PW peers: 2 (2 Operational)
Peer address: 12.12.12.12, State: Operational, Uptime: 2 hr 55 min
      Load-balance: True , Cos enabled:False,
      Assigned LSP;s:
      Tnnl in use: tnl2[RSVP]
      Local VC lbl: 983040, Remote VC lbl: 983040
      Local VC MTU: 1500, Remote VC MTU: 1500,
      Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
Peer address: 15.15.15.15, State: Operational, Uptime: 2 hr 55 min
         Load-balance: False , Cos enabled:False,
      Assigned LSP's: lsp1, lsp2
      Tnnl in use: tnl1[MPLS]
      Local VC lbl: 983041, Remote VC lbl: 983043
      Local VC MTU: 1500, Remote VC MTU: 1500 ,
      Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)

Bridge-domain 2
-------------------------------
Bridge-domain Type: mp , VC-ID: 100, MCT Enabled: FALSE
Number of configured end-points:  5 , Number of Active end-points: 4
VE if-indx:  NA, Local switching: FALSE, bpdu-drop-enable:FALSE
```

```
PW-profile: profile_1, mac-limit: 262144
Number of Mac's learned:90000,     Static-mac count: 10,
VLAN: 100, Tagged ports: 2(1 up), Un-tagged ports: 0 (0 up)
      Tagged ports: eth 0/2/10, eth 0/1/10
      Un-tagged ports:
VLAN: 150, Tagged ports: 1(1 up), Un-tagged ports: 0 (0 up)
      Tagged ports: eth 0/1/5
      Un-tagged ports:

Bridge-domain 3
-------------------------------
Bridge-domain Type: mp , VC-ID: 200, MCT Enabled: FALSE
Number of configured end-points:  5 , Number of Active end-points: 4
VE if-indx: 120793855, Local switching: FALSE, bpdu-drop-enable:FALSE
PW-profile: 2, mac-limit: 262144
Number of Mac's learned:90000,     Static-mac count: 10,
Local switching: TRUE,
VLAN: 500, Tagged ports: 2(2 up), Un-tagged ports: 2 (1 up)
Tagged ports:     eth 0/11/6, eth 0/4/3
Un-tagged ports:

Total VPLS peers: 3 (2 Operational)
Peer address: 5.5.5.5, State: Operational, Uptime: 2 hr 35 min
         Load-balance: False , Cos enabled:False,
      Assigned LSP;s:
      Tnnl in use: tnl2[RSVP]
      Local VC lbl: 983050, Remote VC lbl: 983050
      Local VC MTU: 1500,Remote VC MTU: 1500,
      Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
Peer address: 20.20.20.20, State: Operational, Uptime: 0 hr 18 min
         Load-balance: False , Cos enabled:True,
      Assigned LSP's:
      Tnnl in use: NA,
      Local VC lbl: NA, Remote VC lbl: NA
      Local VC MTU: 1500,Remote VC MTU: 1500,
      Local VC-Type: Ethernet(0x05), Remote VC-Type: Ethernet(0x05)
Peer address: 10.10.10.10, State: Not-Operational (Tunnel Not Available),
         Load-balance: True , Cos enabled:False,
      Assigned LSP's: lsp10, lsp15
      Tnnl in use: NA,
      Peer Index:2
      Local VC lbl: NA, Remote VC lbl: NA
      Local VC MTU: 1500,Remote VC MTU: NA ,
      Local VC-Type: Ethernet(0x05), Remote VC-Type: NA
```

The following example shows information about a bridge domain (501) in which the **load-balance** and **cos** options are configured for the peer device 10.9.9.9.

```
device# show bridge-domain 501

Bridge-domain 501
-------------------------------
Bridge-domain Type: MP , VC-ID: 501, MCT Enabled: FALSE
Number of configured end-points:  2 , Number of Active end-points: 2
VE if-indx: 0, Local switching: TRUE, bpdu-drop-enable: TRUE
PW-profile: default, mac-limit: 0
VLAN: 501, Tagged ports: 1(1 up), Un-tagged ports: 0 (0 up)
Tagged Ports: eth1/6.501
Un-tagged Ports:
Total VPLS peers: 1 (1 Operational):

VC id: 501, Peer address: 10.9.9.9, State: Operational, uptime: 2 min
      Load-balance: True , Cos Enabled: True ,
```

```
      Tunnel cnt: 16
      rsvp  p101(cos_enable:True cos_value:1)
      rsvp  p102(cos_enable:True cos_value:1)
      rsvp  p103(cos_enable:True cos_value:1)
      rsvp  p104(cos_enable:True cos_value:1)
      rsvp  p105(cos_enable:True cos_value:1)
      rsvp  p106(cos_enable:True cos_value:1)
      rsvp  p107(cos_enable:True cos_value:1)
      rsvp  p108(cos_enable:True cos_value:1)
      rsvp  p109(cos_enable:True cos_value:1)
      rsvp  p110(cos_enable:True cos_value:1)
      rsvp  p111(cos_enable:True cos_value:1)
      rsvp  p112(cos_enable:True cos_value:1)
      rsvp  p113(cos_enable:True cos_value:1)
      rsvp  p114(cos_enable:True cos_value:1)
      rsvp  p115(cos_enable:True cos_value:1)
      rsvp  p116(cos_enable:True cos_value:1)
      Assigned LSPs count:0 Assigned LSPs:
      Local VC lbl: 989046, Remote VC lbl: 983040,
      Local VC MTU: 1500, Remote VC MTU: 1500,
      Local VC-Type: 5, Remote VC-Type: 5
```

The following example shows information about bridge domain 501 in which the **load-balance** option, **cos** option and three assigned label-switched paths (p1001, p1002, and p1003) are configured for the peer device 10.9.9.9.

```
device# show bridge-domain 501

Bridge-domain 501
-------------------------------
Bridge-domain Type: MP , VC-ID: 501, MCT Enabled: FALSE
Number of configured end-points:  2 , Number of Active end-points: 2
VE if-indx: 0, Local switching: TRUE, bpdu-drop-enable: TRUE
PW-profile: default, mac-limit: 0
VLAN: 501, Tagged ports: 1(1 up), Un-tagged ports: 0 (0 up)
Tagged Ports: eth1/6.501
Un-tagged Ports:
Total VPLS peers: 1 (1 Operational):

VC id: 501, Peer address: 10.9.9.9, State: Operational, uptime: 19 sec
      Load-balance: True , Cos Enabled: True ,
      Tunnel cnt: 2
      rsvp  p1001(cos_enable:True cos_value:1)
      rsvp  p1002(cos_enable:True cos_value:1)
      Assigned LSPs count:3 Assigned LSPs:p1001 p1002 p1000
      Local VC lbl: 989047, Remote VC lbl: 983040,
      Local VC MTU: 1500, Remote VC MTU: 1500,
      Local VC-Type: 5, Remote VC-Type: 5
```

The following example shows the information displayed by the **show bridge-domain brief** command.

```
device# show bridge-domain brief

Total Number of bridge-domains configured:  3
Number of VPLS bridge-domains: 3
Macs Dynamically learned: 100, Macs statically configured: 200

Name    ID(VC-ID) TYPE   Intf(up)   PWs(up)  macs
------- -------    ------ --------- ------       ------
1          3000      MP     5(3)             -           5000
```

```
2          5000      MP     2(1)              -           80
3       8000         MP     1(1)          3(2)     100000
```

The following example shows how to display bridge-domain information for a port-channel interface.

```
device# show bridge-domain interface port-channel 10
BDID 6, logical-interface po10.200, VLAN 200, tagged, DOWN
BDID 6, logical-interface po10.201, VLAN 201, tagged, DOWN
BDID 7, logical-interface po10.202, VLAN 202, tagged, DOWN
BDID 7, logical-interface po10.203, VLAN 203, tagged, DOWN
BDID 7, logical-interface po10.204, VLAN 204, tagged, DOWN
```

show capabilities

Displays whether a variety of network services are enabled ("true") or not ("false").

Syntax

show capabilities

Modes

Privileged EXEC mode

Usage Guidelines

Enter **?** to view available options.

Examples

The following example displays the status of all network services:

```
device# show capabilities
capabilities mqc span true
capabilities qos system-rx-queue-limit false
capabilities qos system-tx-queue-limit true
capabilities qos show-rx-queue-interface false
capabilities qos conf-rx-queue-interface false
capabilities qos cee nas false
capabilities qos cpu slot false
capabilities qos cpu queue false
capabilities l2 port_profile true
capabilities l2 overlap_vlan true
capabilities l2 rspan false
capabilities l2 mac_move true
capabilities l2 consistency_check false
capabilities l2 learning_mode true
capabilities l2 priority_tag true
capabilities l2 internal_nsm true
capabilities l2 lif_untagged_vlan_id false
capabilities l2 bridgedomain_local_switching false
capabilities l2 dot1x false
capabilities l3 ip_mtu true
capabilities ipv6 ipv6Raguard false
capabilities ssm aclTrafficType true
capabilities lag PortchannelRedundancy false
capabilities bgp next-hop-mpls false
capabilities bgp redistribute-isis false
capabilities license eula_display true
capabilities license dpod_display false
capabilities license slot_display false
capabilities ip igmp false
capabilities ip igmp-snooping igmp-snooping-version false
capabilities tm false
capabilities overlay gre false
capabilities cfm false
```

show cee maps default

Displays the current CEE map configuration.

Syntax

show cee maps default

Parameters

default

The name of the CEE map. Only one CEE map can be defined on a system and the name assigned to this policy is *default*.

Modes

Privileged EXEC mode

Examples

This example displays the current CEE Map configuration.

```
device# config term
device(config)# do show cee maps default

CEE Map 'default'
Precedence: 1

Priority Group Table
1: Weight 40, PFC Enabled, BW%40
2: Weight 60, PFC Disabled, BW% 60
15.0: PFC Disabled
15.1: PFC Disabled
15.2: PFC Disabled
15.3: PFC Disabled
15.4: PFC Disabled
15.5: PFC Disabled
15.6: PFC Disabled
15.7: PFC Disabled
Priority Table
CoS: 0 1 2 3 4 5 6 7
---------------------------------------
PGID: 2 2 2 1 2 2 2 15.0
Enabled on the following interfaces:
Ethernet 0/1
```

show cert-util sshkey

Displays the public SSH key for a specified user.

Syntax

show cert-util sshkey user *user_id*

Parameters

user *user_id*

The user ID to display.

Modes

Privileged EXEC mode

Examples

The following example shows typical output for the command.

```
device# show cert-util sshkey user testuser

user's public keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAtTCFzC1lfjwV9hjdtqv2ulSvmsmf7q7MS92Ctc3pDje/
YGYJPHVUi8b
QX0XAsCAuzdsZL0BlVHdYPO1L4HStuIo8okfn4xLxrazqzwVeeL8p5Zcspf9zK8HmDzNpZ/OuQ9MvfOuzbseYrovqg
YLFGfPvY6vleFXZo61vVncFM7uFzasED9o9JUSBRORhBki7vB0SG69yNn6ADnmpQW6QOu+nYuZaWXO0QXk2OIB+hid
j
xSQVAfVLidSIGyfDD0go+JAE3osxZxwQa5jcorASs4q2Gt4tSYERpvzOsjaAR5YivbmmBTIQWdUuR9Laz8s8VKF4Di
9
HQ4kE+xyBeAFNvQ== bmeenaks@blc-10-6
```

show cfm

Displays the current configuration and status of CFM.

Syntax

show cfm [**brief** | **connectivity**]

Parameters

brief

Displays the CFM brief output.

connectivity *session-id*

Dixplays the CFM connectivity configuration

Modes

Privileged EXEC mode

Output

The **show cfm** command displays the following information:

Output field	Description
Domain	The Domain is the network or the part of the network for which faults in connectivity are displayed.
Level	The level is the domain level in the range <0-7>.
Maintenance Association	The maintenance association name.
MAID Format	MAID format setting
CCM interval	The time interval between two successive Continuity Check messages (CCMs) that are sent by MEPs in the specified Maintenance Domain.
VLAN ID/ Bridge-Domain ID	The VLAN or Bridge-domain identifier of the maintenance association.
Priority	The priority of the CCM messages, sent by 'MEPs, in the range <0-7>.
MEP	The maintenance end point ID
Direction	Displays the direction the MEP was sent: Up - The MEP direction away from the monitored VLAN. Down - The MEP direction is towards the monitored VLAN.
MAC	Displays the associated MAC address.
PORT	Displays the associated port.
MIP	Displays the associated MIP.

Examples

Typical command output displaying the CFM settings for domain MD1.

```
device# show cfm
Domain: md1
Index: 1
Level: 7
  Maintenance association: ma5
  MA Index: 5
  CCM interval: 100 ms
  Bridge-Domain ID: 50
  Priority: 7
  MAID Format: Short
  MEP   Direction  MAC              PORT       VLAN         INNER-VLAN   PORT-STATUS-TLV
  ====  =========  =========        ====       ====         ===========  ===============
  1     UP         609c.9f5f.700d   Eth 1/9    50           --           N
```

Typical command output displaying the connectivity information.

```
device# show cfm connectivity
Domain: md1
Index: 1
Level: 7
  Maintenance association: ma5
  MA Index: 5
  CCM interval: 100 ms
  Bridge-Domain ID: 50
  Priority: 7
  MAID Format: Short
    MEP Id: 1
    MEP Port: Eth 1/9
      RMEP  MAC             VLAN/PEER         INNER-VLAN    PORT      STATE
      ====  ===             =========         ==========    ====      =====
      2     609c.9f5e.4809  19.1.1.1           --            --       OK
```

Typical command output displaying the brief output.

```
device# show cfm brief
Domain: md1
Index: 1
Level: 7  Num of MA: 1
  Maintenance association: ma5
  MA Index: 5
  CCM interval: 100 ms
  Bridge-Domain ID: 50
  Priority: 7
  MAID Format: Short
  Num of MEP: 1  Num of RMEP: 1
  rmepfail: 0 rmepok: 1
```

show cfm y1731 action-profile

Displays the Y.1731 action profile.

Syntax

show cfm y1731 action-profile

Modes

Privileged EXEC mode

Examples

This example displays the Y. 1731 action-profiles.

```
device# show cfm y1731 action-profile
----------------------------------------
  Name                  : a1

  Event                 : CCM Down
  Action(s)             : Interface Down
----------------------------------------
```

show cfm y1731 client-signal-fail

Displays ETH-CSF configuration information and packet statistics for all Maintenance Entity Group End Point (MEP) and associated Client interfaces.

Syntax

show cfm y1731 client-signal-fail

Modes

Privileged EXEC mode

Examples

This example displays ETH-CSF configuration information and packet statistics.

```
device# show cfm y1731 client-signal-fail
--------------------------------------------------------------------------------
Domain Name : md1
MA Name     : ma1
--------------------------------------------------------------------------------
ETH-CSF Statistics :
--------------------------------------------------------------------------------
MEP RMEP MEP    RMEP   Client CSF    Transmit  Transmit Receive  Transmit Receive
ID  ID   Status Status I/F    Type   Period    Frames   Frames   C-DCI    C-DCI
--------------------------------------------------------------------------------
1   2    UP     UP     1/1    C-LOS  1 minute  10       10       1        0
2   1    UP     DOWN   1/2    C-LOS  1 second  0        0        0        0
```

This example displays ETH-CSF configuration information and packet statistics after the **clear cfm y1731 client-signal-fail** command is issued.

```
device# show cfm y1731 client-signal-fail
--------------------------------------------------------------------------------
Domain Name : md1
MA Name     : ma1
--------------------------------------------------------------------------------
ETH-CSF Statistics :
--------------------------------------------------------------------------------
MEP RMEP MEP    RMEP   Client CSF    Transmit  Transmit Receive  Transmit Receive
ID  ID   Status Status I/F    Type   Period    Frames   Frames   C-DCI    C-DCI
--------------------------------------------------------------------------------
1   2    UP     UP     1/1    C-LOS  1 minute  0        0        0        0
2   1    UP     DOWN   1/2    C-LOS  1 second  0        0        0        0
```

show cfm y1731 delay-measurement

Displays detailed info for all measurement sessions.

Syntax

show cfm y1731 delay-measurement

show cfm y1731 delay-measurement brief

show cfm y1731 delay-measurement session *session-id*

show cfm y1731 delay-measurement statistics

show cfm y1731 delay-measurement statistics brief

show cfm y1731 delay-measurement statistics session *session-id* **brief**

show cfm y1731 delay-measurement statistics session *session-id* **brief**

Parameters

brief

Specifies brief.

session *session-id*

Specifies session and the session ID.

statistics

Specifies statistics.

history*history-index*

Specifies history and the history index..

Modes

Privileged EXEC mode

Examples

This example displays detailed info for all measurement sessions.

```
device# show cfm y1731 delay-measurement statistics brief
------------------------------------------------------------------------------
Session Index : 1
Test Profile Name : my_test_profile2
------------------------------------------------------------------------------
HISTORY TABLE :
------------------------------------------------------------------------------------------------
----
Index     Start    Elapsed    Avg Delay(us)   Max Delay(us)   Min Delay(ns)   FDV
Avg(ns)     FDV Max(ns)     FDV Min(ns)
------------------------------------------------------------------------------------------------
----
4         03:13:34 00:15:00      33.281      33.542      32.851      39      79      12
3         02:58:34 00:15:00   27.162      27.690      26.745      41      85      13
```

```
2         02:43:34 00:15:00   28.260      30.452      27.540      40      83      12
1         02:28:34 00:15:00   29.120      32.164      28.242      41      84      13
-------------------------------------------------------------------------------
Session Index : 2
Test Profile Name : my_test_profile2
-------------------------------------------------------------------------------------------------
----
HISTORY TABLE :
-------------------------------------------------------------------------------------------------
----
Index     Start    Elapsed    Avg Delay(us)   Max Delay(us)   Min Delay(ns)   FDV
Avg(ns)     FDV Max(ns)     FDV Min(ns)
-------------------------------------------------------------------------------------------------
----
4         05:12:14 00:15:00  32.180      33.543      31.589      38      79      11
3         04:48:54 00:15:00  29.060      29.950      27.654      41      83      12
2         04:30:40 00:15:00  30.105      30.154      28.764      40      82      12
1         04:15:14 00:15:00  31.234      31.665      29.143      40      81      12
-------------------------------------------------------------------------------------------------
----
```

show cfm y1731 synthetic-loss-measurement

Displays detailed info for all measurement sessions.

Syntax

show cfm y1731 synthetic-loss-measurement

show cfm y1731 synthetic-loss-measurement brief

show cfm y1731 synthetic-loss-measurement session *session-id*

show cfm y1731 synthetic-loss-measurement statistics

show cfm y1731 synthetic-loss-measurement statistics brief

show cfm y1731 synthetic-loss-measurement statistics session *session-id* **brief**

show cfm y1731 synthetic-loss-measurement statistics session *session-id* **brief**

show cfm y1731 synthetic-loss-measurement statistics session *session-id* **history** *history-index*

Parameters

brief

Specifies brief.

session *session-id*

Specifies session and the session ID.

statistics

Specifies statistics.

history*history-index*

Specifies history and the history index..

Modes

Privileged EXEC mode

Examples

This example displays detailed info for all measurement sessions.

```
device# show cfm y1731 synthetic-loss-measurement
    SLM Session Index       : 1
Test Profile Name              : my_test_profile1
Status                        : Active
Session Type                  : Initiator
Domain                        : md1
MA                            : ma1
Source MEP                    : 1
```

```
Target MEP                     : 2
Cos                            : 5
Start time                     : 19:49:55
Start time type                : Fixed
Stop time                      : 00:00:00
Stop time type                 : Fixed
Tx-interval(sec)               : 1
Measurement-interval(min)      : 15
Forward Average (milliPercent) : 4294967295
Forward Max     (milliPercent) : 4294967295
Backward Average(milliPercent) : 1
Backward Max    (milliPercent) : 4
-----------------------------------

SLM Session Index               : 2
Test Profile Name                : my_test_profile2
Status                          : Active
Session Type                    : Responder
Domain                          : md2
MA                              : ma2
Source MEP                      : 2
Target MEP                      : 1
Cos                             : 7
Start time                      : 01:30:30
Start time type                 : Fixed
Stop time                       : 02:30:30
Stop time type                  : Fixed
Tx-interval(sec)                : 2
Measurement-interval(min)       : 10
Forward Average  (milliPercent) : 4294967295
Forward Max      (milliPercent) : 4294967295
Backward Average (milliPercent) : 1
Backward Max     (milliPercent) : 3
```

show cfm y1731 test-profile

Displays the Y.1731 test profile.

Syntax

show cfm y1731 synthetic-loss-measurement

Modes

Privileged EXEC mode

Examples

This example displays the Y.1731 test profile.

```
-------------------------------------------------
Default Test Profiles:
-------------------------------------------------
  Name                          : 2dm-default-profile
  Type                          : ETH-DM
  Cos Value                     : 7
  Tx-Interval                   : 1 Second
  Tx-Frame-Count                : 10
  Measurement Interval          : 15 Minute(s)
  Threshold Average             : 4294967295 (uSec)
  Threshold Max                 : 4294967295 (uSec)
  Start time                    : 00:05:00 (After)
  Stop time                     : 01:05:00 (After)
  Timeout                       : 1 Second
-------------------------------------------------
-------------------------------------------------
  Name                          : 2slm-default-profile
  Type                          : ETH-SLM
  Cos Value                     : 7
  Tx-Interval                   : 1 Second
  Tx-Frame-Count                : 10
  Measurement Interval          : 15 Minute(s)
  Threshold Backward Average    : 4294967295
  Threshold Backward Max        : 4294967295
  Threshold Forward Average     : 4294967295
  Threshold Forward Max         : 4294967295
  Start time                    : 00:05:00 (After)
  Stop time                     : 01:05:00 (After)
  Timeout                       : 1 Second
```

show chassis

Displays the status for components in the device.

Syntax

show chassis

Modes

Privileged EXEC mode

Usage Guidelines

This command is executed on the local switch and is supported only on the local switch. The output of this command depends on the platforms on which it is executed.

Pagination is not supported with this command. Use the "more" parameter to display the output one page at a time.

Supply power values are positive; consumer power values are negative.

Examples

The following example displays chassis information on an SLX 9540.

```
device# show chassis
Chassis Name:BR-SLX9540
switchType: 4000

POWER SUPPLY  Unit: 1
Factory Part Num:
Factory Serial Num:
Time Awake:            0 days

POWER SUPPLY  Unit: 2
Factory Part Num:
Factory Serial Num:
Time Awake:            0 days

FAN  Unit: 1
Time Awake:            0 days

FAN  Unit: 2
Time Awake:            0 days

FAN  Unit: 3
Time Awake:            0 days

FAN  Unit: 5
Time Awake:            0 days

CHASSIS/WWN  Unit: 1
Power Consume Factor: 0
Factory Part Num:      40-1001198-03
Factory Serial Num:    FBK0319M00J
Manufacture:           Day:  0  Month:  0  Year: 2000
```

```
Update:                Day:  1  Month:  2  Year: 2018
Time Alive:            646 days
Time Awake:            0 days
Rework: 0
Serial Num:   0
Rework: 0
```

show cipherset

Displays the current cipherset status for LDAP and SSH.

Syntax

show cipherset { **ldap** | **radius** }

Parameters

radius

Specifies secure RADIUS ciphers.

ldap

Specifies secure LDAP ciphers.

Modes

Privileged EXEC mode

Examples

To display configured cipher list on the device:

```
device# show cipherset

RADIUS Cipher List(FIPS 140-2 Approved) : AES256-SHA256 AES256-SHA AES128-SHA256 AES128-
SHA
LDAP Cipher List(FIPS 140-2 Approved) :AES256-SHA256 AES256-SHA AES128-SHA256 AES128-SHA
```

show cli

Displays all the current CLI settings.

Syntax

show cli

Modes

Privileged EXEC mode

Examples

Typical command output display.

```
device# show cli
autowizard             false
complete-on-space      false
history                100
idle-timeout           600
ignore-leading-space   false
output-file            terminal
paginate               true
prompt1                \H\M#
prompt2                \H(\m)#
screen-length          73
screen-width           120
service prompt config  true
show-defaults          false
terminal               ansi
```

show clock

Returns the local time, date, and time zone.

Syntax

show clock

Command Default

The local clock is used.

Modes

Privileged EXEC mode

Usage Guidelines

The command displays the current time for the device.

Examples

The following example shows the clock time.

```
device# show clock
2017-02-28 17:58:30 Etc/GMT
```

show cluster

Displays the MCT cluster information including client, PW client, member bridge domain, and member VLAN information.

Syntax

show cluster

show cluster client [*cluster-ID* | *A.B.C.D*]

show cluster client-pw

show cluster icl { **brief** | **detail** | **statistics** }

show cluster member { **bridge-domain** | **vlan** }

Parameters

client

Specifies the cluster ID or IP address.
cluster-ID

Specifies the cluster client ID.

A.B.C.D

Specifies the cluster IP address.

client-pw

(is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.) Specifies PW client information for VPLS or VLL MCT.

icl

Specifies inter-chassis link (ICL) information.
brief

Specifies brief ICL information.

detail

Specifies detailed ICL information.

statistics

Specifies ICL statistics.

member

Specifies member bridge-domains or VLANs.
bridge-domain

Specifies cluster bridge domains.

vlan

Specifies cluster VLANs.

Modes

Privileged EXEC mode

Usage Guidelines

When you delete an IP router ID that is used as the neighbor ID and IP address on an MCT peer, the **show cluster** command on the MCT peer devices displays inconsistent cluster states.

Output

The **show cluster** command displays the following information:

Output field		Description
Cluster		Name of the cluster
	Cluster State	Whether the cluster is deployed or undeployed
	Client Isolation Mode	Client-isolation mode configuration: Strict or Loose.
	DF Hold Time	Designated-forwarder hold timer value.
	Configured Member Vlan Range	Configured VLANs as members to the MCT cluster.
	Active Member Vlan Range	Active member VLANs.
	Configured Member BD Range	Configured bridge domains as members to the MCT cluster.
	Active Member BD Range	Active member bridge domains.
	No. of Peers	Number of cluster peers.
	No. of Clients	Number of cluster clients.
Peer Info		Peer information
	Peer IP	Configured IP address for the MCT cluster peer.
	State	Whether the peer state is UP or DOWN.
	Peer Interface	Configured peer interface slot and port.
	ICL Tunnel Type	State of the MPLS tunnel to reach the MCT peer.
PW client Info		PW client information. The SLX 9150 and SLX 9250 devices do not support the PW client.

Output field		Description
	ESI	Configured Ethernet Segment ID (ESI) value.
	Deploy	Whether the PW client is deployed (TRUE or FALSE).
	State	Whether the client state is UP or DOWN.
Client Info		Cluster client information
	Name	Configured client name.
	ID	Configured client ID.
	ESI	Configured 9-byte Ethernet Segment ID (ESI) value or 10-byte auto-generated ESI.
	Interface	Configured interface assigned to the client.
	Local/Remote State	Local and remote state of the client; Up or Down, Deployed (Dep) or Undeployed (UnDep).

On the SLX 9540 and SLX 9640 devices, the **client-pw** option with the **show cluster** command displays the following information:

Output field	Description
Client	Client type as Client-pw.
Client ID	Internally-generated PW client ID.
Deployed or Undeployed	Whether the PW client is deployed or undeployed
State	Whether the PW client state is Up or Down.
Bridge-domains	Configured bridge domains IDs.
Elected DF for Bridge-domains	Bridge domain ID elected as the designated forwarder.

Examples

On the SLX 9540 and SLX 9640 devices, the following example shows the information of the cluster on the SLX-OS device.

```
device# show cluster 1

Cluster default
================
Cluster State: Active
Bringup Delay: 90 seconds
Local Bias mode for LVTEP Broadcast: Yes
Configured Member Vlan Range: All
Active Member Vlan Range: 1,10-19,2004
Configured Member BD Range: All
Active Member BD Range: 1-2,504
No. of Clients: 1
```

```
Peer Info:
==========
Peer IP: 12.0.1.1, State: Up
Peer Interface: Port-channel 256, Source IP: 12.0.1.0


Keep-Alive:
==========
IP: 10.24.15.132, State: Up
Interface: Management 0 (mgmt-vrf), Source IP: 10.24.15.50
Client-Isolation Role: Secondary


Client Info:
============
Interface          Id   Description   Local/Remote State     Exceptions
-----------        --   -----------   ------------------     ----------
Port-channel 10   1010                Up   / Up
```

On the SLX 9540 and SLX 9640 devices, the following example shows the PW client information.

```
device#show cluster 1 client-pw
Client Info:
============
Client: Client-pw, client-id: 34816, Deployed, State: Up
Interface: PW
Bridge-domains: 8100-8101
Elected DF for Bridge-domains:
8100
```

The following example shows the member bridge-domain information.

```
device# show cluster member bridge-domain
 BD-ID     Mcast-label(Lo/Re)    Unicast-label(Lo/Re)    Forwarding state
-------    ------------------    --------------------    ----------------
  1000       822248/ -1                 805864/ 0                 Down
  1001       822249/ -1                 805865/ 0                 Down
```

The following example shows the addition made for displaying the status of Local Bias on an LVTEP.

```
device# show cluster 1

Cluster default
================
Cluster State: Active
Bringup Delay: 90 seconds
Local Bias mode for LVTEP Broadcast: Yes
Configured Member Vlan Range: All
Active Member Vlan Range: 1,10-19,2004
Configured Member BD Range: All
Active Member BD Range: 1-2,504
No. of Clients: 1


Peer Info:
==========
Peer IP: 12.0.1.1, State: Up
Peer Interface: Port-channel 256, Source IP: 12.0.1.0
```

```
Keep-Alive:
==========
IP: 10.24.15.132, State: Up
Interface: Management 0 (mgmt-vrf), Source IP: 10.24.15.50
Client-Isolation Role: Secondary


Client Info:
============
Interface          Id   Description   Local/Remote State     Exceptions
-----------        --   -----------   ------------------     ----------
Port-channel 10   1010               Up   / Up
```

show cluster track

Displays list of interfaces with cluster-track configured along with their operational state.

Syntax

show cluster track

Parameters

show cluster track

Displays all interfaces that are currently tracking cluster status using cluster-track configuration.

Modes

Global mode

Output

The **show cluster-track** command displays the following information:

Examples

```
show cluster track

Cluster tracking Interfaces:

Interface       Description     Local State   Exceptions

Ethernet 0/3     uplink_spine1   Down          Maintenance mode triggered cluster shutdown
```

show config-drift-track

Displays configuration drift information and status of the current session on the SLX device.

Syntax

show config-drift-track { **values** | **status** }

Parameters

values

Displays the current values for the configuration drift **Timestamp** and **Counter** values.

status

Displays the status of configuration for the current session.

Modes

Privilege Execution Mode

Examples

The following example displays the current configuration drift tracking values.

```
SLX# show config-drift-track values
Config Drift Timestamp: 1635487552
Config Drift Counter: 12344
```

The following example shows the status of configuration drift tracking for the current session.

```
SLX# show config-drift-track status
Config Drift Tracking is OFF
```

show copy-support status

Displays the status of the copy support operation.

Syntax

show copy-support status

Modes

Privileged EXEC mode

Usage Guidelines

The status is indicated by the percentage of completion. NORMAL indicates process is proceeding or completed without errors. FAULTY indicates a faulty blade.

This command is supported only on the local device.

Examples

To display the support upload status:

```
device# show copy-support status
```

show core-isolation track

Displays the list of core-isolation tracked interfaces.

Syntax

show core-isolation track

Modes

Privilege Exec Mode

Examples

The following example shows the list of tracked interfaces.

```
SLX # show core-isolation track

 Core-isolation tracking Interfaces:
 ===================================
 Interface       Description   Local State   Exceptions
 ---------       -----------   -----------   ----------
 Port-channel 8                 Down         EVPN-MH Core Isolation
 Port-channel 10                Down         EVPN-MH Core Isolation
```

show crypto ca

Displays trust point and certificate information.

Syntax

show crypto ca {**trustpoint** | **certificates**}

Parameters

trustpoint

Displays the trustpoint and associated key pair details.

certificates

Displays the CA certificate and Identity certificate details.

Modes

Privileged EXEC mode

Usage Guidelines

To run this command from other configuration modes, use the **do** command modifier.

Examples

This example shows typical output for a trustpoint.

```
device# show crypto ca trustpoint
trustpoint: t1; key-pair: k1
```

This example shows typical output for certificates.

```
device# show crypto ca certificates
oauth2 certificate(OAuth2 token signature validation):
  SHA1 Fingerprint=CB:B8:11:7D:25:9F:74:95:9D:44:83:CD:18:25:0B:11:AD:7C:7E:35
  Subject: O=f1c67be8-f3d3-4f2e-86cf-5e7d930c13f3, CN=Token Signing Service
  Issuer: O=f1c67be8-f3d3-4f2e-86cf-5e7d930c13f3, CN=Token Signing Service
  Not Before: Nov 11 17:04:04 2019 GMT
  Not After : Nov 10 22:53:16 2020 GM
```

show crypto key

Displays the crypto key pair.

Syntax

show crypto key *key_name*

Modes

Privileged EXEC mode

Usage Guidelines

To execute this command from other configuration modes, use the **do** command modifier.

Examples

Typical command output:

```
device# show crypto key mypubkey
key type: ecdsa
key label: k1
key size: 384
```

show debug all

Displays a list of all modules for which debug is enabled.

Syntax

show debug all

Modes

Privileged EXEC mode

Examples

The following example shows the a list of all modules for which debug is enabled.

```
device# show debug all
BGP Module
         BGP(T):  bfd debugging is on
OSPF Module
        BFD debugging is on
        events debugging is on
        packet debugging is on
        shortcuts debugging is on
```

show debug arp packet

Displays the ARP-packet debug configuration.

Syntax

show debug arp packet [**buffer**]

Parameters

buffer

Displays ARP packets saved in the relevant buffer.

Modes

Privileged EXEC mode

Output

The **show debug arp packet** command displays the following information:

Output field	Description
Protocol Type	Displays "ARP".
Package Flow	Displays "Sending" or "Rcvd".
Packet Type	Displays "ARP".
VRF ID	Displays the VRF ID.
Interface Info	Displays the physical or port-channel interface.
ScrMAC	Displays the MAC address of the source.
DstMAC	Displays the MAC address of the destination.
SrcIP	Displays the IP address of the source.
DstIP	Displays the IP address of the destination.

Examples

The following example is a typical output of the **show debug arp packet buffer** option.

```
device# show debug arp packet buffer
 Protocol Type        : ARP
 Packet Flow          : Sending
 Packet Type          : Req
 VRF ID               : 1
 Interface info       : Eth 1/1
 Ethernet,     SrcMAC : 768e.f807.2005, DstMAC: 0000.0000.0000
 Internet proto,SrcIP : 11.1.1.1, DstIP: 11.1.1.1

 Protocol Type        : ARP
```

```
Packet Flow         : Sending
Packet Type         : Req
VRF ID              : 1
Interface info      : Eth 1/1
Ethernet,     SrcMAC : 768e.f807.2005, DstMAC: 0000.0000.0000
Internet proto,SrcIP : 11.1.1.1, DstIP: 11.1.1.1

Protocol Type        : ARP
Packet Flow         : Rcvd
Packet Type         : Req
VRF ID              : 1
Interface info      : Eth 1/1
Ethernet,     SrcMAC : 0010.9400.0001, DstMAC: 0000.0000.0000
Internet proto,SrcIP : 11.1.1.2, DstIP: 11.1.1.1

Protocol Type        : ARP
Packet Flow         : Sending
Packet Type         : Rep
VRF ID              : 1
Interface info      : Eth 1/1
Ethernet,     SrcMAC : 768e.f807.2005, DstMAC: 0010.9400.0001
Internet proto, SrcIP : 11.1.1.1, DstIP: 11.1.1.2
```

show debug dhcp packet

Displays the Dynamic Host Control Protocol (DHCP) packet capture configuration for interfaces configured for DHCP packet capturing.

Syntax

show debug dhcp packet

Modes

Privileged EXEC mode

Examples

The following example displays the DHCP packet capture configuration on interfaces.

```
device# show debug dhcp packet
%  DHCP  protocol  RCV debug is enabled on interface Eth 0/18
%  DHCP  protocol  TX debug is enabled on interface Eth 0/18
PCAP Buffer Configuration for Vrf ID 0: Buffer Type is Linear and BufferSize is 2056
```

show debug dhcp packet buffer

Displays Dynamic Host Configuration Protocol (DHCP) packets saved in the DHCP packet capture buffer for all VRF IDs.

Syntax

show debug dhcp packet buffer

Modes

Privileged EXEC mode

Examples

The following command displays buffer content for all VRF IDs.

```
device# show debug dhcp packet buffer
Protocol Type       : DHCP
Packet Flow         : RX
Src Port            : 68 (DHCP Client)
Dst Port            : 67 (DHCP Server)
Message Type        : 1 (DHCP-Discover)
Hardware Type       : 1 (Ethernet (10Mb))
Hw Address Len      : 6
Hops                : 0
Transaction ID      : 0
Seconds Elapsed     : 0
BootP Flags         : 8000
Client IP           : 0.0.0.0
Your (client) IP    : 0.0.0.0
Next Server IP      : 0.0.0.0
Relay Agent IP      : 0.0.0.0
Client MAC Add      : 00:10:94:00:00:01
Server Host Name    : Not Given
Boot File Name      : Not Given
*****************************************
Protocol Type       : DHCP
Packet Flow         : TX
Src Port            : 67 (DHCP Server)
Dst Port            : 68 (DHCP Client)
Message Type        : 2 (DHCP-Offer)
Hardware Type       : 1 (Ethernet (10Mb))
Hw Address Len      : 6
Hops                : 1
Transaction ID      : 0
Seconds Elapsed     : 0
BootP Flags         : 8000
Client IP           : 0.0.0.0
Your (client) IP    : 10.10.10.30
Next Server IP      : 20.20.20.20
Relay Agent IP      : 10.10.10.10
Client MAC Add      : 00:10:94:00:00:01
Server Host Name    : Not Given
Boot File Name      : Not Given
*****************************************
Protocol Type       : DHCP
Packet Flow         : RX
```

```
Src Port            : 68 (DHCP Client)
Dst Port            : 67 (DHCP Server)
Message Type        : 3 (DHCP-Request)
Hardware Type       : 1 (Ethernet (10Mb))
Hw Address Len      : 6
Hops                : 0
Transaction ID      : 0
Seconds Elapsed     : 0
BootP Flags         : 8000
Client IP           : 0.0.0.0
Your (client) IP    : 0.0.0.0
Next Server IP      : 0.0.0.0
Relay Agent IP      : 0.0.0.0
Client MAC Add      : 00:10:94:00:00:01
Server Host Name    : Not Given
Boot File Name      : Not Given
*****************************************
Protocol Type       : DHCP
Packet Flow         : TX
Src Port            : 67 (DHCP Server)
Dst Port            : 68 (DHCP Client)
Message Type        : 5 (DHCP-Ack)
Hardware Type       : 1 (Ethernet (10Mb))
Hw Address Len      : 6
Hops                : 1
Transaction ID      : 0
Seconds Elapsed     : 0
BootP Flags         : 8000
Client IP           : 0.0.0.0
Your (client) IP    : 10.10.10.30
Next Server IP      : 20.20.20.20
Relay Agent IP      : 10.10.10.10
Client MAC Add      : 00:10:94:00:00:01
Server Host Name    : Not Given
Boot File Name      : Not Given
*****************************************
```

show debug ip bgp all

Displays all BGP4 debugging options that are enabled.

Syntax

show debug ip bgp all

Modes

Privileged EXEC mode

Examples

The following example displays all BGP4 debugging options that are enabled.

```
device# show debug ip bgp all
```

show debug ip igmp

Displays the Internet Group Management Protocol (IGMP) packets received and transmitted, as well as related events.

Syntax

show debug ip igmp

Modes

Privileged EXEC mode

Examples

The following displays example output.

```
device# show debug ip igmp
IGMP debugging status:

---------------------------------------

 errors          : off

 group           : off

 packets         : off

 query           : off

 report          : off

 direction       : none

 vlan            : none

 l2_port         : none
```

show debug ip ospf internal lsp-shortcuts

Displays the internal debugging information for OSPF LSP shortcuts.

Syntax

show debug ip ospf internal lsp-shortcuts

Parameters

None

Modes

Privilege Executable mode

Output

The command displays the following information:

Output field	Description
Num entries	The number of OSPF LSP Hash entries.
To	The IP address of the neighbor.
List Num	A indexed list of LSP shortcut entries. The first list always starts from 0 (zero).
count	The number of entires in the indexed list.
<name>	The internal name of the LSP created by combining LSP and tunnel ID.
<Metric>	The assigned metrics for this entry.

Examples

```
SLX# show debug ip ospf internal lsp-shortcuts
OSPF LSP Hash, Num entries 2
To 2.2.2.2 List Num 0, count 2
    Lsp 1     Metric 0
    Lsp 2     Metric 0
To 2.2.2.2 List Num 1, count 1
    Lsp 3     Metric 10

To 3.3.3.3 List Num 0, count 2
    Lsp 4     Metric 0
    Lsp 5     Metric 0
To 3.3.3.3 List Num 1, count 1
    Lsp 6     Metric 1
```

show debug ip ospf all

Displays the status of the debugging of various modules.

Syntax

show debug ip ospf all

Parameters

None

Modes

Privilege Execution Mode

Examples

The following example shows the output of the **show debug ip ospf all** command.

```
 SLX# show debug ip ospf all
    BFD debugging is on
    events debugging is on
    packet debugging is on
    shortcuts debugging is on

SLX#
```

show debug ipv6 pim

Displays the state (on or off) of all IPv6 PIM debug flags.

Syntax

show debug ipv6 pim

Modes

Privileged EXEC mode

Examples

The following example shows sample output for the command.

```
device# show debug ipv6 pim

PIM debugging status:
--------------------------
add-del-oif     : off
bootstrap       : off
group           : off
join-prune      : on
nbr-change      : off
packets         : off
parent          : off
regproc         : on
route-change    : on
rp              : off
source          : off
--------------------------
```

show debug lacp

Displays the status of Link Aggregation Control Protocol (LACP) debugging on the device.

Syntax

show debug lacp

Modes

Privileged EXEC mode

show debug lldp

Displays the status of Link Layer Discovery Protocol (LLDP) debugging on the device.

Syntax

show debug lldp

Modes

Privileged EXEC mode

Examples

The following example displays the status of LLDP debugging on the device.

```
device# show debug lldp
 LLDP debugging status:
Interface Eth0/0    : Transmit Receive  Detail
```

show debug spanning-tree

Displays the status of STP debugging flags on the device.

Syntax

show debug spanning-tree

Modes

Privileged EXEC mode

show debug vrrp

Displays the status of Virtual Router Redundancy Protocol (VRRP) debugging on the device.

Syntax

show debug vrrp

Modes

Privileged EXEC mode

Usage Guidelines

This command is for VRRP and VRRP-E. You can modify or redirect the displayed information by using the default Linux tokens (|, >).

Examples

If you run this command and the debug parameter has already been set to debug all VRRP events, the following is displayed:

```
device# show debug vrrp
 VRRP event debugging is on
```

show defaults threshold

Displays the default thresholds for environmental and alert values for small form-factor pluggable (SFP) types.

Syntax

show defaults threshold sfp type *sfp-type*

Parameters

sfp-type

The following SFP types are supported:

1GCOP

— 1G SFP Copper

1GCWDM

— 1G SFP CWDM

1GLR

— 1G SFP LR

1GSR

— 1G SFP SR

10GDWDMT

— 10G SFP+ DWDM Tunable

10GER

— 10G SFP+ ER

10GLR

— 10G SFP+ LR

10GSR

— 10G SFP+ SR

10GUSR

— 10G SFP+ USR

10GZR

— 10G SFP+ ZR

40GER

— 40G QSFP+ ER4

40GESR

— 40G QSFP+ eSR4 INT

40GLM

— 40G QSFP+ LM4

40GLR

— 40G QSFP+ LR4

40GSR

— 40G QSFP+ SR4

40GSRINT

— 40G QSFP+ SR4 INT

100GAOC

— 100G QSFP28 AOC

100GCLR

— 100G QSFP28 CLR4

100GCWDM

— 100G QSFP28 CWDM4

100GESR

— 100G QSFP28 eSR4

100GLR

— 100G QSFP28 LR4

100GLRLT

— 100G QSFP28 LR4 Lite

100GPSM

— 100G QSFP28 PSM4

100GSR

— 100G QSFP28 SR4

Modes

Privileged EXEC mode

Usage Guidelines

You can modify these thresholds with the **threshold-monitor sfp** command.

Examples

The following example displays the default sfp thresholds for 1G SFP Copper.

```
device# show defaults threshold sfp type 1GCOP
Type: 1GCOP
+------------+-------------------------+-------------------------+---------+
|            |     High Threshold      |     Low Threshold       | Buffer |
| Area       | Value | Above  | Below  | Value     |  Below     | Value  |
|            |       | Action | Action |           |  Action    |        |
+------------+-------+--------+--------+-----------+------------+--------+
| Temp C     |    90 | raslog | none   |        -45|  raslog    |       0|
+------------+-------+--------+--------+-----------+------------+--------+
| RXP uWatts |   501 | raslog | none   |          6|  raslog    |       0|
+------------+-------+--------+--------+-----------+------------+--------+
| TXP uWatts |   794 | raslog | none   |         71|  raslog    |       0|
```

```
+------------+-------+--------+--------+-----------+-------------+--------+
| Current mA |    45 | raslog | none   |          1|  raslog     |       0|
+------------+-------+--------+--------+-----------+-------------+--------+
| Voltage mV |  3700 | raslog | none   |       2900|  raslog     |       0|
+------------+-------+--------+--------+-----------+-------------+--------+
```

show dot1x

Displays 802.1X-related information.

Syntax

show dot1x [**all**]

show dot1x [**interface ethernet** *slot/port*]

show dot1x [**diagnostics** | **session-info** | **statistics**] { **interface ethernet** *slot/port* }

Parameters

all

Displays detailed dot1x information for all of the ports.

interface

Displays the state of a specified interface.

diagnostics

Displays diagnostics information for the authenticator associated with a port.

session-info

Displays all statistical information of an established session.

statistics

Displays the statistics of a specified interface.

Modes

Privileged EXEC mode

Examples

The following example shows the overall state of 802.1X authentication on the system.

```
device# show dot1x
802.1X Port-Based Authentication: Enabled
PAE Capability:                   Authenticator Only
Protocol Version:                 2
Auth Server:                      RADIUS
Readiness test timeout:           10
RADIUS Configuration
--------------------
Position:                 1
Server Address:           10.24.65.6
Port:                     1812
Secret:                   xxxxxxxxx
Retry Interval:           5 seconds
```

The following example shows detailed 802.1X authentication information for all of the ports.

```
device# show dot1x all
802.1X Port-Based Authentication: Enabled
PAE Capability:                   Authenticator Only
Protocol Version:                 2
Auth Server:                      RADIUS
Readiness test timeout:           10

RADIUS Configuration
--------------------
Position:                 1
Server Address:           10.20.106.144
Port:                     1812
Secret:                   testing123
Retry Interval:           4 seconds

Position:                 2
Server Address:           10.20.106.189
Port:                     1812
Secret:                   testing123
Retry Interval:           4 seconds

802.1X info for interface Eth 1/31
---------------------------------
Port Control:             Auto
Protocol Version:         2
ReAuthentication:         Enabled
Auth Fail Max Attempts:   0
ReAuth Max:               2
Tx Period:                30 seconds
Quiet Period:             60 seconds
Supplicant Timeout:       30 seconds
Re-Auth Interval:         3600 seconds
Dynamic VLAN assigned:    50
Filter-strict-security:   Enabled
IP ACL assigned (IN|OUT): IPEXT-50 | IPEXT-OUT-50
MAC ACL assigned:         mac-ext
```

The following example shows all diagnostics information for the authenticator associated with a port.

```
device# show dot1x diagnostics interface ethernet 1/2
802.1X Diagnostics for interface Eth 1/2
----------------------------------------
authEnterConnecting:                1
authEaplogoffWhileConnecting:       0
authEnterAuthenticating:            1
authSuccessWhileAuthenticating:     1
authTimeoutWhileAuthenticating:     0
authFailWhileAuthenticating:        0
authEapstartWhileAuthenticating:    0
authEaplogoffWhileAuthenticating:   0
authReauthsWhileAuthenticated:      0
authEapstartWhileAuthenticated:     0
authEaplogoffWhileAuthenticated:    0
BackendResponses:                   11
BackendAccessChallenges:            10
BackendOtherrequestToSupplicant:    11
BackendAuthSuccess:                 1
BackendAuthFails:                   0
```

The following example shows state of a specified interface.

```
device# show dot1x interface ethernet 1/31
802.1X info for interface Eth 1/31
---------------------------------
Port Control:             Auto
Protocol Version:         2
ReAuthentication:         Enabled
Auth Fail Max Attempts:   0
ReAuth Max:               2
Tx Period:                30 seconds
Quiet Period:             60 seconds
Supplicant Timeout:       30 seconds
Re-Auth Interval:         3600 seconds
Dynamic VLAN assigned:    50
Filter-strict-security:   Enabled
IP ACL assigned (IN|OUT): IPEXT-50 | IPEXT-OUT-50
MAC ACL assigned:         mac-ext
```

The following example shows information for all clients on the port.

```
device# show dot1x session-info interface ethernet 1/2
802.1X Session info for interface Eth 1/2
----------------------------------------
Mac Address: 0021.5ec6.15ce
----------------------------------------
User Name:                md5user2
Session Time:             2 secs
Terminate Cause:          Not terminated yet
Session Status:           Authorized
PAE State:                Authenticated
BE State:                 Idle
VLAN:                     N/A
IP ACL (IN | OUT):        N/A | N/A
MAC ACL:                  N/A
Current Id:               18
Id From Server:           17
```

The following example shows the statistics of a specified interface.

```
device# show dot1x statistics interface ethernet 1/2
802.1X statistics for interface Eth 1/2
---------------------------------------
EAPOL Frames Rx:                    12
EAPOL Frames Tx:                    43
EAPOL Start Frames Rx:              1
EAPOL Logoff Frames Rx:             0
EAP Rsp/Id Frames Rx:               1
EAP Response Frames Rx:             10
EAP Req/Id Frames Tx:               23
EAP Request Frames Tx:              10
Invalid EAPOL Frames Rx:            0
EAPOL Length Error Frames Rx:       0
EAPOL Last Frame Version Rx:        1
Invalid EAP Frames Rx:              0
EAP Length Error Frames Rx:         0
EAPOL Last Frame Src:               0021.5ec6.15ce
```

show environment fan

Displays fan status information.

Syntax

show environment fan

Modes

Privileged EXEC mode

Output

The **show environment fan** command displays the following information:

Output field	Description
OK	Fan is functioning correctly at the displayed speed (RPM).
absent	Fan is not present.
below minimum	Fan is present but rotating too slowly or stopped.
above maximum	Fan is rotating too quickly.
unknown	Unknown fan unit installed.
faulty	Fan has exceeded hardware tolerance and has stopped. In this case, the last known fan speed is displayed.
Airflow direction	Port side intake or Port side exhaust. This value is not applicable to modular chassis.
speed	Fan RPM.

Examples

The following example displays fan status information:

```
device# show environment fan

Fan 1 is Ok, speed is 4243 RPM
Fan 2 is Ok, speed is 4249 RPM

Fan 3 is Ok, speed is 4402 RPM
```

show environment history

Displays the field-replaceable unit (FRU) history log.

Syntax

show environment history

Modes

Privileged EXEC mode

Usage Guidelines

The history log records insertion and removal events for field-replaceable units (FRUs), such as blades, power supplies, fans, and world wide name (WWN). The type of FRU supported depends on the hardware platform.

Output

The **show environment history** command displays the following information:

Output field	Description
Object type	Displays FAN, POWER SUPPLY, WWN (WWN card), or UNKNOWN.
Object number	Displays the unit number.
Event type	Displays Inserted, Removed, or Invalid.
Time of the event	Displays the date in the following format: Day Month dd hh:mm:ss yyyy.
Factory Part Number	Displays the part number (xx-yyyyyyy-zz) or Not available.
Factory Serial Number	Displays the FRU serial number (xxxxxxxxxxxx) or Not available.

Examples

The following example displays the FRU history on a device.

```
device# show environment history
POWER SUPPLY  Unit 1  Inserted at Sun Jul 12 21:59:17 2015
Factory Part Number:
Factory Serial Number:

POWER SUPPLY  Unit 2  Inserted at Sun Jul 12 21:59:17 2015
Factory Part Number:
Factory Serial Number:

FAN  Unit 1  Inserted at Sun Jul 12 21:59:17 2015
Factory Part Number:   60-1003113-03
Factory Serial Number: DUX0343K00A
```

```
(Output truncated)
```

show environment power

Displays the type and current status of the switch power supply.

Syntax

show environment power

Modes

Privileged EXEC mode

Output

The **show environment power** command displays the following status for each of the installed power supply:

Status	Description
OK	Power supply is functioning correctly.
absent	Power supply is not present.
unknown	Unknown power supply unit is installed.
predicting failure	Power supply is present but predicting failure. Replace the power supply as soon as possible.
faulty	Power supply is present but faulty (no power cable, power switch turned off, fuse blown, or other internal error).

The following information is also displayed for each of the installed and working power supply.

Field	Description
Manufacture ID	The manufacturer information for the power supply.
Part Number	The unique part number assigned for the power supply.
Serial Number	The unique serial number for this power supply.
Airflow	The direction of airflow. Can be one of *Port Side Intake* or *Port Side Exhaust*.
Type	The type of power supply. Can be either *AC* or *DC*.
Power In (W)	The input power in Watts.
Power Out (W)	The output power in Watts.
Current In (A)	The input current in Amperes.
Current Out (A)	The output current in Amperes.
Voltage In (V)	The input voltage in Volts.
Voltage Out (V)	The output voltage in Volts.

Field	Description
PS Fan (RPM)	The current speed in RPM of the fan installed in the power supply.
PS Temp1 (C)	The temperature reading, in Degree Celsius of sensor 1 installed in the power supply.
PS Temp2 (C)	The temperature reading, in Degree Celsius of sensor 2 installed in the power supply.
PS Temp3 (C)	The temperature reading, in Degree Celsius of sensor 3 installed in the power supply.

Examples

The following example displays the power supply status when one of the power supplies is absent.

```
SLX# show environment power

Power Supply #1 is OK
---
    Manufacturer ID     : ARTESYN
    Part Number         : 700-013684-0100
    Serial Number       : L214VP003L05P
    Airflow             : Port Side Intake
    Type                : AC
    Power In (W)        : 119
    Power Out (W)       : 102
    Current In (A)      : 0.62
    Current Out (A)     : 8.45
    Voltage In (V)      : 200.00
    Voltage Out (V)     : 12.18
    PS Fan (RPM)        : 3040
    PS Temp1 (C)        : 29
    PS Temp2 (C)        : 48
    PS Temp3 (C)        : 34

Power Supply #2 is absent

SLX #
```

The following example displays the power supply status for multiple power supply units where one of them is faulty.

```
SLX# show environment power

Power Supply #1 is faulty
---
    Manufacturer ID     : ARTESYN
    Part Number         : 700-013684-0100
    Serial Number       : L723VP003L05P
    Airflow             : Port Side Intake
    Type                : AC
    Power In (W)        : NA
    Power Out (W)       : NA
    Current In (A)      : NA
    Current Out (A)     : NA
    Voltage In (V)      : NA
    Voltage Out (V)     : NA
    PS Fan (RPM)        : NA
```

```
    PS Temp1 (C)        : NA
    PS Temp2 (C)        : NA
    PS Temp3 (C)        : NA

Power Supply #2 is OK
---
    Manufacturer ID     : ARTESYN
    Part Number         : 700-013684-0100
    Serial Number       : L214VP003L05P
    Airflow             : Port Side Intake
    Type                : AC
    Power In (W)        : 119
    Power Out (W)       : 102
    Current In (A)      : 0.62
    Current Out (A)     : 8.45
    Voltage In (V)      : 200.00
    Voltage Out (V)     : 12.18
    PS Fan (RPM)        : 3040
    PS Temp1 (C)        : 29
    PS Temp2 (C)        : 48
    PS Temp3 (C)        : 34

SLX #
```

The following example displays the output when the installed power supplies are OK.

```
SLX# show environment power

Power Supply #1 is OK
---
    Manufacturer ID     : ACBEL POWER
    Part Number         : FSG059-930G
    Serial Number       : B3293739294
    Airflow             : Port Side Intake
    Type                : DC
    Power In (W)        : 119
    Power Out (W)       : 102
    Current In (A)      : 0.62
    Current Out (A)     : 8.45
    Voltage In (V)      : 200.00
    Voltage Out (V)     : 12.18
    PS Fan (RPM)        : 3040
    PS Temp1 (C)        : 29
    PS Temp2 (C)        : 48
    PS Temp3 (C)        : 34

Power Supply #2 is OK
---
    Manufacturer ID     : ARTESYN
    Part Number         : 700-013684-0100
    Serial Number       : L783VP003L05P
    Airflow             : Port Side Intake
    Type                : DC
    Power In (W)        : 125
    Power Out (W)       : 110
    Current In (A)      : 0.79
    Current Out (A)     : 8.57
    Voltage In (V)      : 200.00
    Voltage Out (V)     : 12.38
    PS Fan (RPM)        : 3170
    PS Temp1 (C)        : 39
    PS Temp2 (C)        : 41
    PS Temp3 (C)        : 33
```

```
SLX #
```

show environment sensor

Displays the environment sensor status.

Syntax

show environment sensor

Modes

Privileged EXEC mode

Usage Guidelines

The command output displays the current temperature, fan, and power supply status readings from sensors located on the switch. For an explanation of power supply status values, refer to the **show environment power** topic.

Examples

The following example displays sensor readings on the device:

```
device# show environment sensor
sensor  1: (Temperature) is Ok, value is 31 C
sensor  2: (Temperature) is Ok, value is 53 C
sensor  3: (Temperature) is Ok, value is 52 C
sensor  4: (Temperature) is Ok, value is 37 C
sensor  5: (Temperature) is Ok, value is 32 C

(Output truncated)

sensor 50: (Fan         ) is Ok,speed is 4297 RPM
sensor 51: (Fan         ) is Ok,speed is 4240 RPM
sensor 52: (Fan         ) is Ok,speed is 4350 RPM
sensor 53: (Power Supply) is Ok
sensor 54: (Power Supply) is Ok
sensor 55: (Power Supply) is Absent
sensor 56: (Power Supply) is Absent
sensor 57: (Power Supply) is Absent
sensor 58: (Power Supply) is Absent
```

show environment temp

Displays information pertaining to the environment temperature.

Syntax

show environment temp

Parameters

detail

(Not currently supported) Specifies to display information in detail.

Modes

Privileged EXEC mode

Output

The command displays the following information

Output Field	Description
Sensor ID	The numerical ID of the sensor for which the values are being displayed.
Grid	The grid location captures the approximate XYZ location of the sensor within the switch and is formatted as XXZ-YY. This value is interpreted as follows: • The first two characters (XX) capture the sensor location along the depth of the chassis. The values are: ◦ NP - Non-port side ◦ PS - Port side ◦ MI - Middle • The third character indicates the vertical location of the sensor. The values are: ◦ T - Top of the board (sensors are not limited to the motherboard) ◦ B - Bottom of the board (sensors are not limited to the motherboard) • The last number captures the horizontal location of the sensor. It ranges from 0 to 10. ◦ 0 is at the left edge of the chassis. ◦ 10 is at the right edge of the chassis.
Description	The description of the location where the sensor is deployed and area it is monitoring.

Output Field	Description
State	The current state of the sensor along with its description. The states are as follows: • Ok • Alarm • Critical
Value (C)	The current temperature value (in degree Celsius) for the monitored area.
Threshold (C) AL	The configured Alarm threshold value (in degree Celsius) for the monitored area. If alarm threshold value is not configured, this will display *N/A*.
Threshold (C) CR	The configured Critical threshold value (in degree Celsius) for the monitored area. If critical threshold value is not configured, this will display *N/A*.

Usage Guidelines

Caution

The *Critical* notification is generated at a temperature that is lower than the configured critical temperature. This is to enable the SLX-OS to generate and send the appropriate notifications before the device is shutdown on reaching the configured critical temperature.

Examples

This example displays the environment temperature.

```
 SLX# show environment temp

Sensor  Grid    Description            State          Value  Thresholds(C)
  ID                                                   (C)     AL     CR
================================================================================
  1     NPT-4   CPU Board 1            Alarm            74     73     77
  2     NPB-5   CPU Board 2            Critical         79     76     80
  3     PST-9   MGMT Board 1           Ok               31     55     59
  4     MIT-4   Switch ASIC 1          Ok               47     73     77
  5     MIB-5   Switch ASIC 2          Ok               48     78     82
  6     MIB-3   CoProcessor 1          Ok               40     76     80
  7     MIT-3   CoProcessor 2          Ok               41     69     73
  8     MIB-4   Fan Controller 1       Ok               45     71     75
  9     NPB-6   Fan Controller 2       Ok               34     63     67
 10     MIT-9   Fan Controller 3       Ok               35     61     65
 11     MIT-6   Switch ASIC 3          Ok               47     83     N/A
================================================================================

Legend for 'Grid' column:
-------------------------
First two letters: NP = Non-Port side; PS = Port side; MI = Middle
Third letter: T = Top of the board; B = Bottom of the board
Number: 0 = Left chassis edge; 5 = Middle; 10 = Right chassis edge
```

```
SLX#
```

show erp

Displays information about all Ethernet Ring Protocol (ERP) instances, or for a specified instance.

Syntax

show erp [*erp_id*]

Parameters

erp_id

Specifies an ERP ID.

Modes

Privileged EXEC mode

Examples

The following example displays information about all ERP instances.

```
device# show erp
ERP 5 (Version 2) - VLAN 6
================================================================================
Erp ID  Status     Oper              Node          Non-revertive      Topo
                   state             role          mode               group
5       enabled    Idle              rpl-node      disabled           -

Fast         Ring         WTR        WTB        Guard      Holdoff    Msg
convergence  type         time(min)  time(ms)   time(ms)   time(ms)   intv(ms)
enabled      Major ring   5          5500       1500       0          5000

Raps-default-mac   Parent-ring-erp-id   Raps-propagate-tc   Mel-Config   Mel-Oper
ON                 0                    OFF                 2            3

I/F     Port       ERP port state   Interface status   Interface type
L       eth0/4     forwarding       normal              non-rpl
R       eth0/7     blocking         normal              rpl
```

show erp statistics

Displays statistics for a specified Ethernet Ring Protocol (ERP) instance.

Syntax

show erp statistics *erp_id*

Parameters

erp_id

Specifies an ERP ID.

Modes

Privileged EXEC mode

Examples

The following example displays statistics for ERP instance 1.

```
device# show erp statistics 1
ERP: 1, VLAN 222

Left interface: Port eth1/3
Physical state - UP, ERP Port state - blocking

                 Transmitted    Received       Ignored        Dropped
RAPS(FS)         0              0              0              0
RAPS(SF)         6              3              0              0
RAPS(MS)         0              0              0              0
RAPS(NR)         3              934262         3              3
RAPS(EVENT)      1284           0              0              1375
INVALID          0              0              0              0

Right interface: Port eth1/12
Physical state - UP, ERP Port state - forwarding

                 Transmitted    Received       Ignored        Dropped
RAPS(FS)         0              0              0              0
RAPS(SF)         6              0              0              0
RAPS(MS)         0              0              0              0
RAPS(NR)         3              59             3              0
RAPS(EVENT)      1284           0              0              1284
INVALID          0              0              0              0
```

show event-handler activations

Displays operational data of activated event-handlers.

Syntax

show event-handler activations

Modes

Privileged EXEC mode

Output

The **show event-handler activations** command displays the following information:

Output field	Description
Event-handler	Displays the event-handler name.
Last Trigger Activation Time	Displays the time of the last trigger activation. If no trigger was activated, displays "Never".
Total Trigger Activations	Displays the total number of trigger activations.
Last Action Completion Time	Displays the completion time of the last event-handler action run. If no event-handler action ran, displays "Never".
Last Action Completion Status. Exit Code =	Displays the status of the last completed event-handler action. If the Python script assigns exit codes, such codes are displayed here. An exit code of 0 indicates one of the following: • No code was assigned to this condition. • The script author assigned 0 to a specified condition.
Total Action Completions	Displays the number of completed event-handler actions.

Examples

The following example displays event-handler operational data.

```
device# show event-handler activations

Event-handler : evh1
Last Trigger Activation Time: 2015-04-30 17:28:12
Total Trigger Activations: 25
Last Action Completion Time: 2015-04-30 17:28:57
Last Action Completion Status: Exit Code = 0
Total Action Completions: 25

Event-handler : evh2
Last Trigger Activation Time: 2015-04-28 22:02:51
Total Trigger Activations: 8
Last Action Completion Time: 2015-04-28 22:02:58
Last Action Completion Status: Exit Code = 0
Total Action Completions: 8
```

show file

Displays the contents of a file in the local flash memory.

Syntax

show file *filename*

Parameters

filename

The name of the file to be displayed.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local device.

Examples

The following example displays the contents of a file in the flash memory.

```
device# show file defaultconfig.cluster
vlan dot1q tag native
!
cee-map default
remap fabric-priority priority 0
remap lossless-priority priority 0
priority-group-table 15.0 pfc off
priority-group-table 1 weight 40 pfc on
priority-group-table 2 weight 60 pfc off
priority-table 2 2 2 1 2 2 2 15.0
!!
port-profile default
vlan-profile
  switchport
  switchport mode trunk
  switchport trunk allowed vlan all
!
interface Port-channel 1
vlag ignore-split
  description Homerun port-channel on MM1
  shutdown
!
interface Port-channel 2
  vlag ignore-split
  description Homerun port-channel on MM2
  shutdown
!
protocol lldp
!!
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
```

```
logging auditlog class SECURITY
!
end
```

show firmware peripheral cpld

Displays the current and latest version of the Complex Programmable Logic Device (CPLD).

Syntax

show firmware peripheral cpld

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The firmware upgrade can be invoked from either Linux shell or SLX CLI console. The Linux shell command is **cpld_upgrade -p**.

Output

The **show firmware peripheral cpld** command displays the following information:

Output field	Description
Type	The identifier of the CPLD.
Current Version	The current version.
Latest Version	The latest available version for the CPLD.

Examples

This example displays output for an SLX 9540.

```
device# show firmware peripheral cpld
+----------+---------------+----------------+
|  Type    | Current Version| Latest Version |
+----------+---------------+----------------+
|  CPLD0   | 02/09/2017(92) | 02/09/2017(92) |
+--------- +---------------+----------------+
|  CPLD1   | 02/09/2017(92) | 02/09/2017(92) |
+--------- +---------------+----------------+
```

This example displays output for an SLX 9640.

```
device# show firmware peripheral cpld
+----------+---------------+----------------+
|  Type    | Current Version| Latest Version |
+----------+---------------+----------------+
|  CPLD0   | 02/09/2017(92) | 02/09/2017(92) |
+--------- +---------------+----------------+
```

```
|  CPLD1   | 02/09/2017(92) | 02/09/2017(92) |
+--------- +----------------+----------------+
```

show firmware peripheral fpga

Displays the current and latest version of the Field Programmable Gate Array (FPGA).

Syntax

show firmware peripheral fpga

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The firmware upgrade can be invoked from either Linux shell or SLX CLI console. The Linux shell command is **fpga_upgrade -p**.

Examples

This example displays output for an SLX 9540.

```
device# show firmware peripheral fpga
+---------------+--------------------------+-------------------------------------+
|     Type      |   Current Version    |   Latest Version Availalble   |
+---------------+--------------------------+-------------------------------------+
|    sysfpga    |    09/28/2016(54)    |        09/28/2016(54)             |
+---------------+--------------------------+-------------------------------------+
```

This example displays output for an SLX 9640.

```
device# show firmware peripheral fpga
System FPGA version: 0x18050350
```

show firmwaredownloadhistory

Displays the firmware download history for the device.

Syntax

show firmwaredownloadhistory

Modes

Privileged EXEC mode

Usage Guidelines

The log records the date and time of the firmware download, the device name, slot number, process ID, and firmware version.

Examples

The following example displays the firmware download history.

```
SLX# show firmwaredownloadhistory

Firmware version history

Sno   Date & Time                Switch Name  Slot  PID    OS Version
1     Thu Mar  2 05:52:27 2017   SLX          0     33552  17r.1.00
2     Wed Feb 22 17:10:45 2017   SLX          0     3187   16r.1.00
```

show firmwaredownloadstatus

Displays the firmware download activity log.

Syntax

show firmwaredownloadstatus [**brief**] [**summary**]

Parameters

brief

Displays only the last entry of the firmware download event log.

summary

Displays a high-level summary of the firmware download status.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display an event log that records the progress and status of events that occur during a firmware download. The event log is created by the **firmware download** command and is retained until you issue another **firmware download** command. A time stamp is associated with each event.

The output of **show firmwaredownloadstatus** and **show firmwaredownloadstatus brief** are equivalent.

The output varies depending on the hardware platform.

Examples

The following example displays the firmware download event log.

```
device# show firmwaredownloadstatus
 [1]: Wed Mar  1 21:58:34 2017
Slot M1: Firmware install begins.

[2]: Wed Mar  1 22:03:59 2017
Slot M1: Firmware install ends.

[3]: Wed Mar  1 22:03:59 2017
Slot M1: Firmware starts to swap.

[4]: Wed Mar  1 22:04:19 2017
Slot M1: Firmware is swapped.

[5]: Wed Mar  1 22:04:20 2017
Slot M1: The blade begins to reboot.

[6]: Wed Mar  1 22:09:03 2017
```

```
Slot L2/0: Firmware install begins.

[7]: Wed Mar  1 22:09:08 2017
Slot L4/0: Firmware install begins.

[8]: Wed Mar  1 22:11:37 2017
Slot L2/0: Firmware install ends.

[9]: Wed Mar  1 22:11:37 2017
Slot L2/0: Firmware starts to swap.

[10]: Wed Mar  1 22:11:46 2017
Slot L4/0: Firmware install ends.

(Output truncated)
```

The following example displays a high-level summary of the firmware download status.

```
device# show firmwaredownloadstatus summary
No Firmware Download session in progress.
```

show grubversion

Displays the installed version of ONIE-GRUB.

Syntax

show grubversion

Modes

Privileged EXEC Mode

Usage Guidelines

This command is only supported on the SLX 9150, SLX 9250, Extreme 8720, and Extreme 8520 devices.

Examples

This example shows the usage of the command.

```
SLX # show grubversion
grub_version="2.06"
SLX #
```

show hardware media-database

Displays the supported media types listed in the hardware media database for the device.

Syntax

show hardware media-database [**all** | **sfp** | **qsfp** | **qsfp28**]

Parameters

all

Specifies all media types in the mediavdatabase.

sfp

Specifies all SFP (small form factor pluggable) media in the media database.

qsfp

Specifies all QSFP (quad small form factor pluggable) media in the media database.

qsfp28

Specifies all QSFP28 (QSFP for 4x28Gbps) media in the media database.

Modes

Privileged EXEC mode

Usage Guidelines

The media database contains the list of port media supported on the device, saved in an .xml file on the device. The default version is provided in the release package. You can download your own version or upload the file to a remote server for modification using the **copy** command. After you download a new media database to the device, you need to activate it.

Examples

This example displays typical output for the QSFP2 media type.

```
device# show hardware media-database qsfp28
qsfp28 Media Database
-------------------------------------------------------------------------------
      Part Number    Vendor             Description
-------------------------------------------------------------------------------
       NDAAFF-0004   Amphenol           100G-QSFP-28 3m cable passive
       NDAAFF-0003   Amphenol           100G-QSFP-28 1m cable passive
     58-0000044-01   Extreme Networks   100G-QSFP28 1m Passive Cable    28 5m
  EQPC1HPCZ50C0100   Extreme Networks   100G Passive DAC QSFP28 0.5mxSFP2able
  EQPT1H4PS4FCM1PG   Extreme Networks   100G PSM4 QSFP28 2km Pigtailedm Cable
  EQPT1H4SR4UCM100   Extreme Networks   100G SR4 QSFP28 100m0mFP28 10m TAA
  EQPT1H4SW4UCL100   Extreme Networks   100G SWDM4 QSFP28 100m8 to 2xQSFP28 3m
  EQPA1HQPSP0C0100   Extreme Networks   100G QSFP28 to SFP28 adapterxQSF28 3mm
```

```
  EQPC1HPC050C0100   Extreme Networks   100G Passive DAC QSFP28 5m 4xSFP2
  EQPT1H4BD2UCL100   Extreme Networks   100G SR4 - BiDi QSFP28 100mm
```

This example displays typical output for the SFP media type.

```
device# show hardware media-database  sfp
SFP Media Database
-------------------------------------------------------------------
      Part Number       Vendor     Description
-------------------------------------------------------------------
      33210-100         AVAGO      1000Base-SX
      33210-100         FINISAR    1000Base-SX
      33211-100         FINISAR    1000Base-LX
      33211-100         AVAGO      1000Base-LX
      33002-100         AVAGO      1G Copper SFP
  57-1000042-02         Extreme    1000Base(copper)
  57-1000042-01         Extreme    1000Base(copper)
  57-0000075-01         Extreme    10GE SR SFP+
  57-1000130-01         Extreme    10GE LRM SFP+
  57-1000130-02         Extreme    10GE SFP+
  58-1000019-01         Extreme    10GE Twinax SFP+-P-0501
  58-1000023-01         Extreme    10GE Direct Attach 5M Active
  58-1000024-01         Extreme    10GE Direct Attach 1M Passive
  58-1000026-01         Extreme    10GE Direct Attach 1M Active
  58-1000025-01         Extreme    10GE Direct Attach 3M Passive
  58-1000027-01         Extreme    10GE Twinax Attach 3M Active
  57-1000273-01         Extreme    10GE AOC 7m Optic Cable
  57-1000274-01         Extreme    10GE AOC 10m Optic Cable
```

show hardware profile

Displays details of the active hardware profile, with options to filter by TCAM profile, counter profile, or LAG profile.

Syntax

show hardware profile

show hardware profile route *profile-name*

show hardware profile cam-share

show hardware profile counters { **counter-profile-1** | **counter-profile-2** | **counter-profile-3** | **counter-profile-4** | **counter-profile-5** | **counter-profile-6** | **default** }

show hardware profile current [**usage**]

show hardware profile etcam { **default** | **ipv4-v6-route** | **ipv6-route** }

show hardware profile lag { **default** | **lag-profile-1** }

show hardware profile tcam { **app-telemetry** | **border-routing** | **default** | **layer2-ratelimit** | **multicast-profile** | **vxlan-visibility** }

Parameters

route *profile-name*

Specifies route information for the specified profile.

cam-share

(SLX 9540 or SLX 9640) Specifies cam-share information.

counters

(SLX 9540 or SLX 9640) Specifies hardware resources for counter profiles.

counter-profile-1

Specifies resources optimized for Ingress ACL, OF, and Egress ACL, with forward and drop counting for Layer 4 ingress traffic.

counter-profile-2

Specifies resources optimized for OF, MPLS, VPLS, VLL, and MCT, with hit counting for Layer 4 ingress traffic.

counter-profile-3

Specifies resources optimized for MPLS, VPLS, VLL, MCT, with hit counting for Layer 4 ingress traffic.

counter-profile-4

Specifies resources optimized for Layer 4 traffic, with forward and drop counting for all Layer 4 ingress traffic.

counter-profile-5

Specifies resources optimized for egress rate limit, with support for counting up to 32,000 VOQs.

counter-profile-6

Specifies resource optimized for reporting egress VE traffic statistics. This is only supported on SLX 9540 and SLX 9640 devices where the corresponding counter engines are setup for counting egress VE statistics.

default

Specifies resources optimized for VLAN and BD local switching, and MCT, with hit counting for Layer 4 ingress and egress traffic.

current

Displays details of the current active hardware profile.

usage

Displays usage information for the current active profile.

etcam

(SLX 9640 only) Specifies hardware resources for external TCAM (ETCAM) profiles.

default

Displays the details of the default ETCAM.

ipv4-v6-route

Displays the details of the ETCAM ipv4-v6-route.

ipv6-route

Displays the details of the ETCAM ipv6-route.

lag

(SLX 9540 or SLX 9640) Specifies hardware resources for link aggregation (LAG) profiles.

default

Specifies the default profile.

lag-profile-1

Specifies a modified LAG profile.

tcam

(SLX 9540 or SLX 9640) Specifies hardware resources for TCAM profiles.

app-telemetry

Optimizes resources for application telemetry.

border-routing

Optimizes resources for BGP Flowspec, ACLs, and so forth.

default

Optimizes resources with basic support for all applications.

layer2-ratelimit

Optimizes resources for Layer 2 ACL egress rate-limiting and related applications.

multicast-profile

Optimizes resources for IPv6 multicast. Layer 2 is also supported.

vxlan-visibility

Optimizes resources for VXLAN transit and termination, and GRE tunnel.

Output

FreeCnt (C,D,F)	The available filters for a threshold group. A Threshold Group is a collection of filters. • C - The total number of filters available for use. In a multi unit device, this value is the sum total of available filters. • D - The maximum number of available filters. In a multi unit device, this value is for a unit in that device. This value is tracked for the Threshold Group. When any filter in the Threshold Group is used, this value is decremented. • F - The number of free filters available for use. This is tracked on a per feature basis. When a filter is used, this value is decremented, however, the number of available free filters for other members in the Threshold Group does not change.
Threshold Group	The name of the Threshold Group. Threshold Group is a collection of features, some of which, might be user configurable.

Modes

Privileged EXEC mode

Usage Guidelines

If the profile counters are changed from **default** to **counter-profile-** and the statistics-based encapsulations are not available, then the LSPs that need statistics will not be brought up (either due to exhaustion or due to activating a counter profile that does not support statistics).

You can check whether the statistics-based encapsulations are needed by using the **show run router mpls policy** command to see if statistics are enabled in MPLS. LSPs that have auto-bandwidth configured and bridge-domains that have statistics configured also need statistics-based encapsulations.

If statistics are enabled, the LSPs and bridge-domains stay down. In the case of LSPs, the **show mpls lsp** {**detail** | **extensive** | **name** <*lsp name*>} command displays, "Statistics not available" in the down reason code.

This example shows profile information for an SLX 9740.

```
SLX# show hardware profile route default

switch type: SLX9740-40C

_____________________________________________________________________
    SLX ROUTE profile: DEFAULT
        v4mcast: 16384
        v6mcast: 8192
        ipv4-routes: 2048000
        ipv6-routes: 2048000
        ECMP next-hops: 32768
        next-hops: 65536
        arp: 104448
        ipv6 nd: 104448
        l2-mac: 614400
```

Examples

The following example displays details of the current active hardware profile.

```
device# show hardware profile current
 switch type:

                      current TCAM profile:    DEFAULT
                                   l2-acl:    2038
                                 l3v4-acl:    6134
                                 l3v6-acl:    6134
                           l3v4-acl-vxlan:    0
                                 l2l3v4Of:    0
                                egrl2-acl:    2038
                                egrl3-acl:    2038
                                  l3v6-of:    0
                                 Flex-acl:    0
                              App_tel_acl:    0
_____________________________________________________________________

                  current SLX ROUTE profile:    ROUTE-DEFAULT
                                      hwopt:    Disabled
                                  v4FibComp:    Disabled
                                  v6FibComp:    Disabled
                                   multivrf:    Disabled
_____________________________________________________________________
                      current LAG  profile:    LAG-DEFAULT
                                   max-lag:    64
_____________________________________________________________________

             current COUNTERS profile:    COUNTERS-PROFILE-6
                            InLIF - HitCount:    16384
                             InL4 - HitCount:    16384
                             InVE - HitCount:    0
                           OutLIF - HitCount:    16384
                            OutL4 - HitCount:    0
                            OutVE - HitCount:    16384
_____________________________________________________________________
                        current CAM Share:
                                   l2In-acl:    no
                                 l3v4In-acl:    no
                                   l3v4-pbr:    no
                                 l3v6In-acl:    no
                                   l3v6-pbr:    no
                                       Ofv4:    no
                                     Ofl3v6:    no
```

The following example displays details of the default counters profile.

```
device# show hardware profile counters default
 switch type: SLX

                           COUNTERS profile:    COUNTERS-DEFAULT
                           InLIF - HitCount:    32768
                            InL4 - HitCount:    16384
                  InVE - HitCount:    12288
                          OutLIF - HitCount:    16384
                           OutL4 - HitCount:    16384
                   OutVE - HitCount:    12288
```

The following example displays information about a specific LAG profile.

```
device# show hardware profile lag lag-profile-1

 switch type: SLX9540

                               LAG  profile:    LAG-PROFILE-1
                                    max-lag:    64
```

The following example displays information about a specific TCAM profile.

```
device# show hardware profile tcam layer2-optimised-1

 switch type: SLX9540

                              TCAM profile:    LAYER2-OPT-1
                                    l2-acl:    6134
                                  l3v4-acl:    6134
                                  l3v6-acl:    2038
                             l3v4-acl-vxlan:    0
                                  l2l3v4Of:    0
                                 egrl2-acl:    1014
                                 egrl3-acl:    1014
                                   l3v6-of:    0
                                  Flex-acl:    0
                                App_tel_acl:    0
```

The following example displays information about profile etcam default, ipv4-v6-route, and ipv6 route.

```
device# show hardware profile etcam default
switch type: SLX9640

                              ETCAM profile:    DEFAULT
                                ipv4-routes:    4000000
                                ipv6-routes:    256000

_____________________________________________________________________

device# show hardware profile etcam ipv4-v6-route
switch type: SLX9640

                              ETCAM profile:    IPV4-V6-ROUTE
                                ipv4-routes:    4000000
                                ipv6-routes:    700000

_____________________________________________________________________

device# show hardware profile etcam ipv6-route

switch type: SLX9640

                              ETCAM profile:    IPV6-ROUTE
```

```
                                ipv4-routes:    1000000
                                ipv6-routes:    1000000
```

The following example shows the cam-sharing status.

```
device# show hardware profile cam-share
switch type: SLX9540
    CAM Share:
          l2In-acl:    no
             l3v4In-acl:  no
             l3v4-pbr:    no
             l3v6In-acl:  no
             l3v6-pbr:    no
             Ofv4:        no
                Ofl3v6:      no
```

The following example displays the hardware profile scale.

```
switch type: SLX9540
SLX# show hardware profile counters counter-profile-6
 switch type: BR-SLX9540

_____________________________________________________________________

                           COUNTERS profile:    COUNTERS-PROFILE-6
                           InLIF - HitCount:    16384
                            InL4 - HitCount:    16384
                            InVE - HitCount:    0
                          OutLIF - HitCount:    16384
                           OutL4 - HitCount:    0
                           OutVE - HitCount:    16384
_____________________________________________________________________
SLX# show hardware profile counters counter-profile-6

 switch type: BR-SLX9640

_____________________________________________________________________

                           COUNTERS profile:    COUNTERS-PROFILE-6
                           InLIF - HitCount:    16384
                            InL4 - HitCount:    16384
                            InVE - HitCount:    0
                          OutLIF - HitCount:    16384
                           OutL4 - HitCount:    0
            OutVE - HitCount:    16384
```

This is the part output of the command showing the 128 ECMP maximum path information.

```
SLX# show hardware profile

<Other output for the command>

_____________________________________________________________________

current SLX ROUTE profile: DEFAULT

Maximum paths:       128
v4mcast:             16384
v6mcast:             8192
ipv4-routes:         2048000
ipv6-routes:         2048000
ECMP next-hops:      32768
next-hops:           65536
arp:                 104448
ipv6 nd:             104448
l2-mac:              600000
rhFlowsetSize:       32768
```

```
8pathFlowsetSize:    128
16pathFlowsetSize:   128
64pathFlowsetSize:   512
128path FlowsetSize: 512

<Other output for the command>
```

The following example displays the output of the usage of ACL resources.

```
SLX (config)# do show hardware profile current usage

Listing Content for Current Profile - DEFAULT(0)
Supported Feature List in Profile 0 for Slot 0 Chip 0
 ========================================================
         Feature-Name(value) Con  DB    Size  Max   Curr    FreeCnt(C,D,F)  Threshold
                             Id  Id         Limit Usage                        Group
                 L2_CTRL( 0)   0   0   FIXED   400     0 ( 2037, 1023,  400)       NA
              L3_V4_CTRL( 1)   0   0   FIXED   400     0 ( 2037, 1023,  400)       NA
         L2_USER_INGRESS( 3)   3   5   FIXED  2045     0 ( 2045, 2045, 2045)   MAC_IN
         L2_USER_WITH_RL( 4)   3   5   FIXED  2045     0 ( 2045, 2045, 2045)   MAC_IN
          L2_USER_EGRESS( 5)   7  10   FIXED  1024     0 ( 2048, 1024, 1024)  MAC_OUT
                 PORT_RL( 7)   0   0   FIXED   400     0 ( 2037, 1023,  400)       NA
                  BUM_RL( 8)   0   0   FIXED   400     0 ( 2037, 1023,  400)       NA
            GLOBAL_BD_RL( 9)   0   0 DYNAMIC  1024     0 ( 2037, 1023, 1024)       NA
              PORT_BD_RL(10)   0   0 DYNAMIC  1024     0 ( 2037, 1023, 1024)       NA
 DAI_AND_ARP_SUPPRESSION(11)   0   0 DYNAMIC  1024     1 ( 2037, 1023, 1023)       NA
    L3_IPV4_USER_INGRESS(13)   1   3 DYNAMIC  8190     0 (16370, 8190, 8190)  IPv4_IN
     L3_IPV4_USER_EGRESS(14)   7  11   FIXED  1024     0 ( 2048, 1024, 1024) IPv4_OUT
L3_IPV4_VXLAN_VISIBILITY(15)   1   3 DYNAMIC  8190     2 (16370, 8178, 8188)  IPv4_IN
    L3_IPV4_USER_WITH_RL(16)   1   3 DYNAMIC  8190    10 (16370, 8178, 8180)  IPv4_IN
            L3_IPV4_RACL(17)   1   3 DYNAMIC  8190     0 (16370, 8178, 8190)  IPv4_IN
             L3_IPV4_PBR(18)   1   3 DYNAMIC  8190     0 (16370, 8178, 8190)  IPv4_IN
    L3_IPV6_USER_INGRESS(19)   2   4 DYNAMIC  2047     0 ( 2047, 2047, 2047)  IPv6_IN
    L3_IPV6_USER_WITH_RL(21)   2   4 DYNAMIC  2047     0 ( 2047, 2047, 2047)  IPv6_IN
            L3_IPV6_RACL(22)   2   4 DYNAMIC  2047     0 ( 2047, 2047, 2047)  IPv6_IN
             L3_IPV6_PBR(23)   2   4 DYNAMIC  2047     0 ( 2047, 2047, 2047)  IPv6_IN
       L3_IPV4_FLOW_SPEC(35)   1   3 DYNAMIC  8190     0 (16370, 8178, 8190)  IPv4_IN
       L3_IPV6_FLOW_SPEC(36)   2   4 DYNAMIC  2047     0 ( 2047, 2047, 2047)  IPv6_IN
         L3_IPV4_RACL_RL(37)   1   3 DYNAMIC  8190     0 (16370, 8178, 8190)  IPv4_IN
         L3_IPV6_RACL_RL(38)   2   4 DYNAMIC  2047     0 ( 2047, 2047, 2047)  IPv6_IN
           L3_IPV4_BCAST(39)   1   3 DYNAMIC  8190     0 (16370, 8178, 8190)  IPv4_IN
     L2_USER_EGR_WITH_RL(41)   7  10   FIXED  1024     0 ( 2048, 1024, 1024)  MAC_OUT
L3_IPV4_USER_EGR_WITH_RL(42)   7  11   FIXED  1024     0 ( 2048, 1024, 1024) IPv4_OUT
          PORT_BD_EGR_RL(44)   7  10   FIXED  1024     0 ( 2048, 1024, 1024)  MAC_OUT
            L2_IPV4_SIPG(45)   1   3 DYNAMIC  8190     0 (16370, 8178, 8190)  IPv4_IN


 Note: [C] indicate CamShare Enabled is enabled for that feature.

SLX (config)#
```

In the above example, the field FreeCnt (C,D,F) displays the available filters for a Threshold Group, where a Threshold Group is a collection of filters.

- C - The total number of filters available for use. In a multi unit device, this value is the sum total of available filters.
- D - The maximum number of available filters. In a multi unit device, this value is for a unit in that device. This value is tracked for the Threshold Group. When any filter in the Threshold Group is used, this value is decremented.

- F - The number of free filters available for use. This is tracked on a per feature basis. When a filter is used, this value is decremented, however, the number of available free filters for other members in the Threshold Group does not change.

The field, Threshold Group, displays the name of the Threshold Group. A Threshold Group is a collection of features, some of which, might be user configurable.

show hardware smt

Displays the active setting for simultaneous multithreading (SMT) and the setting for the next device reboot.

Syntax

show hardware smt

Modes

Privileged EXEC mode

Usage Guidelines

This feature is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only..

Because new SMT settings take effect only after the device is rebooted, the current and next SMT settings can be different after you update the SMT settings but before you reboot the device.

Examples

This example shows typical output for the command.

```
device# show hardware smt
Current:  Enabled, Next Reboot: Disabled
```

show history

Displays the history of commands executed on the device during the current session.

Syntax

show history [*number*]

Parameters

number

Specifies the number of commands to display. Values range from 1 through 1000.

Modes

Privileged EXEC mode

Usage Guidelines

If you enter this command without specifying a number, up to 1000 commands are displayed.

Examples

The following command displays the three last commands entered.

```
device# show history 3
12:45:23 -- show interface switchport
12:45:37 -- show interface stats brief
12:45:45 -- show arp vrf test
```

show http server status

Displays HTTP and HTTPS server status information.

Syntax

show http server status

Modes

Privileged EXEC mode

Output

The **show http server status** command displays the following information:

Output field	Description
VRF-Name	VRF name
Status	HTTP and HTTPS server status (enabled or disabled)

Examples

The following example displays HTTP and HTTPS server status information.

```
 device# show http server status

VRF-Name: mgmt-vrf       Status: HTTP Enabled and HTTPS Disabled
VRF-Name: default-vrf    Status: HTTP Enabled and HTTPS Disabled
```

show hw route-info

Displays IP routes information related to longest exact match (LEM) and longest prefix match (LPM).

Syntax

show hw route-info { **interface** *slot/port* | **linecard** *number* }

Parameters

interface *slot* **/** *port*

Specifies an interface. For devices without slots, specify **0**.

linecard *number*

Specifies the linecard or device level. For devices without slots, specify **0**.

Modes

Privileged EXEC mode

Output

The **show hw route-info** command displays the following information:

Output field	Description
LEM	Route status and count.
LPM	Route status and count.

Examples

The following example displays hardware route information.

```
device# show hw route-info linecard 0

HW-Route-Info
=====================================================

Slot 0

Tower 0
LEM
Total Entries           :750000
95% Threshold           :712500
85% Threshold           :637500
Total In Use            :58 (.000000%)
        IPV4  routes    :58
        IPV6  routes    :0
Status                  :Green

LPM
Total Entries           :1000000
```

```
95% Threshold           :950000
85% Threshold           :850000
Total In Use            :696 (.000000%)
        IPV4  routes    :0
        IPV6  routes    :174
Status                  :Green

eTCAM
Total Entries           :4000000
95% Threshold           :3800000
85% Threshold           :3400000
Total In Use            :156 (.000000%)
        IPV4  routes    :156
        IPV6  routes    :0
Status                  :Green
```

show interface

Displays the detailed interface configuration and capabilities of all interfaces or for specified interfaces.

Syntax

show interface [**description**]

show interface [**ethernet** *slot* **/** *port* | **port-channel** *number*]
[**switchport**]

show interface loopback *number*

show interface management [*management-id*]

show interface trunk

Parameters

description

For all device interfaces, displays a summary that includes the Description field.

ethernet

Specifies an Ethernet interface.

slot

Specifies a valid slot number. For devices that do not support line cards, specify **0**.

port

Specifies a valid port number.

port-channel *number*

Specifies a port-channel number.

switchport

Specifies Layer 2 interfaces.

loopback *number*

Specifies a loopback interface.

management *management-id*

Specifies the management interface. The only supported value is **0**.

trunk

Displays VLANs on the trunk.

Modes

Privileged EXEC mode

Output

The **show interface ethernet** command displays the following information:

Output field	Description
Ethernet *slot* **/** *port*	Displays the port state. The states are "admin down, line protocol is down (admin down)" or "up, line protocol is up (connected)".
Redundant management mode	Displays "enabled" if so configured. (SLX-9250 only)
Hardware	Displays the MAC address of the Ethernet interface.
Pluggable media	Displays "present" or "not present".
Interface index	Displays the interface index.
MTU	Displays the maximum transmission unit (MTU), in bytes.
*n*G interface	Displays the speed of the Ethernet interface, in Gb.
Transparent phy loopback	If **loopback phy** was configured on the interface, displays "configured". If not configured, this line is not displayed.
LineSpeed Actual	Displays the actual line speed in Mb or "Nil".
LineSpeed Configured	Displays "Auto" or a value in Mb.
Duplex	Displays "Half" or "Full".
Priority Tab	Displays "enable" or "disable".
Reload Delay	Displays reload-delay time value, and remaining time, in seconds.
Forward LACP PDU	Displays "enable" or "disable".
Route Only	Displays "enabled" or "disabled".
Queueing strategy	Displays "FIFO".
Primary Internet Address	Displays the primary Internet address
Broadcast	Displays the broadcast Internet address
Receive Statistics	Displays receive statistics: packets, bytes, unicasts, multicasts, broadcasts, packets by byte size, runts, jabbers, cyclic redundancy check (CRC), overruns, errors, and discards.
Transmit Statistics	Displays transmit statistics: packets, bytes, unicasts, multicasts, broadcasts, underruns, errors, and discards.
Rate info	Displays input and output in Mbits/sec, packets/sec, and percentage of the line rate.
Route-Only Packets Dropped	Displays the number or routing-only packets dropped.
FEC - Mode	Displays the current FEC mode of the interface. FEC mode can be *FC-FEC*, *RS-FEC*, or *Disabled*.
FEC - Corrected Blocks	Displays the number of corrected Blocks. Displays Zero (0) when FEC is *Disabled* or is not supported.

Output field	Description
FEC - Uncorrected Blocks	Displays the number of uncorrected Blocks. Displays Zero (0) when FEC is *Disabled* or is not supported.
Time since last interface status change	Lists the time duration since the interface statistics was updated.

The **show interface loopback** command displays the following information:

Output field	Description
Loopback	Displays the loopback number and state and the line protocol state. The states are "Loopback *nn* is up", "Loopback *nn* is admin down, line protocol is down (admin down). "
Hardware	Displays "is Loopback".
Pluggable media	Displays "present" or "not present".
Interface index	Displays the interface index.
MTU	Displays the maximum transmission unit (MTU), in bytes.
LineSpeed Actual	Displays the actual line speed in Mb or "Nil".
LineSpeed Configured	Displays "Auto" or a value in Mb.
Last clearing of show interface counters:	In days, hours, and minutes, displays how much time elapsed since the last counter clear.
Queueing strategy	Displays "FIFO".
Primary Internet Address	Displays the primary Internet address.

The **show interface ethernet management** command displays the following information:

Output field	Description
LineSpeed Actual	Displays "100000baseT" (100Gb), "40000baseT" (40Gb), "25000baseT" (25Gb), "10000baseT" (10Gb), or "1000baseT" (1Gb).
Duplex	Displays "Half" or "Full".
LineSpeed Configured	Displays "Auto" or a value in Mb.
oper-status	Displays "up" or "down".
ip address	Displays "static" or "dynamic" and the IPv4 address.
ip gateway-address	Displays the IPv4 gateway address.
ipv6 ipv6-address	Displays the IPv6 address.
ipv6 ipv6-gateways	Displays the IPv6 gateway address.
redundant management	Displays the port where redundant management is enabled.

The **show interface ethernet switchport** command displays the following information:

Output field	Description
Interface name	Displays "Ethernet *slot* **/** *port* " or "Port-channel *nn* ".
Switchport mode	Displays "access", "trunk", or "trunk-no-default-native".
Ingress filter	Displays "enable".
Acceptable frame types	Displays "vlan-tagged only", "vlan-untagged only", or "all".
Native Vlan	Displays the ID number of the native VLAN.
Active Vlans	Displays ID numbers of the active VLANs.
MAC learn disable Vlans	Displays VLANs for which MAC learning is disabled.

The **show interface trunk** command displays the following information:

Output field	Description
Port	Displays the Ethernet ports by *slot* **/** *port* .
Vlans Allowed on Trunk	Displays "Nil" or a list of the VLANs allowed on the trunk.

Examples

The following example displays detailed information for a specified Ethernet interface.

```
device# show interface ethernet 0/4
Ethernet 3/4 is up, line protocol is up (connected)
Hardware is Ethernet, address is 768d.f804.ca08
    Current address is 768d.f804.ca08
Pluggable media present
Interface index (ifindex) is 207650816
MTU 1548 bytes
IP MTU 1500 bytes
10G Interface
LineSpeed Actual     : 10000 Mbit
LineSpeed Configured : Auto, Duplex: Full
Priority Tag disable
Forward LACP PDU: Disable
Route Only: Disabled
Last clearing of show interface counters: 11:59:37
Queueing strategy: fifo
 Primary Internet Address is 12.2.1.2/24 broadcast is 12.2.1.255
Receive Statistics:
    45756 packets, 34003184 bytes
    Unicasts: 9094, Multicasts: 36650, Broadcasts: 12
    64-byte pkts: 1438, Over 64-byte pkts: 8113, Over 127-byte pkts: 1786
    Over 255-byte pkts: 10132, Over 511-byte pkts: 8432, Over 1023-byte pkts: 15855
    Over 1518-byte pkts(Jumbo): 0
    Runts: 0, Jabbers: 0, CRC: 0, Overruns: 0
    Errors: 0, Discards: 0
Transmit Statistics:
    33405 packets, 25357172 bytes
    Unicasts: 10232, Multicasts: 23162, Broadcasts: 10
    Underruns: 0
    Errors: 0, Discards: 0
```

```
Rate info:
    Input 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
    Output 0.000333 Mbits/sec, 0 packets/sec, 0.00% of line-rate
    Route-Only Packets Dropped: 0
FEC:
    Mode: RS-FEC
    Corrected Blocks: 0, Uncorrected Blocks: 4
Time since last interface status change: 3d10h59m
```

The following example displays detailed information for the specified management interface.

```
device# show interface Management 0
interface Management 0
 line-speed actual "1000baseT, Duplex: Full"
 line-speed configured Auto
 oper-status up
 rme-info "mgmt2(A) mgmt1(P)"
 ip address "static 10.17.110.59/20"
 ip gateway-address 10.17.114.1
 ipv6 ipv6-address [  ]
 ipv6 ipv6-gateways [ fe80::21b:edff:fe0b:9000 fe80::21b:edff:fe0b:3c00 ]
```

The following example displays detailed information for a specified loopback interface.

```
device# show interface loopback 1
Loopback 1 is up, line protocol is up
Hardware is Loopback
Pluggable media not present
Interface index (ifindex) is 1476395009
IP MTU 1500 bytes
LineSpeed Actual     : Nil
LineSpeed Configured : Auto
Last clearing of show interface counters: 00:00:23
Queueing strategy: fifo
 Primary Internet Address is 50.1.1.1/32
```

The following example displays details of a specified Layer 2 interface.

```
device# show interface switchport 0/15
 Interface name          : Ethernet 1/15
 Switchport mode         : trunk
 Ingress filter          : enable
 Acceptable frame types  : vlan-tagged only
 Native Vlan             : 1
 Active Vlans            : 1-201
 MAC learn disable Vlans : -
```

This example shows whether the control plane is receiving packets at the configured rate.

```
device# show int eth 0/1 | inc rate
Queueing strategy: fifo
    Input 8.649182 Mbits/sec, 8446 packets/sec, 0.10% of line-rate
    Output 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
```

show interface stats brief

Displays a brief list of interface statistics.

Syntax

show interface stats brief [**slot** *line-card-number*]

Parameters

slot *line-card-number*

(Not currently supported) Specifies a line card.

Modes

Privileged EXEC mode

Examples

The following example displays brief interface statistics.

```
device# show interface stats brief
                  Packets               Error         Discards      CRC
Interface  rx             tx         rx       tx    rx        tx
rx
=========  =======================   ==========    ============
=====
Eth 0/1    44127          38570      0          0    0          0
0
Eth 0/2    0              0          0          0    0          0
0
Eth 0/3    37319          38572      0          0    0          0
0
Eth 0/4    0              0          0          0    0          0
0
Eth 0/5    37319          38853      0          0    0          0
0
Eth 0/6    0              0          0          0    0          0
0
Eth 0/7    0              0          0          0    0          0
0
Eth 0/8    0              0          0          0    0          0
0
Eth 0/9    4735           6859       0          0    0          0
0
Eth 0/10   37319          45808      0          0    0          0
0
Eth 0/11   290725948      22923725   0          0    0          0
0
Eth 0/12   0              0          0          0    0          0
0
Eth 0/13   3395530417     37764      0          0    0          0
0
Eth 0/14   0              0          0          0    0          0
0
Eth 0/15   0              0          0          0    0          0
```

```
0
Eth 0/16    0               0           0          0     0           0     0
Eth 0/17    0               0           0          0     0           0     0
Eth 0/18    0               0           0          0     0           0     0
Eth 0/19    0               0           0          0     0           0     0
Eth 0/20    0               0           0          0     0           0     0
(output truncated)
```

show interface stats detail

Displays a detailed list of interface statistics.

Syntax

show interface stats detail

show interface stats detail interface { **ethernet** *slot* **/** *port* | **port-channel** *index* | **ve** { **all** | *ve-id* } }

Parameters

interface

Specifies what type of interface is displayed.

ethernet

Specifies an Ethernet interface.

slot

Specifies a valid slot number. For devices that do not support line cards, specify **0**.

port

Specifies a valid port number.

port-channel

Specifies a port channel interface.

index

Specifies the port channel number.

ve

Specifies a VE interface.

ve-id

Shows VE statistics for the specified VE ID.

all

Shows all VE statistics.

Modes

Privileged EXEC mode

Examples

The following example displays detailed statistics for a specified Ethernet interface.

```
device# show interface stats detail interface ethernet 0/41

 Interface Ethernet 0/41 statistics (ifindex 201662464 (0xc052000))
                                  RX                              TX
             Packets         1527093                           30717
               Bytes       195467768                         2933672
            Unicasts         1527089                               0
          Multicasts               4                           30711
```

```
          Broadcasts               0                              6
              Errors               0                              0
            Discards               0                              0
            Overruns               0       Underruns              0
               Runts               0
              Jabbers              0
                 CRC               0
        64-byte pkts               0
   Over 64-byte pkts               4
  Over 127-byte pkts         1527089
  Over 255-byte pkts               0
  Over 511-byte pkts               0
 Over 1023-byte pkts               0
 Over 1518-byte pkts               0
           Mbits/Sec        0.000000                       0.000338
          Packet/Sec               0                              0
           Line-rate           0.00%                          0.00%
```

The following example displays detailed statistics for a specified port channel.

```
device# show interface stats detail interface port-channel 10

 Interface Port-channel 10 statistics (ifindex 671088650 (0x2800000a))
                                 RX                              TX
             Packets         1527093                         30795
               Bytes       195467768                       2941072
           Unicasts         1527089                             0
          Multicasts               4                         30789
          Broadcasts               0                             6
              Errors               0                             0
            Discards               0                             0
            Overruns               0       Underruns             0
               Runts               0
              Jabbers              0
                 CRC               0
        64-byte pkts               0
   Over 64-byte pkts               4
  Over 127-byte pkts         1527089
  Over 255-byte pkts               0
  Over 511-byte pkts               0
 Over 1023-byte pkts               0
 Over 1518-byte pkts               0
           Mbits/Sec        0.000000                       0.000000
          Packet/Sec               0                              0
           Line-rate           0.00%                          0.00%
```

This example displays statistics for all VE interfaces.

```
device# show interface stats detail interface ve all

VE Statistics
Id          Rx Pkts     Rx Bytes      Tx Pkts      Tx Bytes
100         543         69504          0           0


Id          Rx Pkts     Rx Bytes      Tx Pkts      Tx Bytes
200         5430        6954          234          4560
```

This example displays the egress VE statistics. For SLX 9540 and SLX 9640 devices, this output is only relevant in *counter-profile-6*.

```
9540
SLX# show interface stats detail interface Ve all
```

```
 Interface Ve 38 statistics (ifindex 1207959590 (0x48000026))
                                RX                              TX
             Packets            0                          41718669
               Bytes            0                        5256551919
Interface Ve 138 statistics (ifindex 1207959690 (0x4800008a))
                                RX                              TX
             Packets            0                              8
               Bytes            0                            553
SLX#
```

For SLX 9640 devices:

```
SLX# show interface stats detail interface Ve all
 Interface Ve 15 statistics (ifindex 1207959567 (0x4800000f))
                                RX                              TX
             Packets            0                              0
               Bytes            0                              0
 Interface Ve 115 statistics (ifindex 1207959667 (0x48000073))
                                RX                              TX
             Packets            0                          41718663
               Bytes            0                        5256551538
SLX#
```

This example displays the Ingress and Egress VE statistics. For SLX 9540 and SLX 9640, this output is available when *counter-profile-6* is enabled and the command **ingress-vlan-mapped-ve-counter** is also set.

For SLX 9540 devices:

```
 SLX# show interface stats detail interface Ve 38
 Interface Ve 38 statistics (ifindex 1207959590 (0x48000026))
                                RX                              TX
             Packets            41718669                        41718669
               Bytes            5256551919                      5256551919
```

For SLX 9640 devices:

```
 SLX# show interface stats detail interface Ve 115
 Interface Ve 115 statistics (ifindex 1207959667 (0x48000073))
                                RX                              TX
             Packets            41718663                        41718663
               Bytes            5256551538                      5256551538
```

show interface stats utilization-watermark

Displays high and low—incoming and outgoing—current hour, previous hour, current 24-hour, and previous 24-hour traffic watermarks.

Syntax

show interface stats utilization-watermark

show interface stats utilization-watermark interface { **ethernet** *slot* **/** *port* | **port-channel** *index* }

Parameters

interface

Specifies what type of interface to display.

ethernet

Specifies an Ethernet interface.

slot

Specifies a valid slot number.

port

Specifies a valid port number.

port-channel *index*

Specifies a port-channel number.

Modes

Privileged EXEC mode

Usage Guidelines

You can filter the results by interface.

Output

The **show interface stats utilization-watermark** command displays the following information:

Output field	Description
Cur1Hr-InHigh	Displays the high watermark for incoming traffic during the current hour.
Cur1Hr-InLow	Displays the low watermark for incoming traffic during the current hour.
Cur1Hr-OutHigh	Displays the high watermark for outgoing traffic during the current hour.

Output field	Description
Cur1Hr-OutLow	Displays the low watermark for outgoing traffic during the current hour.
Last1Hr-InHigh	Displays the high watermark for incoming traffic during the previous hour.
Last1Hr-InLow	Displays the low watermark for incoming traffic during the previous hour.
Last1Hr-OutHigh	Displays the high watermark for outgoing traffic during the previous hour.
Last1Hr-OutLow	Displays the low watermark for outgoing traffic during the previous hour.
Cur24Hr-InHigh	Displays the high watermark for incoming traffic during the current 24 hours.
Cur24Hr-InLow	Displays the low watermark for incoming traffic during the current 24 hours.
Cur24Hr-OutHigh	Displays the high watermark for outgoing traffic during the current 24 hours.
Cur24Hr-OutLow	Displays the low watermark for outgoing traffic during the current 24 hours.
Last24Hr-InHigh	Displays the high watermark for incoming traffic during the previous 24 hours.
Last24Hr-InLow	Displays the low watermark for incoming traffic during the previous 24 hours.
Last24Hr-OutHigh	Displays the high watermark for outgoing traffic during the previous 24 hours.
Last24Hr-OutLow	Displays the low watermark for outgoing traffic during the previous 24 hours.

Examples

The following example displays utilization watermarks for a specified Ethernet interface.

```
device# show interface stats utilization-watermark interface ethernet 1/1

 Starting time of watermark windows:
 Cur1Hr : Apr  4 08:11:19       Cur24Hr : Apr  4 03:11:18

 Interface eth1/1 statistics watermark
                            Mbits/Sec         Pkts/Sec             Time

    Cur1Hr-InHigh   :        0.000000                0               00:00:00
    Cur1Hr-InLow    :        0.000000                0               00:00:00
    Cur1Hr-OutHigh  :        0.000000                0               00:00:00
    Cur1Hr-OutLow   :        0.000000                0               00:00:00
    Last1Hr-InHigh  :        0.000000                0               00:00:00
    Last1Hr-InLow   :        0.000000                0               00:00:00
    Last1Hr-OutHigh :        0.000000                0               00:00:00
    Last1Hr-OutLow  :        0.000000                0               00:00:00
    Cur24Hr-InHigh  :        0.000000                0               00:00:00
    Cur24Hr-InLow   :        0.000000                0               00:00:00
    Cur24Hr-OutHigh :        0.000000                0               00:00:00
```

```
    Cur24Hr-OutLow  :        0.000000              0                00:00:00
    Last24Hr-InHigh :        0.000000              0                00:00:00
    Last24Hr-InLow  :        0.000000              0                00:00:00
    Last24Hr-OutHigh:        0.000000              0                00:00:00
    Last24Hr-OutLow :        0.000000              0                00:00:00
```

show interface status

Displays the status of all device interfaces.

Syntax

show interface status

Modes

Privileged EXEC mode

Output

The **show interface status** command displays the following information:

Output field	Description
Port	Displays the physical port or port channel.
Status	Displays the port status. The states are "adminDown", "notconnected", "connected (up)", or "sfpAbsent".
Mode	Displays "access" or "trunk".
Speed	Displays the speed of the Ethernet interface, in Gb.
Type	Displays 1G-SFP, 10G-SFP-LR, 10G-SFP-SR, 10G-SFP-SX, 40G-QSFP, or 100G.
Description	Displays a Description defined for the port.

Examples

The following example displays the status of all device interfaces.

```
device# show interface status
--------------------------------------------------------------------------------
Port          Status           Mode       Speed    Type            Description
--------------------------------------------------------------------------------
Eth 1/1       adminDown        --         --       --
Eth 1/2       adminDown        --         --       --
Eth 1/3       adminDown        --         --       --
...
Eth 1/15      notconnected     --         --       40G-QSFP                     -
...
Eth 3/4       connected (up)   --         10G      10G-SFP-SR
(output truncated)
```

show inventory

Displays the hardware inventory of the device.

Syntax

show inventory [**chassis** | **fan** | **module** | **powerSupply**]

Parameters

chassis

Displays information about the device.

fan

Displays information about the fan.

module

Displays information about the module.

powerSupply

Displays information about the power supply.

Modes

Privileged EXEC mode

Examples

The following is an example of typical command output.

```
device# show inventory

NAME:AP BLADE, Slot SW DESCR:Chassis Blade module
PN:40-1001198-03  SN:FBK0319M00J

NAME:POWER SUPPLY 1 DESCR:Chassis PS module
PN:N/A            SN:N/A

NAME:POWER SUPPLY 2 DESCR:Chassis PS module
PN:N/A            SN:N/A

NAME:FAN 1 DESCR:Chassis Fan module
PN:N/A            SN:N/A

NAME:FAN 2 DESCR:Chassis Fan module
PN:N/A            SN:N/A

NAME:FAN 3 DESCR:Chassis Fan module
PN:N/A            SN:N/A

NAME:FAN 5 DESCR:Chassis Fan module
PN:N/A            SN:N/A

NAME: Chassis  DESCR:System Chassis
SID:BR-SLX9540     SwitchType:4000
PN:40-1001198-03  SN:FBK0319M00J
```

show ip arp inspection

Displays Dynamic ARP Inspection (DAI) information for one or more VLANs.

Syntax

show ip arp inspection [**vlan** *vlan-range*]

Parameters

vlan *vlan-range*

Specifies a VLAN, multiple VLANs (separated by commas with no spaces), a range of VLANs, or a combination of specified VLANs and ranges of VLANs. Valid values are from 1 through 4090.

Modes

Privileged EXEC mode

Output

The **show ip arp inspection** command displays the following information:

Output field	Description
Vlan	Displays the VLAN name.
Configuration	Displays "Enabled" (**ip arp inspection**) or "Disabled" (**no ip arp inspection**).
Operation	Displays "Active" if ARP configuration is successfully saved to the database. "Inactive" indicates one of the following conditions: • The "Configuration" value is "Disabled". • There is an internal issue that prevents successful application of ACLs.
ACL Match	Displays the name of the ARP ACL that is applied.

Examples

The following example displays DAI information for all VLANs.

```
device# show ip arp inspection
  Vlan  Configuraton     Operation     ACL Match
-------------------------------------------------
     1       Enabled        Active
    10      Disabled      Inactive
   100       Enabled        Active          acl1
  1000       Enabled        Active
    20      Disabled      Inactive
   200      Disabled      Inactive
  2000       Enabled        Active          acl1
```

The following example displays DAI information for specified VLANs and a range of VLANs.

```
device# show ip arp inspection vlan 1,100,200-2000
  Vlan  Configuraton     Operation     ACL Match
-------------------------------------------------
     1       Enabled        Active
   100       Enabled        Active          acl1
  1000       Enabled        Active
   200      Disabled      Inactive
  2000       Enabled        Active          acl1
```

show ip arp inspection interfaces

Displays a list of trusted interfaces on VLANs enabled for Dynamic ARP Inspection (DAI).

Syntax

show ip arp inspection interfaces [**ethernet** *slot* **/** *port* | **port-channel** *index*]

Parameters

ethernet

Specifies a physical Ethernet interface.

slot

Specifies a valid slot number. For devices that do not support line cards, specify **0**.

port

Specifies a valid port number.

port-channel *index*

Specifies a port-channel interface.

Modes

Privileged EXEC mode

Usage Guidelines

On VLANs that are enabled for Dynamic ARP Inspection (DAI), interfaces that are not listed in the command output are untrusted.

Output

The **show ip arp inspection interfaces** command displays the following information:

Output field	Description
Interface	Displays a prefix specifying the interface type, followed by the interface identifier.
Trust State	Displays "Trusted".

Examples

The following example displays all trusted interfaces.

```
device# show ip arp inspection interfaces
Interface     Trust State
--------------------------------------
Po 200        Trusted
```

```
Eth 2/0       Trusted
Eth 4/0       Trusted
---------------------------------------

All other interfaces are untrusted.
```

The following example displays the trust state of Ethernet interface 4/0.

```
device# show ip arp inspection interfaces ethernet 4/0
Interface     Trust State
---------------------------------------
Eth 4/0       Trusted
```

show ip arp suppression-cache

Multiple tunnel entries can be present per ARP.

Examples

The following example shows the multiple tunnel entries can be present per ARP.

```
sw# show ip arp suppression-c
Flags: L - Locally Learnt Adjacency
R - Remote Learnt Adjacency
RS - Remote Static Adjacency
Number of Locally Learnt Adjacency : 0
Number of Remotely Learnt Adjacency: 2794
Vlan/Bd IP Mac Interface Age Flags
-------------------------------------------------------------------------------------------
---------
0001 (B) 20.100.0.1 f46e.959f.2c27 Po 17.1801 Never R 0001 (B) 20.100.0.8 887e.25d3.180b
Tu 32771 (1.89.0.2) Never RS Tu 32775 (1.89.0.5)
```

show ip arp suppression-statistics

Displays IPv4 ARP-suppression statistics.

Syntax

show ip arp suppression-statistics

show ip arp suppression-statistics bridge-domain *bridge-domain-id*

show ip arp suppression-statistics vlan *vlan-id*

Parameters

bridge-domain *bridge-domain-id*

Specifies one or more bridge domain IDs. To specify a range of IDs, insert a hyphen between the beginning and ending integers (for example, 5-16). To specify individual IDs and ranges of IDs, separate them with commas (for example: 1,5-7,55). Do not insert spaces after commas. You can enter a maximum of 253 characters.

vlan *vlan-id*

Specifies one or more VLAN IDs. To specify a range of IDs, insert a hyphen between the beginning and ending integers (for example, 5-16). To specify individual IDs and ranges of IDs, separate them with commas (for example: 1,5-7,55). Do not insert spaces after commas. You can enter a maximum of 253 characters.

Modes

Privileged EXEC mode

Output

The **show ip arp suppression-statistics** command displays the following information:

Output field	Description
Vlan/Bd	Displays the VLAN (V) ID or bridge-domain (B) ID.
Forwarded	Displays the number of packets forwarded.
Suppressed	Displays the number of packets suppressed.
Remote-arp Proxy	Displays the number of packets for which the device has sent proxy-ARP replies.

Examples

The following example displays the results of the basic form of this command.

```
device# show ip arp suppression-statistics
Vlan/Bd       Forwarded     Suppressed    Remote-arp Proxy
-----------------------------------------------------------
110 (V)       0             24            0
254 (V)       3             10            0
```

show ip arp suppression-status

Displays the IPv4 ARP-suppression status.

Syntax

show ip arp suppression-status

show ip arp suppression-status bridge-domain *bridge-domain-id*

show ip arp suppression-status vlan *vlan-id*

Parameters

bridge-domain *bridge-domain-id*

Specifies one or more bridge domain IDs. To specify a range of IDs, insert a hyphen between the beginning and ending integers (for example, 5-16). To specify individual IDs and ranges of IDs, separate them with commas (for example: 1,5-7,55). Do not insert spaces after commas. You can enter a maximum of 253 characters.

vlan *vlan-id*

Specifies one or more VLAN IDs. To specify a range of IDs, insert a hyphen between the beginning and ending integers (for example, 5-16). To specify individual IDs and ranges of IDs, separate them with commas (for example: 1,5-7,55). Do not insert spaces after commas. You can enter a maximum of 253 characters.

Modes

Privileged EXEC mode

Output

The **show ip arp suppression-status** command displays the following information:

Output field	Description
Vlan/Bd	Displays the VLAN (V) ID or bridge-domain (B) ID.
Configuration	Displays "Enabled" or "Disabled".
Evpn-Register	Displays "Yes" if the VLAN is extended through EVPN or "No" if it is not extended.
Operation	Displays "Active" or "Inactive".

Examples

The following example displays the results of the basic form of this command.

```
device# show ip arp suppression-status
Vlan/Bd          Configuration   Evpn-Register Operation
```

```
-------------------------------------------------------------------------------
4003 (V)         Enabled         Yes           Active
4005 (V)         Disabled        No            Inactive
4006 (V)         Enabled         Yes           Active
4007 (V)         Enabled         Yes           Active
4008 (V)         Disabled        No            Inactive
4013 (V)         Enabled         Yes           Active
4015 (V)         Disabled        No            Inactive
```

show ip bgp

Displays BGP4 route information.

Syntax

show ip bgp

show ip bgp *ip-addr* [*/prefix*]

show ip bgp *ip-addr* [*/prefix*] [**longer-prefixes**] [**vrf** *vrf-name*]

Parameters

ip-addr

IPv4 address of a neighbor in dotted-decimal notation, with an optional mask.

/prefix

IPv4 mask length in CIDR notation.

longer-prefixes

Filters prefixes equal to or greater than that specified by *prefix*.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example displays sample output from the **show ip bgp** command.

```
device# show ip bgp

Total number of BGP Routes: 4
Status codes: s suppressed, d damped, h history, * valid, > best, i internal, S stale, x
best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network            Next Hop        MED        LocPrf     Weight Path
*>i 110.110.110.0/24   50.50.50.10                150        0      i
*x  110.110.110.0/24   20.20.20.10                100        0      200 i
*   110.110.110.0/24   30.30.30.10                100        0      300 i
*   110.110.110.0/24   40.40.40.10                100        0      400 i
```

show ip bgp attribute-entries

Displays BGP4 route-attribute entries that are stored in device memory.

Syntax

show ip bgp attribute-entries [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

The route-attribute entries table lists the sets of BGP4 attributes that are stored in device memory. Each set of attributes is unique and can be associated with one or more routes. In fact, the device typically has fewer attribute entries than routes. Use this command to view BGP4 route-attribute entries that are stored in device memory.

Examples

The following example show sample output for the **show ip bgp attribute-entries** command.

```
device# show ip bgp attribute-entries
```

show ip bgp dampened-paths

Displays all BGP4 dampened routes..

Syntax

show ip bgp dampened-paths [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example shows sample output from the **show ip bgp dampened-paths** command.

```
device# show ip bgp dampened-paths

    Status Code  >:best d:damped h:history *:valid
    Network            From            Flaps Since       Reuse       Path
*d  110.110.114.0/24   160.160.160.10  38    0 :3 :49    0 :10:10    111
*d  110.110.113.0/24   160.160.160.10  38    0 :3 :49    0 :10:10    111
*d  110.110.112.0/24   160.160.160.10  38    0 :3 :49    0 :10:10    111
*d  110.110.111.0/24   160.160.160.10  38    0 :3 :49    0 :10:10    111
*d  110.110.110.0/24   160.160.160.10  38    0 :3 :49    0 :10:10    111
```

show ip bgp filtered-routes

Displays BGP4 filtered routes that are received from a neighbor or peer group.

Syntax

show ip bgp filtered-routes [**detail**] [*ip-addr* { **/** *mask* } [**longer-prefixes**]] | **as-path-access-list** *name* | **prefix-list** *name*] [**vrf** *vrf-name*]

Parameters

detail

Optionally displays detailed route information.

ip-addr

IPv4 address of the destination network in dotted-decimal notation.

mask

(Optional) IPv4 mask of the destination network in CIDR notation.

longer-prefixes

Specifies all statistics for routes that match the specified route, or that have a longer prefix than the specified route.

as-path-access-list *name*

Specifies an AS-path ACL. The name must be between 1 and 32 ASCII characters in length.

prefix-list *name*

Specifies an IP prefix list. The name must be between 1 and 32 ASCII characters in length.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example displays BGP4 filtered routes.

```
device# show ip bgp filtered-routes 10.11.12.13 prefix-list myprefixlist
```

show ip bgp flap-statistics

Displays BGP4 route-dampening statistics for all dampened routes with a variety of options.

Syntax

show ip bgp flap-statistics

show ip bgp flap-statistics *ip-addr* { **/** *mask* } [**longer-prefixes** [**vrf** *vrf-name*] | **vrf** *vrf-name*]

show ip bgp flap-statistics neighbor *ip-addr* [**vrf** *vrf-name*]

show ip bgp flap-statistics regular-expression *name* [**vrf** *vrf-name*]

show ip bgp flap-statistics vrf *vrf-name*

Parameters

ip-addr

IPv4 address of a specified route in dotted-decimal notation.

mask

IPv4 mask of a specified route in CIDR notation.

longer-prefixes

Displays statistics for routes that match the specified route or have a longer prefix than the specified route.

vrf *vrf-name*

Specifies a VRF instance.

neighbor

Displays flap statistics only for routes learned from the specified neighbor.
ip-addr

IPv4 address of the neighbor.

regular-expression

Specifies a regular expression in the display output on which to filter.

name

Name of an AS-path filter or regular expression.

Modes

Privileged EXEC mode

Examples

The following example displays flap statistics for a neighbor.

```
device# show ip bgp flap-statistics neighbor 10.11.12.13
```

show ip bgp neighbors

Displays configuration information and statistics for BGP4 neighbors.

Syntax

show ip bgp neighbors [*ip-addr*]

show ip bgp neighbors last-packet-with-error [**vrf** *vrf-name*]

show ip bgp neighbors routes-summary [**vrf** *vrf-name*]

show ip bgp neighbors vrf *vrf-name*

Parameters

ip-addr

Specifies the IPv4 address of a neighbor.

last-packet-with-error

Displays the last packet with an error.

route-summary

Displays routes received, routes accepted, number of routes advertised by peer, and so on.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

Output shows all configured parameters for the neighbors. Only the parameters whose values differ from the default values are shown.

Dynamic neighbors are displayed only by using the **show ip bgp neighbors** commands with no options.

Examples

```
device# show ip bgp neighbors

Total number of BGP Neighbors: 2

1   IP Address: 123.123.123.3, AS: 333 (EBGP), RouterID: 9.9.9.9, VRF: default-vrf
    State: ESTABLISHED, Time: 0h1m32s, KeepAliveTime: 60, HoldTime: 180
       KeepAliveTimer Expire in 17 seconds, HoldTimer Expire in 147 seconds
    Minimal Route Advertisement Interval: 0 seconds
       PeerGroup: lldp-grp
         Auto discovered LLDP neighbor
```

```
       MD5 Password: $M1VzZCFAbg==
       RefreshCapability: Received
    Messages:    Open    Update  KeepAlive Notification Refresh-Req
       Sent    : 2       15      3339      1            0
       Received: 2       0       3356      0            0
    Last Update Time: NLRI              Withdraw               NLRI
Withdraw
                  Tx: 0h1m32s           ---                 Rx: ---
---
    Last Connection Reset Reason:User Reset Peer Session
    Notification Sent:     Cease/Administrative Reset
    Notification Received: Unspecified
    Neighbor NLRI Negotiation:
      Peer configured for IPV4 unicast  Routes
    Neighbor AS4 Capability Negotiation:
    Outbound Policy Group:
       ID: 2, Use Count: 2
    BFD:Disabled
       Byte Sent:   146, Received: 0
       Local host:  123.123.123.2, Local  Port: 44575
       Remote host: 123.123.123.3, Remote Port: 179
G-Shut:
       Enabled: yes, g-shut timer: 600 seconds, Route-map: none
       g-shut timer Expire in 200 seconds
       local-preference 0 gshut community 1200

2   IP Address: 160.160.160.10, AS: 111 (EBGP), RouterID: 193.24.0.1, VRF: default-vrf
    State: ESTABLISHED, Time: 0h1m33s, KeepAliveTime: 30, HoldTime: 90
       KeepAliveTimer Expire in 12 seconds, HoldTimer Expire in 86 seconds
    Minimal Route Advertisement Interval: 0 seconds
       RefreshCapability: Received
    Messages:    Open    Update  KeepAlive Notification Refresh-Req
       Sent    : 8       0       553       5            0
       Received: 8       9       498       0            0
    Last Update Time: NLRI              Withdraw               NLRI
Withdraw
                  Tx: ---               ---                 Rx: 0h1m33s
---
    Last Connection Reset Reason:User Reset Peer Session
    Notification Sent:     Cease/Administrative Reset
    Notification Received: Unspecified
    Neighbor NLRI Negotiation:
      Peer configured for IPV4 unicast  Routes
    Neighbor AS4 Capability Negotiation:
    Outbound Policy Group:
       ID: 2, Use Count: 2
    BFD:Disabled
       Byte Sent:   121, Received: 0
       Local host:  160.160.160.20, Local  Port: 53791
       Remote host: 160.160.160.10, Remote Port: 179
    G-Shut:
       Enabled: yes, g-shut timer: 600 seconds, Route-map: none
       g-shut timer Expire in 200 seconds
       local-preference 0 gshut community 1200
```

The following example shows sample output about dynamically created BGP neighbors.

```
device# show ip bgp neighbors

1   IP Address: 98.0.0.1, AS: 100 (IBGP), RouterID: 98.0.0.1, VRF: default-vrf
    State: ESTABLISHED, Time: 1h56m21s, KeepAliveTime: 60, HoldTime: 180
       KeepAliveTimer Expire in 40 seconds, HoldTimer Expire in 157 seconds
    Minimal Route Advertisement Interval: 0 seconds
```

```
       PeerGroup: pg1
       DYNAMIC neighbor belongs to the subnet range group: 98.0.0.0/24
       RefreshCapability: Received
    Address Family : L2VPN EVPN
       SendExtendedCommunity: yes
    Messages:    Open    Update  KeepAlive Notification Refresh-Req
       Sent    : 4       18      178       3            0
       Received: 4       42      177       0            0
    Last Update Time: NLRI              Withdraw               NLRI
Withdraw
                  Tx: 1h56m21s          ---                 Rx: 1h56m20s
---
    Last Connection Reset Reason:User Reset Peer Session
    Notification Sent:     Cease/Administrative Reset
    Notification Received: Unspecified
    Neighbor NLRI Negotiation:
      Peer Negotiated L2VPN EVPN address family
      Peer configured for IPV4 unicast  Routes
      Peer configured for L2VPN EVPN address family
    Neighbor ipv6 MPLS Label Capability Negotiation:
    Neighbor AS4 Capability Negotiation:
    Outbound Policy Group:
       ID: 2, Use Count: 3
       Last update time was 4667 sec ago
    BFD:Disabled
       Byte Sent:   2968, Received: 0
       Local host:  98.0.0.2, Local  Port: 8231
       Remote host: 98.0.0.1, Remote Port: 179
```

show ip bgp neighbors advertised-routes

Displays the routes that the device has advertised to the neighbor during the current BGP4 session.

Syntax

show ip bgp neighbors *ip-addr* **advertised-routes** [**detail** | **/** *mask-bits*] [**vrf** *vrf-name*]

Parameters

ip-addr

IPv4 address of a neighbor in dotted-decimal notation.

detail

Displays details of advertised routes.

mask-bits

Number of mask bits in CIDR notation.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example displays the details of advertised routes.

```
device# show ip bgp neighbors 123.123.123.3 advertised-routes

       There are 5 routes advertised to neighbor 123.123.123.3
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
       Prefix             Next Hop        MED        LocPrf     Weight Status
1      110.110.110.0/24   123.123.123.2    0                     0      BE
         AS_PATH: 222 111
2      110.110.111.0/24   123.123.123.2    0                     0      BE
         AS_PATH: 222 111
3      110.110.112.0/24   123.123.123.2    0                     0      BE
         AS_PATH: 222 111
4      110.110.113.0/24   123.123.123.2    0                     0      BE
         AS_PATH: 222 111
5      110.110.114.0/24   123.123.123.2    0                     0      BE
         AS_PATH: 222 111
```

show ip bgp neighbors flap-statistics

Displays the route flap statistics for routes received from or sent to a BGP4 neighbor.

Syntax

show ip bgp neighbors *ip-addr* **flap-statistics** [**vrf** *vrf-name*]

Parameters

ip-addr

IPv4 address of a neighbor in dotted-decimal notation.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example shows flap statistics.

```
device# show ip bgp neighbors flap-statistics
```

show ip bgp neighbors last-packet-with-error

Displays information about the last packet that contained an error from any of a device's neighbors.

Syntax

show ip bgp neighbors *ip-addr* **last-packet-with-error** [**decode**] [**vrf** *vrf-name*]

Parameters

ip-addr

IP address of a neighbor in dotted-decimal notation.

decode

Decodes last packet that contained an error from any of a device's neighbors.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example shows sample output from the **show ip bgp neighbors last-packet-with-error** command when no packet from a specified neighbor contained an error.

```
device# show ip bgp neighbors 123.123.123.3 last-packet-with-error

 Received Message Length: 45
 BGP Message:
  0xffffffff  0xffffffff  0xffffffff  0xffffffff  0x002d0104
  0x014b00b4  0x09090909  0x10020601  0x04010000  0x01020202
  0x00020280  0x00

 BGP Header
  Marker:   0xffffffff  0xffffffff  0xffffffff  0xffffffff
  Message Length: (0x002d) 45
  Message Type: (0x01) OPEN

 OPEN Message
 Version: (0x04) 4
 AS Number: (0x014b) 331
 Hold Time: (0x00b4) 180
 BGP Identifier: (0x09090909) 9.9.9.9
 Optional Parameter length: (0x10) 16

 OPEN message optional parameters
  Parameter Type: (0x02) Capability
  Parameter Length: (0x06) 6
   Capability Type: (0x01) MULTIPROTOCOL EXTENSIONS
   Capability Length: (0x04) 4
```

```
 AFI: (0x0100) Unknown(256)
 Reserved: (0x00) 0
 SAFI: (0x01) Unicast

Parameter Type: (0x02) Capability
Parameter Length: (0x02) 2
 Capability Type: (0x02) ROUTE REFRESH(new)
 Capability Length: (0x00) 0

Parameter Type: (0x02) Capability
Parameter Length: (0x02) 2
 Capability Type: (0x80) ROUTE REFRESH(old)
 Capability Length: (0x00) 0
```

show ip bgp neighbors received

Displays Outbound Route Filters (ORFs) received from BGP4 neighbors of the device.

Syntax

show ip bgp neighbors *ip-addr* **received**

show ip bgp neighbors *ip-addr* **received detail** [**vrf** *vrf-name*]

show ip bgp neighbors *ip-addr* **received prefix-filter** [**vrf** *vrf-name*]

show ip bgp neighbors *ip-addr* **vrf** *vrf-name*

Parameters

ip-addr

IPv4 address of a neighbor in dotted-decimal notation.

detail

Displays detailed information for ORFs received from BGP4 neighbors of the device.

vrf *vrf-name*

Specifies a VRF instance.

prefix-filter

Displays the results for ORFs that are prefix-based.

Modes

Privileged EXEC mode

Examples

The following example displays output for the **show ip bgp neighbors received** command.

```
device# show ip bgp neighbors 10.5.5.6 received
```

show ip bgp neighbors received-routes

Lists all route information received in route updates from BGP4 neighbors of the device since the soft-reconfiguration feature was enabled.

Syntax

show ip bgp neighbors *ip-addr* **received-routes** [**detail**] [**vrf** *vrf-name*]

Parameters

ip-addr

IPv4 address of a neighbor in dotted-decimal notation.

detail

Displays detailed route information.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example displays output for the **show ip bgp neighbors received-routes** command.

```
device# show ip bgp neighbors 160.160.160.10 received-routes

       There are 5 received routes from neighbor 160.160.160.10
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix             Next Hop        MED        LocPrf     Weight Status
1      110.110.110.0/24   160.160.160.10   0         100        0      BE
         AS_PATH: 111
2      110.110.111.0/24   160.160.160.10   0         100        0      BE
         AS_PATH: 111
3      110.110.112.0/24   160.160.160.10   0         100        0      BE
         AS_PATH: 111
4      110.110.113.0/24   160.160.160.10   0         100        0      BE
         AS_PATH: 111
5      110.110.114.0/24   160.160.160.10   0         100        0      BE
         AS_PATH: 111
```

show ip bgp neighbors rib-out-routes

Displays information about BGP4 outbound RIB routes.

Syntax

show ip bgp neighbors *ip-addr* **rib-out-routes** *ip-addr mask* [**vrf** *vrf-name*]

show ip bgp neighbors *ip-addr* **rib-out-routes detail** *ip-addr mask* [**vrf** *vrf-name*]

show ip bgp neighbors *ip-addr* **rib-out-routes detail** [**vrf** *vrf-name*]

show ip bgp neighbors *ip-addr* **rib-out-routes** [**vrf** *vrf-name*]

Parameters

ip-addr

IP address of a neighbor in dotted-decimal notation.

vrf *vrf-name*

Specifies a VRF instance.

detail

Displays detailed RIB route information.

Modes

Privileged EXEC mode

Examples

This example shows sample output from the **show ip bgp neighbors rib-out-routes** command.

```
device# show ip bgp neighbors 123.123.123.3 rib-out-routes

       There are 5 RIB_out routes for neighbor 123.123.123.3
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
       Prefix             Next Hop        MED        LocPrf     Weight Status
1      110.110.110.0/24   160.160.160.10   0         100        0      BE
         AS_PATH: 111
2      110.110.111.0/24   160.160.160.10   0         100        0      BE
         AS_PATH: 111
3      110.110.112.0/24   160.160.160.10   0         100        0      BE
         AS_PATH: 111
4      110.110.113.0/24   160.160.160.10   0         100        0      BE
         AS_PATH: 111
5      110.110.114.0/24   160.160.160.10   0         100        0      BE
         AS_PATH: 111
```

show ip bgp neighbors routes

Lists a variety of route information received in UPDATE messages from BGP4 neighbors.

Syntax

show ip bgp neighbors *ip-addr* **routes**

show ip bgp neighbors *ip-addr* **routes** { **best** | **not-installed-best** | **unreachable** } [**vrf** *vrf-name*]

show ip bgp neighbors *ip-addr* **routes detail** { **best** | **not-installed-best** | **unreachable** } [**vrf** *vrf-name*]

Parameters

ip-addr

IPv4 address of a neighbor in dotted-decimal notation.

best

Displays routes received from the neighbor that are the best BGP4 routes to their destination.

not-installed-best

Displays routes received from the neighbor that are the best BGP4 routes to their destination but were not installed in the route table because the device received better routes from other sources.

unreachable

Displays routes that are unreachable because the device does not have a valid RIP, OSPF, or static route to the next hop.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example displays

```
device# show ip bgp neighbors 10.11.12.13 routes best vrf red

Searching for matching routes, use ^C to quit...
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE x:BEST-EXTERNAL
       Prefix             Next Hop        MED        LocPrf     Weight Status
```

```
1       2.2.2.2/32          10.11.12.13         0           100         0       BI
          AS_PATH:
```

show ip bgp neighbors routes-summary

Lists all route information received in UPDATE messages from BGP4 neighbors.

Syntax

show ip bgp neighbors *ip-addr* **routes-summary** [**vrf** *vrf-name*]

Parameters

ip-addr

IPv4 address of a neighbor in dotted-decimal notation.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example displays route summary information received in UPDATE messages.

```
device# show ip bgp neighbors routes-summary
```

show ip bgp peer-group

Displays peer-group information.

Syntax

show ip bgp peer-group *peer-group-name* [**vrf** *vrf-name*]

Parameters

peer-group-name

Specifies a peer group name.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

Only the parameters that have values different from their defaults are listed.

Examples

This example shows sample output from the **show ip bgp peer-group** command.

```
device# show ip bgp peer-group
1   BGP peer-group is pg
      Address family : IPV4 Unicast
        activate
      Address family : IPV6 Unicast
        no activate
    Members:
       IP Address: 1.1.1.1, AS: 100
       IP Address: 1::1, AS: 100

2   BGP peer-group is pg6
      Address family : IPV4 Unicast
        activate
      Address family : IPV6 Unicast
        no activate
    Currently there are no members
```

show ip bgp routes

Displays BGP4 route information that is filtered by the table entry at which the display starts.

Syntax

show ip bgp routes [*num* | *ip-address/prefix* | **age** *num* | **as-path-access-list** *name* | **best** | **cidr-only** | **community-access-list** *name* | **community-reg-expression** *expression* | **detail** | **large-community** | **local** | **neighbor** *ip-addr* | **nexthop** *ip-addr* | **no-best** | **not-installed-best** | **prefix-list** *string* | **regular-expression** *name* | **route-map** *name* | **summary** | **unreachable**] [**vrf** *vrf-name*]

Parameters

num

Table entry at which the display starts.

ip-address/prefix

Table entry at which the display starts.

age

Displays BGP4 route information that is filtered by age.

as-path-access-list *name*

Displays BGP4 route information that is filtered by autonomous system (AS)-path access control list (ACL). The name must be between 1 and 32 ASCII characters in length.

best

Displays BGP4 route information that the device selected as best routes.

cidr-only

Displays BGP4 routes whose network masks do not match their class network length.

community-access-list *name*

Displays BGP4 route information for an AS-path community access list. The name must be between 1 and 32 ASCII characters in length.

community-reg-expression *expression*

Displays BGP4 route information for an ordered community-list regular expression.

detail

Displays BGP4 detailed route information.

large-community

Displays routes that match the large community identifier.

local

Displays BGP4 route information about selected local routes.

neighbor *ip-addr*

Displays BGP4 route information about selected BGP neighbors.

nexthop *ip-addr*

Displays BGP4 route information about routes that are received from the specified next hop.

no-best

Displays BGP4 route information that the device selected as not best routes.

not-installed-best

Displays BGP4 route information about best routes that are not installed.

prefix-list *string*

Displays BGP4 route information that is filtered by prefix list. The string must be between 1 and 32 ASCII characters in length.

regular-expression *name*

Displays BGP4 route information about routes that are associated with the specified regular expression.

route-map *name*

Displays BGP4 route information about routes that use the specified route map.

summary

Displays BGP4 summary route information.

unreachable

Displays BGP4 route information about routes whose destinations are unreachable through any of the BGP4 paths in the BGP4 route table.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example shows sample output from the **show ip bgp routes** command when an IP address is specified.

```
SLX# show ip bgp routes 93.175.135.0/24
Number of BGP Routes matching display condition : 1
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE x:BEST-EXTERNAL
RPKI State V: Valid I: Invalid N: Not found ?: Undefined
       Prefix             Next Hop        MED        LocPrf     Weight RPKI State Status
1      93.175.135.0/24    50.0.0.2         none      100        0      I          BEx
         AS_PATH: 12654
       Last update to IP routing table: 0h1m12s
       Route is advertised to 1 peers:
        40.0.0.1(100)
```

The following example shows sample input from the **show ip bgp routes summary** command.

```
device# show ip bgp routes summary

  Total number of BGP routes (NLRIs) Installed     : 1
  Distinct BGP destination networks                : 1
  Filtered bgp routes for soft reconfig            : 0
  Routes originated by this router                 : 1
  Routes selected as BEST routes                   : 1
  Routes Installed as BEST routes                  : 1
  BEST routes not installed in IP forwarding table : 0
  Unreachable routes (no IGP route for NEXTHOP)    : 0
  IBGP routes selected as best routes              : 0
  EBGP routes selected as best routes              : 0
  BEST routes not valid for IP forwarding table    : 0
```

This example shows the output for BGP RPKI state.

```
SLX# show ip bgp routes
Total number of BGP Routes: 1
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE x:BEST-EXTERNAL
RPKI State V: Valid I: Invalid N: Not found ?: Undefined
       Prefix             Next Hop          MED        LocPrf     Weight RPKI State Status
1      10.10.10.10/32     10.10.10.1         1          100        0      V          BI
         AS_PATH:
```

show ip bgp routes community

Displays BGP4 route information that is filtered by community and other options.

Syntax

show ip bgp routes community { *num* | **internet** | **local-as** | **no-advertise** | **no-export** } [**vrf** *vrf-name*]

Parameters

community

Displays routes filtered by a variety of communities.

num

Specific community member.

internet

Displays routes for the Internet community.

local-as

Displays routes for a local sub-AS within the confederation.

no-advertise

Displays routes with this community that cannot be advertised to any other BGP4 devices at all.

no-export

Displays routes for the community of sub-ASs within a confederation.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example shows output from the **show ip bgp routes community** command when the **internet** keyword is used.

```
device# show ip bgp routes community internet
```

show ip bgp routes large-community

Displays information for all BGP routes with large-community attributes matching the specified value.

Syntax

show ip bgp routes [**detail**] **large-community** *ADMIN:OPER1:OPER2* [**vrf** *vrf-name*]

Modes

Privileged EXEC mode

Parameters

detail

Optionally displays detailed information for all BGP routes with large-community attributes matching the specified value. If you omit this keyword, brief information is displayed.

ADMIN

A four-octet namespace identifier for a BGP Large-Communities Global Administrator.

OPER1

A four-octet operator-defined value for BGP Large-Communities Local Data Part 1.

OPER2

A four-octet operator-defined value for BGP Large-Communities Local Data Part 2.

vrf *vrf-name*

Specifies a VRF instance.

Examples

The following example provides a summary of information about the large community.

```
device# show ip bgp routes large-community 1:2:3
Searching for matching routes, use ^C to quit...
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE x:BEST-EXTERNAL
       Prefix             Next Hop        MED        LocPrf     Weight Status
1      150.150.150.0/24   192.168.1.20    0          100        0      BEx
         AS_PATH: 1639
2      150.150.151.0/24   192.168.1.20    0          100        0      BEx
         AS_PATH: 1639
3      150.150.152.0/24   192.168.1.20    0          100        0      E
         AS_PATH: 1639
```

The following example provides detailed information about the large community.

```
device# show ip bgp routes detail large-community 1:2:3
Searching for matching routes, use ^C to quit...
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE x:BEST-EXTERNAL
1       Prefix: 150.150.150.0/24, Rx path-id:0x00000000, Tx path-id:0x00040001,
rank:0x00000001, Status: BEx,  Age: 5d3h17m25s
         NEXT_HOP: 192.168.1.20, Metric: 0, Learned from Peer: 192.168.1.20 (1639)
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: igp,  Weight: 0,  GROUP_BEST: 1
         AS_PATH: 1639
            LARGE-COMMUNITIES: 1:1:1 2:2:2 3:3:3 4:4:4 5:5:5 6:6:6
            Adj_RIB_out count: 6,  Admin distance 20
2       Prefix: 150.150.151.0/24, Rx path-id:0x00000000, Tx path-id:0x00040001,
rank:0x00000001, Status: BEx,  Age: 5d3h17m25s
         NEXT_HOP: 192.168.1.20, Metric: 0, Learned from Peer: 192.168.1.20 (1639)
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: igp,  Weight: 0,  GROUP_BEST: 1
         AS_PATH: 1639
            LARGE-COMMUNITIES: 1:1:1 2:2:2 3:3:3 4:4:4 5:5:5 6:6:6
            Adj_RIB_out count: 6,  Admin distance 20
3       Prefix: 150.150.152.0/24, Rx path-id:0x00000000, Tx path-id:0x00040001,
rank:0x00000002, Status: E,  Age: 5d3h17m25s
         NEXT_HOP: 192.168.1.20, Metric: 0, Learned from Peer: 192.168.1.20 (1639)
          LOCAL_PREF: 100,  MED: 0,  ORIGIN: igp,  Weight: 0,  GROUP_BEST: 1
         AS_PATH: 1639
            LARGE-COMMUNITIES: 1:1:1 2:2:2 3:3:3 4:4:4 5:5:5 6:6:6
```

show ip bgp routes large-community access-list

Displays information for all BGP routes matching the large community access list.

Syntax

show ip bgp routes [**detail**] **large-community access-list**
large_community_ACL [**vrf** *vrf-name*]

Modes

Privileged EXEC mode

Parameters

detail

Optionally displays detailed information for all BGP routes matching the specified large community access list. If you omit this keyword, brief information is displayed.

large_community_ACL

Name of the large community defined in a standard or extended large community access list

vrf *vrf-name*

Specifies a VRF instance.

Examples

The following example displays brief information of all BGP routes with large community attributes that match the large community access-list, lcstdacl1.

```
device# show ip bgp routes large-community access-list lcstdacl1
Searching for matching routes, use ^C to quit...
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE x:BEST-EXTERNAL
       Prefix             Next Hop        MED        LocPrf     Weight Status
1      150.150.150.0/24   192.168.2.20    0          100        0      E
         AS_PATH: 1639
2      150.150.151.0/24   192.168.2.20    0          100        0      E
         AS_PATH: 1639
3      150.150.152.0/24   192.168.2.20    0          100        0      E
         AS_PATH: 1639
```

show ip bgp routes large-community reg-expression

Displays information for all BGP routes with large-community attributes matching the specified regular expression (REGEX).

Syntax

show ip bgp routes [**detail**] **large-community reg-expression** *regex_value*

Modes

Privileged EXEC mode

Parameters

detail

Optionally displays detailed information for all BGP routes with large-community attributes matching the specified REGEX. If you omit this keyword, brief information is displayed.

regex_value

REGEX value.

Examples

The following example displays the BGP routes that match the specified REGEX value.

```
device# show ip bgp routes large-community reg-expression (1|8):(.*):(.*)
Searching for matching routes, use ^C to quit...
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE x:BEST-EXTERNAL
       Prefix             Next Hop        MED        LocPrf     Weight Status
1      150.150.150.0/24   192.168.1.20    0          100        0      BEx
         AS_PATH: 1639
2      150.150.150.0/24   192.168.2.20    0          100        0      E
         AS_PATH: 1639
3      150.150.151.0/24   192.168.1.20    0          100        0      BEx
         AS_PATH: 1639
4      150.150.151.0/24   192.168.2.20    0          100        0      E
         AS_PATH: 1639
5      150.150.152.0/24   192.168.1.20    0          100        0      E
         AS_PATH: 1639
6      150.150.152.0/24   192.168.2.20    0          100        0      E
         AS_PATH: 1639
```

show ip bgp rpki details

This command displays the list of configured RPKI priorities, the RPKI servers configured for each of those priorities, and the status of the connection for these RPKI servers.

Syntax

show ip bgp rpki details

Modes

Privileged EXEC mode

Usage Guidelines

By default you can use one RPKI server for validation. The current in use server is indicated with the status *RTR_ESTABLISHED*.

Examples

This command displays the list of configured RPKI priorities, the RPKI servers configured for those priorities, and the status of the connection for these RPKI servers.

```
SLX# show ip bgp rpki details
  BGP RPKI Server Detail
  Priority number 1
  Protocol VRF        Host                Port  Status
  TCP      mgmt-vrf   141.22.28.252       8283  RTR_ESTABLISHED
  Priority number 2
  Protocol VRF        Host                Port  Status
  TCP      mgmt-vrf   1.2.3.4             323   RTR_CLOSED
SLX#
```

show ip bgp rpki server summary

This command displays the current state of communication with the RPKI cache server that is used for RPKI validation.

Syntax

show ip bgp rpki server summary

Modes

Privileged EXEC mode

Examples

This example shows the output of the **show ip bgp RPKI server summary** command which displays the state of the connection with the RPKI server being used for validation.

```
SLX(config)# show ip bgp rpki server summary
  BGP RPKI Server Summary
  Protocol VRF        Host                Port  Status
  TCP      mgmt-vrf   141.22.28.252       8283  RTR_ESTABLISHED
```

show ip bgp rpki table

This command displays the currently cached list of networks and AS numbers received from the RPKI server.

Syntax

show ip bgp rpki table

Modes

Privileged EXEC mode

Examples

This example shows the output of the **show ip bgp rpki table** command which displays the currently cached list of networks and AS numbers received from the RPKI server.

```
SLX# show ip bgp rpki table
  BGP RPKI table
  Network             Min-Len Max-Len Origin-AS
  1.128.0.0           11      11      1221
  1.0.7.0             24      24      38803
  1.0.6.0             24      24      38803
  1.0.5.0             24      24      38803
  1.0.4.0             24      24      38803
  1.0.0.0             24      24      13335
```

show ip bgp summary

Displays BGP information such as the local autonomous system number (ASN), maximum number of routes supported, and BGP4 statistics.

Syntax

show ip bgp summary [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example displays summary BGP information.

```
device# show ip bgp summary
  BGP4 Summary
  Router ID: 10.10.10.10   Local AS Number: 2040
  Confederation Identifier: not configured
  Confederation Peers:
  Maximum Number of IP ECMP Paths Supported for Load Sharing: 1
  Number of Neighbors Configured: 1040, UP: 4
  Number of Routes Installed: 3079574, Uses 483493118 bytes
  Number of Routes Advertising to All Neighbors: 107925658 (17078048 entries), Uses
1297931648 bytes
  Number of Attribute Entries Installed: 1296243, Uses 230731254 bytes
  '+': Data in InQueue '>': Data in OutQueue '-': Clearing
  '*': Update Policy 'c': Group change 'p': Group change Pending
  'r': Restarting 's': Stale '^': Up before Restart '<': EOR waiting
  '$': Learning-Phase (for Delayed Route Calculation)
  '#': RIB-in Phase
  Neighbor Address  AS#         State     Time     Rt:Accepted Filtered Sent     ToSend
  16.1.1.1          65200       ESTAB     2h26m 8s    10011    0        1        0
  17.1.1.1          65200       ESTAB     2h26m 8s    10011    0        10010    0
  18.1.1.1          65200       ESTAB     2h26m 7s    10011    0        10011    0
  19.1.1.1          65200       ESTAB     2h26m 7s    10011    0        10011    0
  20.1.1.1          65200       ESTAB     2h26m 7s    10011    0        10011    0
  21.1.1.1          65200       ESTAB     2h26m 7s    10011    0        10011    0
  22.1.1.1          65200       ESTAB     2h26m 2s    10011    0        10011    0
  23.1.1.1          65200       ESTAB     2h26m 7s    10011    0        10011    0
…
```

The $: Learning-Phase (for Delayed Route Calculation) notation denotes that the BGP peer with this notation is learning bulk route updates. More than one peer can be in Learning-Phase. BGP BEST-Path selection is delayed until all the peers complete Learning-Phase. A peer can be in Learning-Phase only if BGP delayed route calculation feature is enabled and in specific scenarios as described in the **init-route-calc-delay** command.

The # : RIB-IN Phase notation denotes that a peer is learning bulk route updates. When one or more peer is in RIB-IN phase, BGP provides high preference for learning incoming route-updates and less preference for advertising routes (to outbound peers). An incoming route-update can possibly cause a BGP BEST-path change and eventually recompute RIB-OUT for outbound peers. Slowing down RIB-OUT until all peers complete learning route updates will improve BGP performance. This feature is enabled by default and does not require additional configuration. Unlike BGP delayed route calculation, BGP BEST-Path selection is not delayed in this Phase.

This example displays summary information when automatic discovery of neighbors is enabled for BGP.

```
device# show ip bgp summary
  BGP4 Summary
  Router ID: 4.4.4.4   Local AS Number: 100
  Confederation Identifier: not configured
  Confederation Peers:
  Maximum Number of IP ECMP Paths Supported for Load Sharing: 1
  Number of Neighbors Configured: 1, UP: 1
  Number of Routes Installed: 0
  Number of Routes Advertising to All Neighbors: 0 (0 entries)
  Number of Attribute Entries Installed: 0
 *Dynamically created based on a listen range command
  Dynamically created neighbors: 0/100(max)
  A – Auto discovered LLDP neighbors using LLDP
  Auto discovered LLDP neighbors: 1
  Neighbor Address  AS#         State     Time     Rt:Accepted Filtered Sent     ToSend
A 56.1.1.2          100         ESTAB     0h20m 7s    0        0        0        0
```

This example displays summary information about dynamically created BGP neighbors.

```
device# show ip bgp summary
 BGP4 Summary
 Router ID: 10.1.1.1 Local AS Number: 100
 Confederation Identifier: not configured
 Confederation Peers:
 Maximum Number of IP ECMP Paths Supported for Load Sharing: 1
 Number of Neighbors Configured: 3, UP: 1
 Number of Routes Installed: 7, Uses 840 bytes
 Number of Routes Advertising to All Neighbors: 6 (2 entries), Uses 120 bytes
 Number of Attribute Entries Installed: 4, Uses 460 bytes
 Neighbor Address   AS#  State Time     Rt:Accepted  Filtered  Sent  ToSend
*10.1.2.1           100  CONN  1h51m27s 0            0         0     2
* Dynamically created based on a listen range command
  Dynamically created neighbors: 1/(200 max)
```

show ip bgp vpnv4 routes large-community

Displays information for all BGP VPNv4 routes with large-community attributes matching the specified value.

Syntax

show ip bgp vpnv4 routes [**detail**] **large-community** *ADMIN:OPER1:OPER2*

Modes

Privileged EXEC mode

Parameters

detail

Optionally displays detailed information for all BGP VPNv4 routes with large-community attributes matching the specified value. If you omit this keyword, brief information is displayed.

ADMIN

A four-octet namespace identifier for a BGP Large-Communities Global Administrator.

OPER1

A four-octet operator-defined value for BGP Large-Communities Local Data Part 1.

OPER2

A four-octet operator-defined value for BGP Large-Communities Local Data Part 2.

Examples

The following is an example command.

```
device# show ip bgp vpnv4 routes large-community 1:2:3
```

show ip bgp vpnv4 routes large-community access-list

Displays information for all BGP VPNv4 routes matching the large community access list.

Syntax

show ip bgp vpnv4 routes [**detail**] **large-community access-list** *large_community_ACL*

Modes

Privileged EXEC mode

Parameters

detail

Optionally displays detailed information for all BGP VPNv4 routes matching the specified large community access list. If you omit this keyword, brief information is displayed.

large_community_ACL

Name of the large community defined in a standard or extended large community access list

Examples

The following example displays brief information of all BGP VPNv4 routes with large community attributes that match the large community access-list, lcstdacl1.

```
device# show ip bgp vpnv4 routes large-community access-list lcstdacl1
```

show ip bgp vpnv4 routes large-community reg-expression

Displays information for all BGP VPNv4 routes with large-community attributes matching the specified regular expression (REGEX).

Syntax

show ip bgp vpnv4 routes [**detail**] **large-community reg-expression** *regex_value*

Modes

Privileged EXEC mode

Parameters

detail

Optionally displays detailed information for all BGP VPNv4 routes with large-community attributes matching the specified REGEX. If you omit this keyword, brief information is displayed.

regex_value

REGEX value.

Examples

The following example displays the BGP VPNv4 routes that match the specified REGEX value.

```
device# show ip bgp vpnv4 routes large-community reg-expression _456778*
```

show ip bgp vpnv6 routes large-community

Displays information for all BGP VPNv6 routes with large-community attributes matching the specified value.

Syntax

show ip bgp vpnv6 routes [**detail**] **large-community** *ADMIN:OPER1:OPER2*

Modes

Privileged EXEC mode

Parameters

detail

Optionally displays detailed information for all BGP VPNv6 routes with large-community attributes matching the specified value. If you omit this keyword, brief information is displayed.

ADMIN

A four-octet namespace identifier for a BGP Large-Communities Global Administrator.

OPER1

A four-octet operator-defined value for BGP Large-Communities Local Data Part 1.

OPER2

A four-octet operator-defined value for BGP Large-Communities Local Data Part 2.

Examples

The following is an example command.

```
device# show ip bgp vpnv6 routes large-community 1:2:3
```

show ip bgp vpnv6 routes large-community access-list

Displays information for all BGP VPNv6 routes matching the large community access list.

Syntax

show ip bgp vpnv6 routes [**detail**] **large-community access-list** *large_community_ACL*

Modes

Privileged EXEC mode

Parameters

detail

Optionally displays detailed information for all BGP VPNv6 routes matching the specified large community access list. If you omit this keyword, brief information is displayed.

large_community_ACL

Name of the large community defined in a standard or extended large community access list

Examples

The following example displays brief information of all BGP VPNv6 routes with large community attributes that match the large community access-list, lcstdacl1.

```
device# show ip bgp vpnv6 routes large-community access-list lcstdacl1
```

show ip bgp vpn6 routes large-community reg-expression

Displays information for all BGP VPNv6 routes with large-community attributes matching the specified regular expression (REGEX).

Syntax

show ip bgp vpn6 routes [**detail**] **large-community reg-expression** *regex_value*

Modes

Privileged EXEC mode

Parameters

detail

Optionally displays detailed information for all BGP VPNv6 routes with large-community attributes matching the specified REGEX. If you omit this keyword, brief information is displayed.

regex_value

REGEX value.

Examples

The following example displays the BGP VPNv6 routes that match the specified REGEX value.

```
device# show ip bgp vpnv6 routes large-community reg-expression _456778*
```

show ip dhcp relay address

Displays IP DHCP relay addresses configured globally and also displays this information on the interfaces where it is configured.

Syntax

show ip dhcp relay address [**interface** [**ethernet** *slot/port* | **port-channel** *port-channel-number* | **ve** *ve-number*]]

Parameters

interface

Indicates that the information must be displayed for an interface.

ethernet *slot/port*

Indicates that the information must be displayed for an ethernet port with the provided slot/port number

port-channel *port-channel-number*

Indicates that the information must be displayed for a port-channel with the provided port-channel number

ve *ve-number*

Indicates that the information must be displayed for a Virtual Ethernet interface with the provided ve-interface number

Modes

Privilege Execution Mode

Usage Guidelines

None

Output

The **show ip dhcp relay address** command displays the following information:

Output Field	Description
Interface	The interface for which information is being displayed.
Relay Address	The IP address of the DHCP relay.
VRF Name	The VRF on which the DHCP relay can be reached.
DHCP Relay Information Option	Displays the current state of the DHCP Relay Information Option setting. Displays *Enabled* or *Disabled*.
DHCP Relay Broadcast Flooding	Displays the current state of the DHCP Relay Broadcast Flooding setting. Displays *Enabled* or *Disabled*.

Examples

The following example displays DHCP relay address(es) configured on interface 0/3:

```
SLX# show ip dhcp relay address interface ethernet 0/3

---------                    -------------                    --------
Interface                    Relay Address                    VRF Name
---------                    -------------                    --------
Eth 0/3                           10.3.4.5                         blue
Eth 0/3                           10.5.1.1                         default-vrf
```

The following example displays DHCP relay address(es) configured on VE 300:

```
SLX# show ip dhcp relay address interface ve 300

---------                  -------------                    --------
Interface                  Relay Address                    VRF Name
---------                  -------------                    --------
Ve 300                        10.0.1.2                       default-vrf
```

The following example displays the DHCP relay information globally.

```
SLX# show ip dhcp relay address

DHCP Relay Information Option: Disabled
DHCP Relay Broadcast Flooding: Enabled
---------                    -------------                    --------
Interface                    Relay Address                    VRF Name
---------                    -------------                    --------
Eth 0/3                           10.3.4.5                         blue
Eth 0/3                           10.5.1.1                         default-vrf
Ve  300                           10.0.1.2                         default-vrf
```

show ip dhcp relay gateway

Displays IP DHCP Relay gateway addresses.

Syntax

show ip dhcp relay gateway {**interface** [**ethernet** *slot/port* | **port-channel** *number* | **Ve** *number*]}

Parameters

interface

The interface ethernet slot/port number or the Ve number.

ethernet *slot/port*

Specifies a physical interface.

port-channel *number*

Specifies a port-channel.

ve *ve-number*

Specifies a virtual Ethernet interface.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the gateway address configured on the switch or on the interface.

Examples

To display the gateway address configured on the switch:

```
device# show ip dhcp relay gateway
---------                   -------------
Interface                      Gateway Address
---------                   -------------
Eth 3/5                           10.1.1.1
Ve 100                         100.1.1.1
```

To display the gateway address configured on the interface:

```
device# show ip dhcp relay gateway interface ethernet 3/5
---------                   -------------
Interface                      Gateway Address
---------                   -------------
Eth 3/5                           10.1.1.1
```

show ip dhcp relay statistics

Displays the general information about the DHCP Relay function.

Syntax

show ip dhcp relay statistics

Modes

Privileged EXEC mode

Usage Guidelines

The **show ip dhcp relay statistics** command displays the following information about the IP DHCP Relay function for IP DHCP Relay addresses configured on the switch:

- DHCP Server IP Address configured in the switch.
- Number of DHCP DISCOVERY, OFFER, REQUEST, ACK, NAK, DECLINE, and RELEASE packets received.
- Number of DHCP client packets received (on port 67) and relayed by the Relay Agent.
- Number of DHCP server packets received (on port 67) and relayed by the Relay Agent.

DHCP unicast packets are forwarded directly per route. These packets are not trapped to the management module. As a result, the DHCP renewal Request/ACK and DHCP Release packets are not be counted toward statistics.

Examples

To display general information about the DHCP relay function:

```
device# show ip dhcp relay statistics
             DHCP Relay Statistics:
       ------------------------
Address         Disc.      Offer      Req.     Ack       Nak       Decline     Inform
-------         -----     -----       ----     ---       ---       -------      ------
10.1.0.1        400        100        2972     2968      0          0
0
20.2.0.1        400        100        2979     2975      0          0
0
30.3.0.1        400        100        3003     2998      0          0
0
40.4.0.1        400        100        3026     3018      0          0
0

Client Packets: 12780
Server Packets: 12359
Client Packets Dropped: 0
Server Packets Dropped: 0
```

show ip dhcp snooping

Displays information from the DHCP snooping binding database.

Syntax

show ip dhcp snooping brief

show ip dhcp snooping informationoption

show ip dhcp snooping [**vlan***vlan-id*]

show ip dhcp snooping interface [*switchport interface*]

show ip dhcp snoopingbinding entries [**vlan***vlan-id*] [**interface** *switchport interface* **vlan** *vlan-id* **ip-address** *ip-addr* **mac** *mac-addr*]

show ip dhcp snoopingbinding stats

Parameters

brief

Displays brief information on DHCP snooping-enabled VLANs and the trusted state of member ports.

informationoption

Displays the state of the Option-82 feature on the device, including the Circuit-ID and Remote-ID information for all the DHCP snooping-enabled VLANs.

vlan*vlan-id*

Displays information about DHCP snooping on all configured VLANs or on the specified VLAN.

interface [*switchport interface*

Displays information about DHCP snooping configuration for all switchports or the specified switchport.

binding entries [**vlan***vlan-id*] [**interface** *switchport interface* **vlan** *vlan-id* **ip-address** *ip-addr* **mac** *mac-addr*]

Displays the complete binding database or displays database entries that are specific to the options you select.

binding stats

Displays statistics about the DHCP snooping binding entry database.

Modes

Privileged EXEC mode

Examples

The following example shows....

The following example shows....

show ip flowspec rules

Displays Border Gateway Protocol flow specification (BGP flowspec) rules that are considered for installation into the hardware.

Syntax

show ip flowspec rules [**detail**] [**local** | **remote**] [**vrf** *vrf-name*]

Parameters

detail

Specifies the display of detailed information which includes statistics for flowspec rules.

local

Specifies the display of only local flowspec rules.

remote

Specifies the display of only remote flowspec rules.

vrf *vrf-name*

Specifies the display of flowspec rule information for a VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

When a VRF is not specified, the **show ip flowspec rules** command displays information for the default VRF.

Displayed rules are sorted according to the sorting algorithm described in RFC 5575.

Output

The **show ip flowspec rules** command displays the following information:

Output field	Description
VRF	Name of a VRF instance
Total number of Flowspec rules	Number of configured flowspec rules
Origin	

Output field	Description
Active	Installation status of the BGP flowspec rule in the hardware. Values include: • Yes—The complete rule is installed • Yes (Match criteria contains expressions that always evaluate to FALSE)—Partial match criteria are installed • No (Match criteria always evaluates to FALSE)—The rule is not installed • No (Rule contains unsupported match criteria or actions or no TCAM space available)—The rule was passed to the hardware but could not be installed. • No (invalid Match combinations)—Different Layer 4 protocol types (for example, ICMP type and port) are used in match criteria.
Match	Match criteria
Dst	Destination prefix
Src	Source prefix
Protocol	IP protocol for IPv4
Port	Port number
DPort	Desination port number
SPort	Source port number
ICMP-type	Internet Control Message Protocol type
ICMP-Code	ICMP code
TCP-flags	TCP flags (CWR, ECE, URG, ACK, PSH, RST, SYN, FIN)
Pkt-length	Packet length
DSCP	IP Differentiated Services Code Point
Fragment	Fragment (DF, FF, IsF, DF)
Actions	Traffic filtering actions
Traffic-rate	Traffic-rate
Traffic-action	Traffic-action
Redirect IP Nexthop	Redirect IP Nexthop
Traffic-remarketing (DSCP)	Traffic-remarketing (DSCP)
Statistics	Statistics
Matched	Number of packets or bytes that match the flowspec rule
Transmitted	Number of packets matching the flowspec rule that are transmitted
Dropped	Number of packets matching the flowspec rule that are dropped

Examples

The following example shows how to display BGP flowspec rule information for the default VRF.

```
device# show ip flowspec rules

VRF :default-vrf VRF ID : 1
Total number of Rules: 2

1  Origin: Remote(51.51.51.254) Active: No (unsupported match/action type OR No TCAM
space available)
   Match:
      Dst          51.0.0.0/8
      DPort        =64051
   Actions:
      Traffic-rate  asn:51 rate 51000000 bytes/sec (operational-rate 51328125 bytes/sec)

2  Origin: Remote(61.61.61.1) Active: Yes
   Match:
      DPort        <9876
   Actions:
      Traffic-rate  asn:111 rate 187500 bytes/sec (operational-rate 186750 bytes/sec)
```

The following example shows how to display detailed BGP flowspec rule information for the default VRF.

```
device# show ip flowspec rules detail

VRF :default-vrf
Total number of Rules: 2

1 Origin: Local(flowmap:23) Active: Yes
  Match:
     DSCP         <60
  Actions:
     Traffic-rate asn 666, rate 125000 bits/sec(operational-rate 132000 bits/sec)

  Statistic       packets/bytes
  -------------   ------------
    Matched       17412786/12589441782
    Transmitted   1453/1048023
    dropped       17411333/12588393759

2 Origin: Remote (50.50.50.254) Active: No (invalid Match combinations)
  Match:
     Dst 91.92.93.0/24
     Src 70.70.70.0/24
     Protocol >=50 & <=67
     Port !=90
     DPort >909
     SPort <65530 | >2
     ICMP-type <=78
     ICMP-code >=90
     TCP-flags (Syn & Ack & Urg)
     Pkt-length =9887 | =50
     DSCP <60
     Fragment !(DF & FF)
  Actions:
     Traffic-rate            asn:50, rate 4800000 bits/sec(operational-rate 4400000 bits/
sec)
     Traffic-action          terminal-action
```

```
    Traffic-action          sample
    Redirect IP Nexthop     (redirect)1.2.3.4
    Redirect IP Nexthop     (mirror)1.2.3.4
    Traffic-remarking(DSCP) 56
```

show ip igmp groups

Displays information related to learned groups in the IGMP protocol module.

Syntax

show ip igmp groups [**detail** | **interface** | **vlan** *vlan_id* | **bridge-domain** *bridge-domain_id* | **cluster** *cluster_id* | **client** *client_id*]

Parameters

detail

Displays detailed information.

interface

Specifies an interface type.

vlan *vlan_id*

Specifies a VLAN interface.

bridge-domain *bridge-domain_id*

Specifies a bridge-domain interface.

cluster *cluster_id*

Specifies a Multi-Chassis Trunk (MCT) cluster.

client *client_id*

Specifies a Cluster Client Edge Port (CCEP) client.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the IGMP database, including configured entries for either all groups on all interfaces, or all groups on specific interfaces, or specific groups on specific interfaces.

Examples

The following example displays the IP IGMP groups.

```
device# show ip igmp groups
Total Number of Groups: 2
IGMP Connected Group Membership
Group Address  Interface Uptime      Expires      Last Reporter   Version
225.1.1.1      vlan25    00:05:27     00:02:32     25.1.1.120       2
Member Ports: eth 2/24

225.1.1.2 bridge-domain20 00:05:27    00:02:32     25.1.1.120       2
Member Ports:  eth4/22.600 eth6/15.200  po2.200
```

show ip igmp interface

Displays Layer 3 IGMP interface configuration information.

Syntax

show ip igmp interface [**ethernet** *slot/port* | **port-channel** | **Ve**]

Modes

Privileged EXEC mode

Usage Guidelines

Examples

The following example displays IGMP protocol information for port-channel 1.

```
device# show ip igmp interface port-channel 1

Interface po1
 IGMP disabled
```

The following example displays the output for the **show ip igmp interface** command.

```
device# show ip igmp interface

Interface eth1/34
IGMP enabled
  IGMP query interval 125 seconds
  IGMP other-querier interval 255 seconds
  IGMP query response time 10 seconds
  IGMP last-member query interval 1
seconds

  IGMP immediate-leave enabled
  IGMP querier 0.0.0.0(this system)
  IGMP version 3

Interface Ve 10
IGMP enabled
 IGMP query interval 125 seconds
 IGMP other-querier interval 255 seconds
 IGMP query response time 10 seconds
 IGMP last-member query interval 1 seconds
 IGMP immediate-leave enabled
 IGMP querier 10.10.10.10(this system)
 IGMP version 2
```

show ip igmp snooping

Displays IGMP snooping information.

Syntax

show ip igmp snooping [**mrouter vlan** *vlan_id* | **vlan** *vlan_id* | **bridge-domain** *bridge-domain_id*]

Parameters

mrouter vlan *vlan_id*

Specifies which VLAN interface to display the mrouter configuration related information.

vlan *vlan_id*

Specifies which VLAN interface to display the snooping configuration related information.

bridge-domain *bridge-domain_id*

Specifies which bridge-domain interface to display the snooping configuration related information.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **show ip igmp snooping** command to display IGMP snooping information, display multicast router port related information for the specified VLAN, or to display snooping statistics for the specified VLAN in the IGMP protocol module.

Examples

The following example displays IGMP snooping information.

```
device# show ip igmp snooping vlan 20
Vlan ID: 20
Multicast Router ports: eth4/2
Querier - Enabled,
IGMP Operation mode: IGMPv2
Is Fast-Leave Enabled : Disabled
Max Response time = 10
Last Member Query Interval = 1
Query interval = 125
Number of Multicast Groups: 1
Group: 225.0.0.1
Member Ports: eth4/2 eth6/15 po1
Mapped MAC address: 0100.5e00.0001


Bridge-domain ID: 20
```

```
Multicast Router ports: eth3/2.300
Querier - Enabled,
IGMP Operation mode: IGMPv2
Is Fast-Leave Enabled : Disabled
Max Response time = 10
Last Member Query Interval = 1
Query interval = 125
Number of Multicast Groups: 1
Group: 225.0.0.1
Member Ports: eth4/22.600 eth6/15.200 po2.200
Mapped MAC address: 0100.5e00.0001
```

show ip igmp ssm-map

Displays the association between a configured prefix list and source address mapped to it.

Syntax

show ip igmp ssm-map

Modes

Privileged EXEC mode

Output

The **show ip igmp ssm-map** command displays the following information:

Output field	Description
PrefixList Name	The name assigned to the prefix list.
Source Address	The source address IP.

Examples

The following example shows the association between a configured prefix list and source address mapped to it.

```
device# show ip igmp ssm-map

+-----------------------------------+-------------------+
|         PrefixList Name           |   Source Address  |
+-----------------------------------+-------------------+
   ssm-map-230-to-232                203.0.0.10
  ssm-map-233-to-234                204.0.0.11
```

show ip igmp statistics bridge-domain

Displays IGMP statistics for the bridge-domain.

Syntax

show ip igmp statistics bridge-domain *bridge-domain_id*

Parameters

bridge-domain *bridge-domain_id*

Specifies the bridge-domain ID.

Modes

Privileged EXEC mode

Examples

The following example displays the output for the **show ip igmp statistics interface bridge-domain** command.

```
device# show ip igmp statistics interface bridge-domain  20
IGMP packet statistics for all interfaces in bridge-domain 20:
IGMP Message type     Edge-Received Edge-Sent Edge-Rx-Errors
Membership Query       40              40              0
V1 Membership Report     40          40          0
V2 Membership Report     0          60          0
Group Leave          20          20          0
V3 Membership Report     0          0          0
PIM hello          0          0          0
IGMP Error Statistics:
Unknown types 0
Bad Length 0
Bad Checksum 0
```

show ip igmp statistics interface

Displays IGMP statistics for an interface.

Syntax

show ip igmp statistics interface [**ethernet** *slot/port* | **ve** *ve interface ID*]

Parameters

ethernet*slot/port*

Represents an Ethernet interface name in slot/port format.

ve *Ve interface number*

Specifies a virtual Ethernet (VE) interface number. The range is 1 - 8192.

Modes

Privileged EXEC mode

Examples

The following example displays the output of the **show ip igmp statistics interface** command.

```
device# show ip igmp statistics interface ve100

IGMP packet statistics for ve100:
IGMP Message type            Edge-Received  Edge-Sent  Edge-Rx-Errors
Membership Query                    0             229           0
V1 Membership Report                0             0             0
V2 Membership Report                0             0             0
Group Leave                         0             0             0
V3 Membership Report                0             0             0
PIM hello                         456             0             0

IGMP Error Statistics:
Unknown types     0
Bad Length        0
Bad Checksum      0
```

show ip igmp statistics vlan

Displays information for a specific VLAN.

Syntax

show ip igmp statistics vlan *vlan-id*

Parameters

vlan-id

Specifies the VLAN-ID. The range is 1 through 4090.

Modes

Privileged EXEC mode

Examples

The following example displays the IP IGMP statistics on VLAN 1.

```
device# show ip igmp statistics interface vlan 1

IGMP packet statistics for all interfaces in vlan 1:
IGMP Message type     Edge-Received   Edge-Sent   Edge-Rx-Errors   ISL Received
Membership Query                  0           0                0              0
V1 Membership Report              0           0                0              0
V2 Membership Report              0           0                0              0
Group Leave                       0           0                0              0
V3 Membership Report              0           0                0              0
PIM hello                         0           0                0              0

IGMP Error Statistics:
Unknown types            0
Bad Length               0
Bad Checksum             0
```

show ip interface

Displays the IP address, status, and configuration for a specified interface or for all interfaces.

Syntax

show ip interface { **brief** | **ethernet** *slot/port* | **port-channel** *number* }

Parameters

brief

Specifies a brief summary of IP interface status and configuration.

ethernet *slot/port*

Specifies an Ethernet slot and port.

port-channel *number*

Specifies a port-channel.

Modes

Privileged EXEC mode

Examples

The following example displays typical summary information about all interfaces.

```
device# show ip interface brief
Flags:  I - Insight Enabled     U - Unnumbered interface    M - Redundant Management
Interface              IP-Address          Vrf
Status                    Protocol
==================     ==========          ==================
====================      ========
Loopback 42            42.42.42.2           mgmt-vrf
up                        up
Loopback 45            unassigned           default-vrf             administratively
down     down
Ethernet 0/1           unassigned           default-vrf
up                        down
Ethernet 0/2           unassigned           default-vrf
up                        down
Ethernet 0/3           43.43.43.2           mgmt-vrf
up                        down
Ethernet 0/4           unassigned           default-vrf
up                        up
Ethernet 0/5           unassigned           default-vrf
up                        down
Ethernet 0/6           unassigned           default-vrf
up                        down
Ethernet 0/7           unassigned           default-vrf
up                        down
Ethernet 0/8           unassigned           default-vrf
up                        down
Ethernet 0/9           unassigned           default-vrf
up                        down
```

```
Ethernet 0/10          unassigned          default-vrf
up                        up
Ethernet 0/11          unassigned          default-vrf
up                        down
Ethernet 0/12          unassigned          default-vrf
up                        down
Ethernet 0/13          unassigned          default-vrf
up                        down
Ethernet 0/14          unassigned          default-vrf
up                        down
Ethernet 0/15          unassigned          default-vrf
up                        down
Ethernet 0/16          unassigned          default-vrf
up                        down
Ethernet 0/17          unassigned          default-vrf
up                        down
Ethernet 0/18          unassigned          default-vrf
up                        down
Ethernet 0/19          unassigned          default-vrf
up                        down
Ethernet 0/20:1        unassigned          default-vrf
up                        up
Ethernet 0/20:2        40.40.40.2          mgmt-vrf
up                        up
Ethernet 0/20:3        unassigned          default-vrf
up                        down
Ethernet 0/20:4        unassigned          default-vrf
up                        down
Ethernet 0/21          unassigned          default-vrf
up                        down
Ethernet 0/22          unassigned          default-vrf
up                        down
Ethernet 0/23          unassigned          default-vrf
up                        down
Ethernet 0/24          unassigned          default-vrf
up                        down
Ethernet 0/25          unassigned          default-vrf
up                        down
Ethernet 0/26          unassigned          default-vrf
up                        down
Ethernet 0/27          unassigned          default-vrf
up                        up
Ethernet 0/28          unassigned          default-vrf
up                        down
Ethernet 0/29          unassigned          default-vrf
up                        down
Ethernet 0/30          unassigned          default-vrf
up                        down
Ethernet 0/31:1(M)     unassigned          mgmt-vrf
up                        up
Ethernet 0/31:2        unassigned          default-vrf             administratively
down     down
Ethernet 0/31:3        unassigned          default-vrf             administratively
down     down
Ethernet 0/31:4        unassigned          default-vrf             administratively
down     down
Ethernet 0/32          unassigned          default-vrf             administratively
down     down
Ve 3                   unassigned          default-vrf             administratively
down     down
Ve 41                  41.41.41.2          mgmt-vrf
up                        up
```

The following example displays the IP interface status of a specified Ethernet port.

```
device# show ip interface ethernet 1/1
 Ethernet 1/2 is up, line protocol is down (Link-OAM blocked link), Link-OAM is enabled
Hardware is Ethernet, address is 00e0.0c70.c005
    Current address is 00e0.0c70.c005
Pluggable media present
Interface index (ifindex) is 406880257
MTU 1548 bytes
10G Interface
LineSpeed Actual     : Nil
LineSpeed Configured : Auto, Duplex: Full
Priority Tag disable
Last clearing of show interface counters: 10:50:20
Queueing strategy: fifo
Receive Statistics:
    67181801 packets, 8867997496 bytes
    Unicasts: 67181799, Multicasts: 1, Broadcasts: 1
    64-byte pkts: 1, Over 64-byte pkts: 4, Over 127-byte pkts: 67181796
    Over 255-byte pkts: 0, Over 511-byte pkts: 0, Over 1023-byte pkts: 0
    Over 1518-byte pkts(Jumbo): 0
    Runts: 0, Jabbers: 0, CRC: 0, Overruns: 0
    Errors: 0, Discards: 0
Transmit Statistics:
    82627975 packets, 10906817712 bytes
    Unicasts: 82627873, Multicasts: 11, Broadcasts: 89
    Underruns: 0
    Errors: 0, Discards: 0
Rate info:
    Input 0.000000 Mbits/sec, 0 packets/sec, 0.00% of line-rate
    Output 0.001014 Mbits/sec, 1 packets/sec, 0.00% of line-rate
Time since last interface status change: 00:08:22
```

show ip multicast snooping

Displays IP multicast snooping configuration information.

Syntax

show ip multicast snooping [**mcache** *vlan interface* | **vlan** *vlan-id*]

Parameters

mcache

Specifies the multicast cache entries.
vlan interface

Specifies which VLAN's snooping mcache entries should be displayed.

vlan

Specifies the VLAN.
vlan-id

Specifies the VLAN-ID.

Modes

User EXEC mode

Examples

The following example displays the output for the **show ip multicast snooping mcache** command.

```
device# show ip multicast snooping mcache
Flags : V2|V3 : IGMP Receiver, P_G : PIM (*,G) Join, P_SG: PIM (S,G) Join
VlanID : 25
-------------
1(*, 225.1.1.1 )00:02:15NumOIF: 1
Outgoing Ports:
eth2/24       Flags: 0x14 ( V2)  00:02:15/126s
```

The following output displays v3 flag for entries learned through the IGMPv3 report.

```
device# show ip multicast snooping mca
Flags : V2|V3 : IGMP Receiver, P_G : PIM (*,G) Join, P_SG: PIM (S,G) Join
                 BR : PIM Blocked RPT
 Vlan ID : 10
 -------------
1     (20.20.20.20, 232.0.0.10 )  22:37:48    NumOIF: 1
        Outgoing Ports:
                eth1/34        Flags: 0x24 ( V3)  00:00:08/252s
```

show ip ospf

Displays OSPF information.

Syntax

show ip ospf [**vrf** *name*]

Parameters

vrf *name*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Usage Guidelines

Examples

The following example shows sample output from the **show ip ospf** command.

```
device# show ip ospf
OSPF Version                    Version 2
Router Id                       10.0.0.4
ASBR Status                     No
ABR Status                      No          (0)
Redistribute Ext Routes from
Initial SPF schedule delay      0           (msecs)
Minimum hold time for SPFs      0           (msecs)
Maximum hold time for SPFs      0           (msecs)
External LSA Counter            0
External LSA Checksum Sum       0
Originate New LSA Counter       0
Rx New LSA Counter              0
External LSA Limit              14913080
Administrative Distance
  -  External Routes:           110
  -  Intra Area Routes:         110
  -  Inter Area Routes:         110
Database Overflow Interval      0
Database Overflow State :       NOT OVERFLOWED
RFC 1583 Compatibility :        Disabled
NSSA Translator:                Enabled
Nonstop Routing:                Disabled
Graceful Restart                Enabled
Graceful Restart Helper         Enabled
Graceful Restart Time           120
LDP-SYNC: Not globally enabled
Interfaces with LDP-SYNC enabled:
    None
```

show ip ospf area

Displays the OSPF area table in a specified format.

Syntax

show ip ospf area { *A.B.C.D* | *decimal* } **database link-state** [**adv-router** *router-id* | **advertise** *index* | **asbr** { *asbr-id* | **adv-router** *router-id* } | **extensive** | **link-state-id** *id* | **network** { *net-id* | **adv-router** *router-id* } | **nssa** { *nssa-id* | **adv-router** *router-id* } | **router** { *router-id* | **adv-router** *router-id* } | **self-originate** | **sequence-number** *num* | **summary** { *id* | **adv-router** *router-id* }] [**vrf** *vrfname*]

show ip ospf area [**vrf** *vrfname*]

Parameters

A.B.C.D

Area address in dotted decimal format.

decimal

Area address in decimal format. Valid values range from 0 to 2147483647.

database link-state

Displays database link-state information.

adv-router *router-id*

Displays the link state for the advertising router that you specify.

advertise *index*

Displays the link state by Link State Advertisement (LSA) index.

asbr

Displays the link state for all autonomous system boundary router (ASBR) links.

asbr-id

Displays the state of a single ASBR link that you specify.

extensive

Displays detailed information for all entries in the OSPF database.

link-state-id *id*

Displays the link state by link-state ID.

network

Displays the link state by network link.

net-id

Displays the link state of a particular network link that you specify.

nssa

Displays the link state by not-so-stubby area (NSSA).

nssa-id

Displays the link state of a particular NSAA area that you specify.

router

Displays the link state by router link.
router-id

Displays the link state of a particular router link that you specify.

self-originate

Displays self-originated link states.

sequence-number *num*

Displays the link-state by sequence number that you specify.

summary

Displays the link state summary. Can specify link-state ID or advertising router ID.
id

Displays the link state for the advertising router that you specify.

vrf vrf *name*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Examples

The following example shows output for the **show ip ospf area** command.

```
device# show ip ospf area

Number of Areas is 1

Index   Area            Type   Cost       SPFR       ABR   ASBR  LSA     Chksum(Hex)
1       0               normal 0          4305       0     0     5       00024f5a
```

show ip ospf border-routers

Displays information about border routers and boundary routers.

Syntax

show ip ospf border-routers [*A.B.C.D*] [**vrf** *vrfname*]

Parameters

A.B.C.D

Specifies the router ID in dotted decimal format.

vrf *vrf name*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display information about area border routers (ABRs) and autonomous system boundary routers (ASBRs). You can display information for all ABRs and ASBRs or for a specific router. Tunnel next-hop is also displayed.

Examples

The following example displays information for all ABRs and ASBRs:

```
device# show ip ospf border-routers
Index  Router-ID       Router-type      Next-hop-router  Outgoing-interface   Area
1      2.2.2.2         ASBR             2.2.2.2          Eth 0/2              1
2      2.2.2.2         ASBR             30.1.1.2         Lsp 1                1
```

show ip ospf config

Displays OSPF information.

Syntax

show ip ospf config [**vrf** *name*]

Parameters

vrf *name*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Usage Guidelines

Examples

The following example shows sample output from the `show ip ospf config` command.

```
device# show ip ospf config

Router OSPF: Enabled
Nonstop Routing: Disabled
Graceful Restart: Enabled
Graceful Restart Helper: Enabled
Graceful Restart Time: 120

Redistribution: Disabled
Default OSPF Metric: 10
Maximum Paths: 8
OSPF Auto-cost Reference Bandwidth: Disabled
Default Passive Interface: Disabled
OSPF Redistribution Metric: Type2
OSPF External LSA Limit: 14913080
OSPF Database Overflow Interval: 0
RFC 1583 Compatibility: Disabled
VRF Lite capability: Disabled
Router id: 10.0.0.4
```

show ip ospf database

Shows OSPFv2 database information.

Syntax

show ip ospf database database-summary [**vrf** *vrfname*]

show ip ospf database external-link-state [**advertise** *index* | **extensive** | **link-state-id** *id* | **router-id** *router-id* | **sequence-number** *num*] [**vrf** *vrfname*]

show ip ospf database grace-link-state [**vrf** *vrfname*]

show ip ospf database link-state [**adv-router** *router-id* | **advertise** *index* | **asbr** { *asbr-id* | **adv-router** *router-id* } | **extensive** | **link-state-id** *id* | **network** { *net-id* | **adv-router** *router-id* } | **nssa** { *nssa-id* | **adv-router** *router-id* } | **router** { *router-id* | **adv-router** *router-id* } | **self-originate** | **sequence-number** *num* | **summary** { *id* | **adv-router** *router-id* }] [**vrf** *vrfname*]

show ip ospf database [**vrf** *vrfname*]

Parameters

database-summary

Displays how many link state advertisements (LSAs) of each type exist for each area, as well as total number of LSAs.

vrf *name*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

external-link-state

Displays information by external link state, based on the following parameters:
advertise *index*

Displays the hexadecimal data in the specified LSA packet. The *index* parameter identifies the LSA packet by its position in the router's External LSA table.
To determine an LSA packet's position in the table, enter the **show ip ospf external-link-state** command.

extensive

Displays LSAs in decrypt format. Do not use this parameter in combination with other display parameters because the entire database is displayed.

link-state-id *id*

Displays external LSAs for the LSA source that you specify.

router-id *router-id*

Displays external LSAs for the advertising router that you specify.

sequence-number *num*

Displays the External LSA entries for the hexadecimal LSA sequence number that you specify.

link-state

Displays the link state, based on the following parameters:
adv-router *router-id*

Displays the link state for the advertising router that you specify.

advertise *index*

Displays the hexadecimal data in the specified LSA packet. The *index* parameter identifies the LSA packet by its position in the router's external-LSA table. To determine an LSA packet's position in the table, enter the **show ip ospf external-link-state** command.

asbr

Displays autonomous system boundary router (ASBR) LSAs.

extensive

Displays LSAs in decrypt format. Do not use this parameter in combination with other display parameters because the entire database is displayed.

link-state-id *id*

Displays LSAs for the LSA source that you specify.

network

Displays either all network LSAs or the LSAs for a network that you specify.

nssa

Displays either all NSSA LSAs or the LSAs for a not-so-stubby area (NSSA) that you specify.

router

Displays LSAs by router link.

router-id *router-id*

Displays LSAs for the advertising router that you specify.

self-originate

Displays self-originated LSAs.

sequence-number

Displays the LSA entries for the hexadecimal LSA sequence number that you specify.

summary

Displays summary information. You can specify link-state ID or advertising router ID.

adv-router *router-id*

Displays the link state for the advertising router that you specify.

Modes

Privileged EXEC mode

Examples

The following example shows output for the **show ip ospf database** command.

```
device# show ip ospf database

Link States

Index Area ID         Type LS ID           Adv Rtr         Seq(Hex)        Age  Cksum
1     0               Rtr  200.1.2.3       200.1.2.3       0x80000bb8      235  0x6a51
2     0               Rtr  20.20.20.20     20.20.20.20     0x80000088      1680 0xcb6a
3     0               Rtr  54.1.1.1        54.1.1.1        0x8000009f      599  0x6c3d
4     0               Net  53.1.1.1        200.1.2.3       0x80000006      235  0xd22
5     0               Net  53.54.43.53     200.1.2.3       0x8000007e      626  0x53e6
```

The following example shows output for the **show ip ospf database** command when the **database-summary** keyword is used.

```
device# show ip ospf database database-summary

Area ID          Router  Network  Sum-Net  Sum-ASBR  NSSA-Ext  Opq-Area  Subtotal
0                3       2        0        0         0         0         5
AS External                                                              0
Total            3       2        0        0         0         0         5
```

show ip ospf filtered-lsa area

Displays information about type3 LSA filters attached to specified OSPFv2 areas and lists LSAs filtered in or out.

Syntax

show ip ospf filtered-lsa area { *ip-address* | *decimal* } { **in** | **out** } [**vrf** *vrf-name*]

Parameters

ip-address

Specifies the IP address of an area.

decimal

Specifies an area address in decimal format. Valid values range from 0 through 2147483647.

in

Specifies the incoming direction.

out

Specifies the outgoing direction.

vrf *vrf-name*

Specifies the name of the VRF instance.

Modes

Privileged EXEC mode

Examples

The following example displays information about type 3 LSA filtering in the out direction for OSPFv2 area 0.

```
device# show ip ospf filtered-lsa area 0 out
```

show ip ospf interface

Displays information about all or specific OSPF-enabled interfaces.

Syntax

show ip ospf interface [*A.B.C.D* | **brief**] [**vrf** *vrf-name*]

show ip ospf interface [**ethernet** *slot/port* | | **loopback** *number* | **port-channel** *number* | **ve** *vlan_id*] [**brief**] [**vrf** *vrf-name*]

show ip ospf interface [**vrf** *vrf-name*]

Parameters

A.B.C.D

Specifies interface IP address in dotted decimal format.

brief

Displays summary information.

vrf *vrf-name*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

ethernet *slot/port*

Specifies an Ethernet slot and port.

loopback *number*

Specifies a loopback port number. Valid values range from 1 through 255.

port-channel *number*

Specifies a port-channel.

ve *vlan_id*

Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096

Modes

Privileged EXEC mode

Usage Guidelines

Examples

The following example displays OSPF information about all enabled interfaces.

```
device# show ip ospf interface

Ethernet 1/2 admin up, oper up
     IP Address 53.1.1.36, Area 0
     BFD is disabled
     Database Filter: Not Configured
```

```
     State BDR, Pri 1, Cost 1, Options ------E-, Type broadcast Events 3
     Timers(sec): Transmit 1, Retrans 5, Hello 10, Dead 40
     DR:  Router ID 200.1.2.3         Interface Address 53.1.1.1
     BDR: Router ID 20.20.20.20       Interface Address 53.1.1.36
     Neighbor Count = 1, Adjacent Neighbor Count= 1
     Neighbor:         53.1.1.1 [id 200.1.2.3] (DR)
     Authentication-Key: None
     MD5 Authentication: Key None, Key-Id  None , Auth-change-wait-time 300
LDP-SYNC: Disabled, State: -

Loopback 1 admin up, oper up
     IP Address 20.20.20.20, Area 0
     BFD is disabled
     Database Filter: Not Configured
     State DR, Pri 1, Cost 1, Options ------E-, Type broadcast Events 2
     Timers(sec): Transmit 1, Retrans 5, Hello 10, Dead 40
     DR:  Router ID 20.20.20.20       Interface Address 20.20.20.20
     BDR: Router ID 0.0.0.0           Interface Address 0.0.0.0
     Neighbor Count = 0, Adjacent Neighbor Count= 0
     Authentication-Key: None
     MD5 Authentication: Key None, Key-Id  None , Auth-change-wait-time 300
LDP-SYNC: Disabled, State: -
```

show ip ospf lsp-shortcuts

Displays OSPF LSP shortcut information.

Syntax

show ip ospf lsp-shortcuts

Parameters

lsp-shortcuts

Displays LSP shortcut information

Modes

Privilege Executable mode

Output

The **show ip ospf lsp-shortcuts** command displays the following information:

Output field	Description
LSP Id	The assigned LSP Id.
State	Displays *Up* or *Down* that indicates the current status of the LSP shortcut.
Nbr IP Address	Displays the IP address of the neighbor device.
Metric	Displays the assigned metric for this neighbor device.

Examples

The following example shows information about the configured OSPF LSP shortcuts.

```
SLX # show ip ospf lsp-shortcuts
OSPF LSP Shortcuts: 1
LSP Id    State          Nbr IP Address     Metric
Lsp 1     Up             2.2.2.2             0
Lsp 3     Up             2.2.2.2             0
Lsp 2     Up             2.2.2.2             5
SLX #
```

show ip ospf neighbor

Displays OSPF neighbor information.

Syntax

show ip ospf neighbor [**extensive**] [**ethernet** *slot/port* | **port-channel** *number* | **router-id** *A.B.C.D* | **ve** *vlan_id*] [**vrf** *vrf-name*]

show ip ospf neighbor [**vrf** *vrf-name*]

Parameters

extensive

Displays detailed neighbor information.

ethernet *slot/port*

Specifies an Ethernet slot and port.

port-channel *number*

Specifies a port-channel.

router-id *A.B.C.D*

Displays neighbor information for the specified router ID (in dotted decimal format).

ve *vlan_id*

Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

vrf *vrf-name*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF instance are shown in the output.

Modes

Privileged EXEC mode

Usage Guidelines

Examples

The following example displays information about OSPF neighbors.

```
device# show ip ospf neighbor

Number of Neighbors is 1, in FULL state 1

Port            Address         Pri State      Neigh Address   Neigh ID        Ev      Opt
Cnt
Eth 1/2         53.1.1.36       1   FULL/DR    53.1.1.1        200.1.2.3       6       66
0
```

show ip ospf redistribute route

Displays routes that have been redistributed into OSPF.

Syntax

show ip ospf redistribute route [*A.B.C.D:M*] [**vrf** *vrfname*]

Parameters

A.B.C.D:M

Specifies an IP address and mask for the output.

vrf *vrfname*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

show ip ospf routes

Displays OSPF calculated routes.

Syntax

show ip ospf routes [*A.B.C.D*] [**vrf** *vrfname*]

Parameters

A.B.C.D

Specifies a destination IP address in dotted decimal format.

vrf *vrfname*

Specifies the name of the VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display routes that OSPF calculated. You can display all routes or you can display information about a specific route. Tunnel next-hop is also displayed.

Examples

The following example displays all OSPF-calculated routes.

```
device# show ip ospf routes

OSPF Regular Routes 8:

      Destination         Mask            Path_Cost Type2_Cost Path_Type
      1.1.1.1             255.255.255.255 1         0          Intra
      Adv_Router          Link_State      Dest_Type State      Tag       Flags
      1.1.1.1             1.1.1.1         Network   Valid      0          6
      Paths Out_Port      Next_Hop        Type      State
      1     Lo 1          0.0.0.0         OSPF      0  0

      Destination         Mask            Path_Cost Type2_Cost Path_Type
      1.1.1.2             255.255.255.255 1         0          Intra
      Adv_Router          Link_State      Dest_Type State      Tag       Flags
      1.1.1.1             1.1.1.1         Network   Valid      0          6
      Paths Out_Port      Next_Hop        Type      State
      1     Lo 2          0.0.0.0         OSPF      0  0

      Destination         Mask            Path_Cost Type2_Cost Path_Type
      1.1.1.3             255.255.255.255 1         0          Intra
      Adv_Router          Link_State      Dest_Type State      Tag       Flags
      1.1.1.1             1.1.1.1         Network   Valid      0          6
      Paths Out_Port      Next_Hop        Type      State
      1     Lo 3          0.0.0.0         OSPF      0  0
```

```
    Destination         Mask            Path_Cost Type2_Cost Path_Type
    1.1.1.4             255.255.255.255 1         0          Intra
    Adv_Router          Link_State      Dest_Type State      Tag       Flags
    1.1.1.1             1.1.1.1         Network   Valid      0          6
    Paths Out_Port      Next_Hop        Type      State
    1     Lo 4          0.0.0.0         OSPF      0  0

    Destination         Mask            Path_Cost Type2_Cost Path_Type
    1.1.1.5             255.255.255.255 1         0          Intra
    Adv_Router          Link_State      Dest_Type State      Tag       Flags
    1.1.1.1             1.1.1.1         Network   Valid      0          6
    Paths Out_Port      Next_Hop        Type      State
    1     Lo 5          0.0.0.0         OSPF      0  0

    Destination         Mask            Path_Cost Type2_Cost Path_Type
    1.1.1.6             255.255.255.255 1         0          Intra
    Adv_Router          Link_State      Dest_Type State      Tag       Flags
    1.1.1.1             1.1.1.1         Network   Valid      0          6
    Paths Out_Port      Next_Hop        Type      State
    1     Lo 6          0.0.0.0         OSPF      0  0

    Destination         Mask            Path_Cost Type2_Cost Path_Type
    1.1.1.7             255.255.255.255 1         0          Intra
    Adv_Router          Link_State      Dest_Type State      Tag       Flags
    1.1.1.1             1.1.1.1         Network   Valid      0          6
    Paths Out_Port      Next_Hop        Type      State
    1     Lo 7          0.0.0.0         OSPF      0  0

    Destination         Mask            Path_Cost Type2_Cost Path_Type
    2.2.2.2             255.255.255.255 1         0          Intra
    Adv_Router          Link_State      Dest_Type State      Tag       Flags
    2.2.2.2             2.2.2.2         Asbr      Valid      0         2
    Paths Out_Port      Next_Hop        Type      State
    1     Lsp 1         2.2.2.2         OSPF      ac 4a
    2     Eth 0/5       30.1.1.2        OSPF      0  0
```

show ip ospf summary

Displays summary information for all OSPF instances.

Syntax

show ip ospf summary [**vrf** *vrfname* | **all-vrfs**| **all-vrfs total**]

Parameters

vrf *vrfname*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

all-vrfs

Specifies all VRF instances. If this option is not used, details for the default VRF are shown in the output.

all-vrfs total

Displays the cumulative summary of OSPF information with the total numbers for all of the VRF intances. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Examples

The following example shows sample output with the details for the default VRF from the **show ip ospf summary** command.

```
device# show ip ospf summary

Seq Instance        Intfs   Nbrs    Nbrs-Full LSAs    Routes
1   default-vrf     5       2       1         12      2
```

The following example shows sample output from the **show ip ospf summary all-vrfs** command.

```
device# show ip ospf summary all-vrfs

Seq Instance        Intfs   Nbrs    Nbrs-Full LSAs    Routes
1   default-vrf     0       0       0         0       0
2   vrf_1           0       0       0         0       0
```

The following example shows sample output from the **show ip ospf summary all-vrfs total** command.

```
device# show ip ospf summary all-vrfs total
```

```
-----------------------------------------
        IPv4 OSPF VRFs Summary Total
-----------------------------------------
Number of VRFs: 1
Number of Interfaces: 200
Number of Neighbors: 200
Number of Neighbors in Full state: 200
Number of LSAs: 182600
Number of Routes: 102600
device#
```

show ip ospf traffic

Displays OSPF traffic details.

Syntax

show ip ospf traffic

show ip ospf traffic [**ethernet** *slot/port* | **loopback** *number* | **ve** *vlan_id*] [**vrf** *vrf-name*]

Parameters

interface

Specifies an interface.

ethernet *slot* **/** *port*

Specifies an Ethernet slot and port.

loopback *number*

Specifies a loopback interface. Valid values range from 1 through 255.

ve *vlan_id*

Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

vrf *vrf-name*

Specifies the name of the VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display details of OSPF traffic sent and received. You can display all traffic or specify a particular interface.

Examples

The following example shows all OSPF traffic.

```
device# show ip ospf traffic

                 Packets Received         Packets Sent
Hello                          10                   10
Database                       90                   89
LSA Req                        12                   11
LSA Upd                        12                   12
LSA Ack                        12                   12
No Packet Errors!
```

show ip ospf virtual link

Displays information about virtual links.

Syntax

show ip ospf virtual link [*index*] [**vrf** *vrfname*]

Parameters

index

Shows information about all virtual links or one virtual link that you specify.

vrf *vrfname*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Usage Guidelines

Examples

The following example shows information about all virtual links.

```
device# show ip ospf virtual link
```

show ip ospf virtual neighbor

Displays information about virtual neighbors.

Syntax

show ip ospf virtual neighbor [*index*] [**vrf** *vrfname*]

Parameters

index

Shows information about all virtual neighbors or one virtual neighbor that you specify.

vrf *vrfname*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Usage Guidelines

Examples

The following example shows information about all virtual neighbors:

```
device# show ip ospf virtual neighbor
```

show ip pim bsr

Displays bootstrap router (BSR) information.

Syntax

show ip pim bsr [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Displays information for a specific VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

When entered without the **vrf** option, this command displays information for the default VRF instance.

Output

The **show ip pim bsr** command displays the following information:

Output Field.	Description
BSR address	The IP address of the interface configured as the PIM Sparse BSR.
BSR priority	The priority assigned to the interface for use during the BSR election process. During BSR election, the priorities of the candidate BSRs are compared and the interface with the highest BSR priority becomes the BSR.
Hash mask length	The number of significant bits in the IP multicast group comparison mask. This mask determines the IP multicast group numbers for which the device can be a BSR. The default is 32 bits, which allows the device to be a BSR for any valid IP multicast group number. **Note:** This field appears only if this device is a candidate BSR.
Next bootstrap message in	Indicates how much time will pass before the BSR sends the next bootstrap message. The time is displayed in "hh:mm:ss" format. **Note:** This field appears only if this device is the BSR.
Next Candidate-RP-advertisement message in	Indicates how much time will pass before the BSR sends the next candidate PR advertisement message. The time is displayed in "hh:mm:ss" format. **Note:** This field appears only if this device is a candidate BSR.
RP	Indicates the IP address of the Rendezvous Point (RP). **Note:** This field appears only if this device is a candidate BSR.
group prefixes	Indicates the multicast groups for which the RP listed by the previous field is a candidate RP. **Note:** This field appears only if this device is a candidate BSR.
Candidate-RP-advertisement period	Indicates how frequently the BSR sends candidate RP advertisement messages. **Note:** This field appears only if this device is a candidate BSR.

Examples

The following example shows information for a device that has been elected as the BSR.

```
device# show ip pim bsr
PIMv2 Bootstrap information
------------------------------------------------------------------------------
  This system is the Elected BSR
```

```
  BSR address: 1.51.51.1. Hash Mask Length 32. Priority 255.
  Next bootstrap message in 00:01:00
  Configuration:
    Candidate loopback 2 (Address 1.51.51.1). Hash Mask Length 32. Priority 255.
Next Candidate-RP-advertisment in 00:01:00
  RP: 1.51.51.1
    group prefixes:
    224.0.0.0 / 4
  Candidate-RP-advertisement period: 60
```

The following example shows information for a device that is not the BSR.

```
device(config)# show ip pim bsr
PIMv2 Bootstrap information
------------------------------------------------------------------------------
  BSR address: 1.51.51.1. Hash Mask Length 32. Priority 255.
Next Candidate-RP-advertisment in 00:00:30
  RP: 1.51.51.3
    group prefixes:
    224.0.0.0 / 4
  Candidate-RP-advertisement period: 60
```

show ip pim interface

Displays information for PIM interfaces.

Syntax

show ip pim interface [**vrf** *vrf-name*]

show ip pim interface { **ethernet** *slot*/*port-id* | **loopback** *loopback-number* | **ve** *vlan ID* } [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Specifies a VRF.

ethernet *slot*/*port-id*

Specifies a physical interface. For devices without linecards, specify `0` for the slot.

loopback *loopback-number*

Specifies a loopback interface.

ve *vlan ID*

Specifies a virtual interface.

Modes

Privileged EXEC mode

Examples

The following example displays unfiltered **show ip pim interface** output.

```
device# show ip pim interface
-------------+---------------+----+-----+-------------------------------+---+------
Interface |Local    |Ver|Mode | Designated Router |TTL| DR
          |Address |    |     |Address      Port   |Thr| Prio
-------------+---------------+-----------------------------------------+---+------
Eth 2/30  55.1.1.1  v2   SM  Itself               1    1
Ve30      30.1.1.1  v2   SM  30.1.1.20    Ve30     1    1
Lo        1 4.4.4.4 v2   SM  Itself 1 1
```

show ip pim mcache

Displays the multicast cache.

Syntax

show ip pim mcache [*A.B.C.D* | **ecmp** *ipv4 address*]

Parameters

A.B.C.D

Specifies the multicast group or source IP address.

ecmp*ipv4 address*

Specifies the PIM ECMP IPv4 information.

Modes

Privileged EXEC mode

Examples

The following example displays the output for **show ip pim mcache**.

```
SLX# sh ip pim mcache 239.1.1.1
IP Multicast Mcache Table
Entry Flags : sm - Sparse Mode, ssm - Source Specific Multicast
RPT - RPT Bit, SPT - SPT Bit, LSrc - Local Source
LRcv - Local Receiver, RegProbe - Register In Progress
RegSupp - Register Suppression Timer, Reg - Register Complete
needRte - Route Required for Src/RP, JDUp - Join Desire Upstream
MDT - Multicast Distribution Tree Join sent/received
Interface Flags: IM - Immediate, IH - Inherited, WA - Won Assert
MJ - Membership Join, MI - Membership Include, ME - Membership Exclude
BR - Blocked RPT, BA - Blocked Assert, BF - Blocked Filter
BI - Blocked IIF, UJ - Unintended Join oif
Total entries in mcache: 16
1 (3.3.3.3, 239.1.1.1) in Eth 0/47, Uptime 02:17:18
SSM=1, RPT=0 SPT=1 Reg=0 RegSupp=0 RegProbe=0 JDUp=0 LSrc=0 LRcv=0 MDT=1
upstream neighbor=15.1.1.200
AgeSltMsk: 0 KAT timer value: Infinity
num_oifs = 0
Flags (0x080281d4)
ssm=1 needRte=0
2 (5.5.5.5, 239.1.1.1) in NIL, Uptime 02:17:17
SSM=1, RPT=0 SPT=1 Reg=0 RegSupp=0 RegProbe=0 JDUp=1 LSrc=0 LRcv=0 MDT=1
No upstream neighbor because source 5.5.5.5 is itself
AgeSltMsk: 0 KAT timer value: Infinity
num_oifs = 1
Eth 0/47(02:17:17/202) Flags: IM
Flags (0x0c0285d0)
ssm=1 needRte=1
```

show ip pim mdt

Displays MDTs maintained by PIM.

Syntax

show ip pim mdt

show ip pim mdt detail

show ip pim mdt group *GROUP-IP-ADDRESS*

Parameters

detail

Displays detailed output for each MDT.

group *GROUP-IP-ADDRESS*

Displays detailed output for one MDT.

Modes

Privileged EXEC mode

Examples

The following examples shows brief output of all MDTs.

```
SLX# show ip pim mdt
Local VTEP IP: 5.5.5.5
MDT Join Role: Primary
Total MDT entries: 4
Group        Tunnel Id      State
(d)-default
------------    ---------    ---------
239.1.1.1(d)    32774        Up
239.1.1.103     32772        Up
239.1.1.110     32773        Up
239.1.1.200     32775        Up
```

The following examples shows detailed output of all PIM MDTs.

```
SLX# show ip pim mdt detail
Local VTEP IP: 5.5.5.5
MDT Join Role: Primary
Total MDT entries: 4
Group: 239.1.1.1(default)
Active VLANs: 100-102
Active BDs:
Remote VTEP IPs: 3.3.3.3, 4.4.4.4, 12.12.12.12
Tunnel Id: 32775 (0x7c208007)
Tunnel State: Up
Rx Path Info:
Source VTEP IP IIF NH IP
-------------- -------------- --------------
3.3.3.3 Eth 0/47 15.1.1.200
4.4.4.4 Eth 0/47 15.1.1.200
```

```
12.12.12.12 Eth 0/47 15.1.1.200
Tx Path Info:
OIF NH IP
-------------- --------------
Eth 0/47 15.1.1.200
Group: 239.1.1.103
Active VLANs: 300
Active BDs:
Remote VTEP IPs: 3.3.3.3, 4.4.4.4, 12.12.12.12
Tunnel Id: 32773 (0x7c208005)
Tunnel State: Up
Rx Path Info:
Source VTEP IP IIF NH IP
-------------- -------------- --------------
3.3.3.3 Eth 0/47 15.1.1.200

4.4.4.4 Eth 0/47 15.1.1.200
12.12.12.12 Eth 0/47 15.1.1.200
Tx Path Info:
OIF NH IP
-------------- --------------
Eth 0/47 15.1.1.200
Group: 239.1.1.110
Active VLANs: 110
Active BDs:
Remote VTEP IPs: 3.3.3.3, 4.4.4.4, 12.12.12.12
Tunnel Id: 32774 (0x7c208006)
Tunnel State: Up
Rx Path Info:
Source VTEP IP IIF NH IP
-------------- -------------- --------------
3.3.3.3 Eth 0/47 15.1.1.200
4.4.4.4 Eth 0/47 15.1.1.200
12.12.12.12 Eth 0/47 15.1.1.200
Tx Path Info:
OIF NH IP
-------------- --------------
Eth 0/47 15.1.1.200
Group: 239.1.1.200
Active VLANs:
Active BDs: 1
Remote VTEP IPs: 3.3.3.3, 4.4.4.4, 12.12.12.12
Tunnel Id: 32776 (0x7c208008)
Tunnel State: Up
Rx Path Info:
Source VTEP IP IIF NH IP
-------------- -------------- --------------
3.3.3.3 Eth 0/47 15.1.1.200
4.4.4.4 Eth 0/47 15.1.1.200
12.12.12.12 Eth 0/47 15.1.1.200
Tx Path Info:
OIF NH IP
-------------- --------------
Eth 0/47 15.1.1.200
```

The following examples shows detailed output for one PIM MDT given by Group address.

```
SLX# show ip pim mdt group 239.1.1.1
Group: 239.1.1.1(default)
Active VLANs: 100-102
Active BDs:
Remote VTEP IPs: 3.3.3.3, 4.4.4.4, 12.12.12.12
Tunnel Id: 32775 (0x7c208007)
```

```
Tunnel State: Up

Rx Path Info:
Source VTEP IP     IIF         NH IP
--------------    ----------    --------------
3.3.3.3         Eth 0/47       15.1.1.200
4.4.4.4         Eth 0/47       15.1.1.200
12.12.12.12        Eth 0/47       15.1.1.200

Tx Path Info:
OIF          NH IP
----------    --------------
Eth 0/47       15.1.1.200
```

show ip pim neighbor

Displays information about PIM neighbors.

Syntax

show ip pim neighbor vrf{ **mgmt-vrf** | **default-vrf** |*vrf-name* }

show ip pim neighbor interface { **ethernet** *slot*/*port-id* | **ve** *vlan ID* }
[**vrf** *vrf-name*]

Parameters

vrf

Specifies a VRF.

mgmt-vrf

Specifies the management VRF.

default-vrf

Specifies the default-vrf.

vrf-name

Specifies a VRF name.

interface

Specifies an interface.

ethernet *slot*/*port*

Specifies a physical interface.

ve *vlan ID*

Specifies a VE interface.

Modes

Privileged EXEC mode

Output

The command displays the following information.

Output Field	Description
Port	The interface through which the device is connected to the neighbor.
Phyport	When there is a virtual interface, this is the physical port to which the neighbor is connected.
Neighbor	The IP interface of the PIM neighbor.
Holdtime sec	Indicates how many seconds the neighbor wants this device to hold the entry for this neighbor in memory. The neighbor sends the Hold Time in Hello packets: • If the device receives a new Hello packet before the Hold Time received in the previous packet expires, the device updates its table entry for the neighbor. • If the device does not receive a new Hello packet from the neighbor before the Hold time expires, the device assumes the neighbor is no longer available and removes the entry for the neighbor.
Age sec	The number of seconds since the device received the last hello message from the neighbor.
UpTime sec	The number of seconds the PIM neighbor has been up. This timer starts when the device receives the first Hello messages from the neighbor.
VRF	The VRF in which the interface is configured. This can be a VRF that the port was assigned to or the default VRF of the device.
Priority	The DR priority that is used in the DR election process. This can be a configured value or the default value of 1.

Examples

The following example shows information about PIM neighbors.

```
device(config)# show ip pim neighbor
--------+--------+---------------+--------+---+---------+---------+-----+-----------
+-----------+----
Port    |PhyPort |Neighbor       |Holdtime|T  |PropDelay|Override |Age  |UpTime
|VRF        |Prio
        |        |               |sec     |Bit|msec     |msec     |sec  |
|           |
--------+--------+---------------+--------+---+---------+---------+-----+-----------
+-----------+----
v2       e1/1     2.1.1.2         105      1   500       3000      0
00:44:10    default-vrf 1
v4       e1/2     4.1.1.2         105      1   500       3000      10
00:42:50    default-vrf 1
v5       e1/1     5.1.1.2         105      1   500       3000      0
00:44:00    default-vrf 1
v22      e1/1     22.1.1.1        105      1   500       3000      0
00:44:10    default-vrf 1
Total Number of Neighbors : 4
```

show ip pim rp-candidate

Displays candidate rendezvous point (RP) information.

Syntax

show ip pim rp-candidate [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Specifies a VRF.

Modes

Privileged EXEC mode

Usage Guidelines

When used without the vrf option, this command displays information for the default VRF.

Output

The basic **show ip pim rp-candidate** command displays the following information.

Output Field	Description
Candidate-RP-advertisement in	How time will pass before the BSR sends the next RP message. The time is displayed in "hh:mm:ss" format. **Note:** This field appears only if this device is a candidate RP.
RP	The IP address of the RP. **Note:** This field appears only if this device is a candidate RP.
group prefixes	The multicast groups for which the RP listed by the previous field is a candidate RP. **Note:** This field appears only if this device is a candidate RP.
Candidate-RP-advertisement period	How frequently the BSR sends candidate RP advertisement messages. **Note:** This field appears only if this device is a candidate RP.

Examples

The following example shows information for a candidate RP.

```
device# show ip pim rp-candidate
Next Candidate-RP-advertisement in 00:00:10
  RP: 207.95.7.1
    group prefixes:
    224.0.0.0 / 4
  Candidate-RP-advertisement period: 60
```

show ip pim rp-hash

Displays rendezvous-point (RP) information for a PIM Sparse group.

Syntax

show ip pim rp-hash rp-hash *A.B.C.D* [**vrf** *vrf-name*]

Parameters

A.B.C.D

Specifies the IP address of a PIM Sparse IP multicast group.

vrf *vrf-name*

Specifies a VRF.

Modes

Privileged EXEC mode

Output

The **show ip pim rp-hash** command displays the following information:

Output Field	Description
RP	Indicates the IP address of the RP for the specified PIM Sparse group.
Info source	Indicates the source of the RP information. It can be a static-RP configuration or learned via the bootstrap router. If RP information is learned from the boot strap, the BSR IP address is also displayed.

Examples

The following example shows RP information for a PIM Sparse group.

```
device# show ip pim rp-hash 239.255.162.1
  RP: 207.95.7.1, v2
    Info source: 207.95.7.1, via bootstrap
```

show ip pim rp-map

Displays rendezvous-point (RP)-to-group mapping information.

Syntax

show ip pim rp-map [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Displays information for the specified VRF instance.

Modes

Privileged EXEC mode

Output

The **show ip pim rp-map** command displays the following information:

Output Field	Description
Group address	Indicates the PIM Sparse multicast group address using the listed RP.
RP address	Indicates the IP address of the RP for the listed PIM Sparse group.

Examples

The following general example shows RP-to-group mapping.

```
device# show ip pim rp-map
Number of group-to-RP mappings: 6
Group address        RP address
------------------------------
1 239.255.163.1  99.99.99.5
2 239.255.163.2  99.99.99.5
3 239.255.163.3  99.99.99.5
4 239.255.162.1  99.99.99.5
5 239.255.162.2  43.43.43.1
6 239.255.162.3  99.99.99.5
```

show ip pim rp-set

Displays rendezvous-point (RP)-set list for the device elected as the bootstrap router (BSR).

Syntax

show ip pim rp-set [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Displays information for the specified VRF instance.

Modes

Privileged EXEC mode

Output

The basic **show ip pim rp-set** command displays the following information:

Output Field	Description
Number of group prefixes	The number of PIM Sparse group prefixes for which the RP is responsible.
Group prefix	Indicates the multicast groups for which the RP listed by the previous field is a candidate RP.
RPs expected or received	Indicates how many RPs were expected and received in the latest bootstrap message.
RP *num*	Indicates the RP number. If there are multiple RPs in the PIM Sparse domain, a line of information for each RP is listed, in ascending numerical order.
priority	The RP priority of the candidate RP. During the election process, the candidate RP with the highest priority is elected as the RP.
age	The age (in seconds) of this RP-set.
holdtime	Indicates the time in seconds for which this rp-set information is valid. If this rp-set information is not received from BSR within the holdtime period, the rp-set information is aged out and deleted.

Examples

The following example shows the RP set list for the device elected as BSR.

```
device# show ip pim rp-set
Static RP
---------
Static RP count: 2
```

```
1.51.51.4
1.51.51.5
Number of group prefixes Learnt from BSR: 1
Group prefix = 224.0.0.0/4      # RPs: 2
      RP 1: 1.51.51.1    priority=0    age=60    holdtime=150
      RP 2: 1.51.51.3    priority=0    age=30    holdtime=150
```

The following example shows the RP set list for devices that are not elected as BSR.

```
device# show ip pim rp-set
Static RP
---------
Static RP count: 2
1.51.51.4
1.51.51.5
Number of group prefixes Learnt from BSR: 1
Group prefix = 224.0.0.0/4      # RPs expected: 2
      # RPs received: 2
      RP 1: 1.51.51.1    priority=0    age=60    holdtime=150
      RP 2: 1.51.51.3    priority=0    age=30    holdtime=150
```

show ip pim rpf

Displays what PIM sees as the best reverse path to the source. While there may be multiple routes back to the source, the one displayed by this command is the one that PIM thinks is best.

Syntax

show ip pim rpf *A.B.C.D* [*A.B.C.D*] [**vrf** *vrf-name*]

Parameters

A.B.C.D

Specifies one or two source addresses for reverse-path forwarding (RPF) check.

vrf *vrf-name*

Displays information for the specified VRF instance.

Modes

Privileged EXEC mode

Examples

This example shows best reverse path to the specified source:

```
device# show ip pim vrf eng rpf 130.50.11.10
Source 130.50.11.10 directly connected on e1/1
```

show ip pim traffic

Displays IPv4 PIM traffic statistics.

Syntax

show ip pim traffic [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Specifies information for a VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

PIM control packet statistics for interfaces that are configured for standard PIM are listed first by the display.

Output

The **show ip pim traffic** command displays the following information:

Output Field	Description
Port	The port or virtual interface on which the PIM interface is configured.
HELLO	The number of PIM Hello messages sent or received on the interface.
JOIN-PRUNE	The number of Join or Prune messages sent or received on the interface. **Note:** Unlike PIM Dense, PIM Sparse uses the same messages for Joins and Prunes.
ASSERT	The number of Assert messages sent or received on the interface.
REGISTER GRAFT (DM)	The number of Register messages sent or received on the interface.
REGISTER STOP (SM)	The number of Register Stop messages sent or received on the interface.
BOOTSTRAP MSGS (SM)	The number of bootstrap messages sent or received on the interface.
CAND. RP ADV. (SM)	The total number of Candidate-RP-Advertisement messages sent or received on the interface.
Err	The total number of messages discarded, including a separate counter for those that failed the checksum comparison.

Examples

This example shows PIM join and prune traffic statistics for received and sent packets:

```
device# show ip pim traffic
Port      |HELLO  |JOIN  |PRUNE  |ASSERT |GRAFT/REGISTER |REGISTER-STOP |BSR-MSGS  |RPC-
MSGS
          |Rx     |Rx    |Rx     |Rx     |Rx             |Rx            |Rx        |
Rx
------------+---------+---------+---------+---------+---------+---------+---------
+---------+
Ve10         54       0       0       0        0           0
0          0
Lo 1         0        0       0       0        0           0
0          0

device# show ip pim traffic
Port        |HELLO |JOIN  |PRUNE |ASSERT |GRAFT/REGISTER |REGISTER-STOP
|BSR-MSGS |RPC-MSGS
             | Tx   |Tx    | Tx   |Tx     |Tx             |Tx
------------+---------+---------+---------+---------+---------+---------+---------
+---------+---
Ve10         29        0     0        0         0            0
0         0
Lo 1         28        0     0        0         0            0
0         0
```

show ip route

Displays IP route information for IPv4 interfaces.

Syntax

show ip route [**vrf** *vrf-name*]

show ip route *A.B.C.D* [**vrf** *vrf-name*]

show ip route *A.B.C.D/M* [**longer**] [**vrf** *vrf-name*]

show ip route all [**vrf** *vrf-name*]

show ip route bgp [**vrf** *vrf-name*]

show ip route brief [**vrf** *vrf-name*]

show ip route connected [**vrf** *vrf-name*]

show ip route import [*src-vrf-name*] [**vrf** *vrf-name*]

show ip route isis

show ip route nexthop [*nexthopID* [**ref-routes**]] [**vrf** *vrf-name*]

show ip route ospf [**vrf** *vrf-name*]

show ip route[**slot** *line-card-number*]

show ip route static [**vrf** *vrf-name*]

show ip route summary [**vrf** *vrf-name*]

show ip route system-summary

Parameters

vrf *vrf-name*

Specifies routes for a selected VRF instance.

A.B.C.D/M

Specifies the IPv4 address and optional mask.

longer

Specifies routes that match the specified prefix.

all

Specifies information for all configured IPv4 routes.

bgp

Specifies BGP route information.

brief

Specifies the display of summary route information.

vrf *vrf-name*

Specifies a VRF instance.

connected

Specifies directly connected routes, such as local Layer 3 interfaces.

import

Specifies imported IPv4 routes.
src-vrf-name

Specifies a VRF instance from which routes are leaked.

isis

Specifies routes learned from the Intermediate System to Intermediate System (IS-IS) protocol.

nexthop

Specifies the configured next hop.
nexthopID

Valid values range from 0 through 4294967294.

ref-routes

Specifies all routes that point to the specified *next-hop ID* .

ospf

Specifies routes learned from the Open Shortest Path First (OSPF) protocol.

slot *line-card-number*

Specifies routes with the provided line card number.

static

Specifies configured static routes.

summary

Specifies summary information for all routes.

system-summary

Specifies a system-level routing summary.

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

If leaked subnet routes are present, that information displays in the output.

To view the status of management routes, use the **show ip route vrf** command and enter **mgmt-vrf** as follows. You must enter the name of the management VRF manually. Example output is shown below.

```
device# show ip route vrf mgmt-vrf
IP Routing Table for VRF "mgmt-vrf"
Total number of IP routes: 3
'*' denotes best ucast next-hop
'[x/y]' denotes [preference/metric]
```

```
0.0.0.0/0
    *via 10.25.96.1, mgmt 1, [1/1], 8d15h, static, tag 0
10.25.96.0/22, attached
    *via DIRECT, mgmt 1, [0/0], 8d15h, direct, tag 0
10.25.96.38/32, attached
    *via DIRECT, mgmt 1, [0/0], 8d15h, local, tag 0
```

Examples

The following example displays output for the **system-summary** option.

```
device# show ip route system-summary
System Route Count: 3 Max routes: 4096 (Route limit not exceeded)
System Nexthop Count: 2 Max nexthops: 1024 (Nexthop limit not exceeded)

VRF-Name: default-vrf
  Route count: 0 Max routes: Not Set (Route limit not exceeded)
  0 connected, 0 static, 0 RIP, 0 OSPF, 0 BGP, 0 ISIS, 0 unnumbered

VRF-Name: mgmt-vrf
  Route count: 3 Max routes: Not Set (Route limit not exceeded)
  1 connected, 1 static, 0 RIP, 0 OSPF, 0 BGP, 0 ISIS, 0 unnumbered
```

The following example displays output for the connected option.

```
device# show ip route connected
 Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
        Destination        Gateway         Port        Cost          Type Uptime
1       1.1.1.0/24         DIRECT          Te 2/1      0/0           D    4m33s
2       1.1.2.0/24         DIRECT          Te 2/2      0/0           D    2m42s
```

The following example displays output for the summary option.

```
device# show ip route summary
IP Routing Table - 7 entries:
  8 direct, 0 static, 0 RIP, 0 OSPF, 8 BGP, 0 ISIS, 80 EVPN Host
  Number of prefixes:
  /24: 7
Nexthop Table Entry - 4 entries
```

The following example displays output for the nexthop option.

```
device# show ip route nexthop
 Total number of IP nexthop entries: 4; Forwarding Use: 4
       NextHopIp        Port             RefCount      ID          Age
1      1.1.1.2          Te 2/1           3/3           2147549184 277
2      0.0.0.0          Te 2/2           1/1           2147484008 191
3      0.0.0.0          Te 2/1           2/2           2147484009 302
4      1.1.1.2          Te 2/1           1/1           2147549185 190
       1.1.2.2          Te 2/2
```

The following example displays output for a specific next-hop ID option.

```
device# show ip route nexthop 2147549184
       NextHopIp        Port             RefCount      ID          Age
1      1.1.1.2          Te 2/1           3/3           2147549184 288
```

The following example displays output for the ref-routes option.

```
device# show ip route nexthop 2147549184 ref-routes
Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
        Destination        Gateway         Port        Cost          Type Uptime
1       100.1.1.0/24       1.1.1.2         Te 2/1      1/1           S    5m10s
2       100.1.2.0/24       1.1.1.2         Te 2/1      1/1           S    4m54s
3       100.1.3.0/24       1.1.1.2         Te 2/1      1
```

The following example displays output for a specific IP address.

```
device# show ip route 100.1.1.1
Type Codes - B:BGP D:Connected I:ISIS O:OSPF R:RIP S:Static; Cost - Dist/Metric
BGP  Codes - i:iBGP e:eBGP
ISIS Codes - L1:Level-1 L2:Level-2
OSPF Codes - i:Inter Area 1:External Type 1 2:External Type 2 s:Sham Link
        Destination        Gateway         Port        Cost          Type Uptime
4       100.1.1.0/24       1.1.1.2         Te 2/1      1/1           S    5m37s
```

The following example displays output for the longer option.

```
device# show ip route 100.0.0.0/8 longer
1       100.1.1.0/24       1.1.1.2         Te 2/1      1/1           S    14m37s
2       100.1.2.0/24       1.1.1.2         Te 2/1      1/1           S    14m21s
3       100.1.3.0/24       1.1.1.2         Te 2/1      1/1           S    14m18s
4       100.2.1.0/24       DIRECT          Te 2/1      1/1           S    14m2s
5       100.3.1.0/24       1.1.1.2         Te 2/1      1/1           S    13m10s
        100.3.1.0/24       1.1.2.2         Te 2/2      1/1           S    13m10s
```

show ip source guard binding entries

Displays the IP Source Guard entries that are programmed a specified interface or displays all entries in the system.

Syntax

show ip source guard binding entries { **interface** *interface-num* | **all** }

Parameters

interface *interface-num*

Specifies the interface for which you want to display IP Source Guard binding entries.

all

Specifies that you want to display all IP Source Guard binding entries.

Modes

Privileged EXEC mode

show ip subnet-rate-limit stats

Displays IPv4 and IPv6 subnet trap statistics.

Syntax

show ip subnet-rate-limit stats

Modes

Control plane configuration mode

Examples

The following example shows packets per second and bytes per second for IPv4 and IPv6 subnet traps.

```
device# configure terminal
device(config)# control-plane
device(config-control-plane)# show ip subnet-rate-limit stats

IPv4/v6 Subnet Trap Statistics

Type              Packets/second - Rx             Bytes/second - Rx
======            ====================            ==================
IPv4              412                             210944
IPv6              120                             61440
```

show ipv6 bgp

Displays BGP4+ route information.

Syntax

show ipv6 bgp

show ipv6 bgp *ipv6-addr* [*/prefix*]

show ipv6 bgp *ipv6-addr* [*/prefix*] [**longer-prefixes**] [**vrf** *vrf-name*]

Parameters

ipv6-addr

IPv6 address of a neighbor in dotted-decimal notation, with optional mask.

/prefix

IPv6 mask length in CIDR notation.

longer-prefixes

Filters on prefixes equal to or greater than that specified by *prefix*.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example displays sample output from the **show ipv6 bgp** command.

```
device# show ipv6 bgp
Total number of BGP Routes: 1
Status codes: s suppressed, d damped, h history, * valid, > best, i internal, S stale, x
best-external
Origin codes: i - IGP, e - EGP, ? - incomplete RPKI State: V - VALID, I - INVALID, N -
NOT FOUND ? - Unknown Network Next Hop MED LocPrf Weight
RPKI State Path *>x 2000:2000::2000/128 5555::2 0 100 0 N (4200000002) 4200000004 i

Network                Next Hop       MED       LocPrf   Weight   RPKI     State Path
*>x 2000:2000::2000/128  5555::2     0          100        0      N          (4200000002)
4200000004 i
```

show ipv6 bgp attribute-entries

Displays BGP4+ route-attribute entries that are stored in device memory.

Syntax

show ipv6 bgp attribute-entries [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

The route-attribute entries table lists the sets of BGP4+ attributes that are stored in device memory. Each set of attributes is unique and can be associated with one or more routes. In fact, the device typically has fewer attribute entries than routes. Use this command to view BGP4+ route-attribute entries that are stored in device memory.

Examples

This example show sample output for the **show ipv6 bgp attribute-entries** command.

```
device# show ipv6 bgp attribute-entries

        Total number of BGP Attribute Entries: 1
1       Next Hop  : ::                                          MED      :0
Origin:INCOMP
        Originator:0.0.0.0            Cluster List:None
        Aggregator:AS Number :0            Router-ID:0.0.0.0          Atomic:None
        Local Pref:100               Communities:Internet
        AS Path   : (length 0)
           AsPathLen: 0  AsNum: 0, SegmentNum: 0, Neighboring As: 0, Source As 0
        Address: 0x0b456c4c  Hash:876 (0x03000000)
        Links: 0x00000000, 0x00000000
        Reference Counts: 1:0:1, Magic: 2
```

show ipv6 bgp dampened-paths

Displays all BGP4+ dampened routes.

Syntax

show ipv6 bgp dampened-paths [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example shows sample output from the **show ipv6 bgp dampened-paths** command.

```
device# show ipv6 bgp dampened-paths

    Status Code  >:best d:damped h:history *:valid
    Network                                       From
Flaps Since       Reuse       Path
*d  110:110:110:4::/64                            160:160:160::10
36    0 :2 :54    0 :10:10    111
*d  110:110:110:3::/64                            160:160:160::10
36    0 :2 :54    0 :10:10    111
*d  110:110:110:2::/64                            160:160:160::10
36    0 :2 :54    0 :10:10    111
*d  110:110:110:1::/64                            160:160:160::10
36    0 :2 :54    0 :10:10    111
*d  110:110:110::/64                              160:160:160::10
36    0 :2 :54    0 :10:10    111
```

show ipv6 bgp filtered-routes

Displays BGP4+ filtered routes that are received from a neighbor or peer group.

Syntax

show ipv6 bgp filtered-routes [**detail**] [*ipv6-addr* { **/** *mask* } [**longer-prefixes**]] | **as-path-access-list** *name* | **prefix-list** *name*] [**vrf** *vrf-name*]

Parameters

detail

Optionally displays detailed route information.

ipv6-addr

IPv6 address of the destination network in dotted-decimal notation.

mask

IPv6 mask of the destination network in CIDR notation.

longer-prefixes

Specifies all statistics for routes that match the specified route, or that have a longer prefix than the specified route.

as-path-access-list *name*

Specifies an AS-path ACL. The name must be between 1 and 32 ASCII characters in length.

prefix-list *name*

Specifies an IP prefix list. The name must be between 1 and 32 ASCII characters in length.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example displays BGP4+ filtered routes.

```
device# show ipv6 bgp filtered-routes
```

show ipv6 bgp flap-statistics

Displays BGP4+ route-dampening statistics for all dampened routes with a variety of options.

Syntax

show ipv6 bgp flap-statistics

show ipv6 bgp flap-statistics *ipv6-addr* { **/** *mask* } [**longer-prefixes** [**vrf** *vrf-name*] | **vrf** *vrf-name*]

show ipv6 bgp flap-statistics neighbor *ipv6-addr* [**vrf** *vrf-name*]

show ipv6 bgp flap-statistics regular-expression *name* [**vrf** *vrf-name*]

show ipv6 bgp flap-statistics vrf *vrf-name*

Parameters

ipv6-addr

IPv6 address of a specified route in dotted-decimal notation.

mask

IPv6 mask of a specified route in CIDR notation.

longer-prefixes

Displays statistics for routes that match the specified route or have a longer prefix than the specified route.

vrf *vrf-name*

Specifies a VRF instance.

neighbor

Displays flap statistics only for routes learned from the specified neighbor.
ip-addr

IPv6 address of the neighbor.

regular-expression

Specifies a regular expression in the display output on which to filter.

name

Name of an AS-path filter or regular expression.

Modes

Privileged EXEC mode

Examples

This example displays flap statistics for a neighbor.

```
device# show ipv6 bgp flap-statistics neighbor 2001:
```

show ipv6 bgp neighbors

Displays configuration information and statistics for IPv6 and IPv4 BGP4+ neighbors of the device.

Syntax

show ipv6 bgp neighbors [*ipv6-addr* | *ipv4-addr*]

show ipv6 bgp neighbors last-packet-with-error [**vrf** *vrf-name* | all-vrfs]

show ipv6 bgp neighbors routes-summary [**vrf** *vrf-name*]

show ipv6 bgp neighbors [**vrf** *vrf-name* | **all-vrfs**]

Parameters

ipv6-addr

IPv6 address of a neighbor, in dotted-decimal notation, to display statistics for.

ipv4-addr

IPv4 address of a neighbor, in dotted-decimal notation, to display statistics for.

last-packet-with-error

Displays the last packet recieved with an error.

route-summary

Displays routes received, routes accepted, number of routes advertised by peer, and other details.

vrf *vrf-name*

Specifies the VRF instance for which to display statistics for.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to view configuration information and statistics for BGP4+ neighbors of the device. Output shows all configured parameters for the neighbors. Only the parameters whose values differ from defaults are shown.

Examples

This example shows typical output from the command.

```
device# show ipv6 bgp neighbors

        Total number of BGP Neighbors: 1
    '+': Data in InQueue '>': Data in OutQueue '-': Clearing
    '*': Update Policy 'c': Group change 'p': Group change Pending
```

```
    'r': Restarting 's': Stale '^': Up before Restart '<': EOR waiting

1   IP Address: 2000::1, AS: 200 (EBGP), RouterID: 20.0.0.1, VRF: default-vrf
    State: ESTABLISHED, Time: 2h21m47s, KeepAliveTime: 60, HoldTime: 180
       KeepAliveTimer Expire in 49 seconds, HoldTimer Expire in 143 seconds
    Minimal Route Advertisement Interval: 0 seconds
       PeerGroup: pg
           DYNAMIC neighbor belongs to the subnet range group:
           2000::/64
       Multihop-EBGP: yes, ttl: 1
       UpdateSource(IPV6): Address 11:11::2
       RefreshCapability: Received
    Address Family : VPNV4 Unicast
       SendExtendedCommunity: yes
    Address Family : VPNV6 Unicast
       SendExtendedCommunity: yes
    Address Family : L2VPN EVPN
       SendCommunity: yes
       SendExtendedCommunity: yes
    Address Family : IPV4 Flowspec
       SendExtendedCommunity: yes
    Messages:    Open        Update      KeepAlive   Notification   Refresh-Req
       Sent    : 1           0           165         0              0
       Received: 1           0           163         0              0
    Last Update Time: NLRI              Withdraw               NLRI
Withdraw
                  Tx: ---               ---                 Rx: ---                 ---
                      Last Connection Reset Reason:Unknown
    Notification Sent:     Unspecified
    Notification Received: Unspecified
    Neighbor NLRI Negotiation:
      Peer Negotiated VPNv4 unicast  capability
      Peer Negotiated VPNv6 unicast  capability
      Peer Negotiated L2VPN EVPN address family
      Peer Negotiated IPV6 unicast  capability
      Peer configured for VPNv4 unicast  Routes
      Peer configured for VPNv6 unicast  Routes
      Peer configured for L2VPN EVPN address family
      Peer configured for IPV6 unicast  Routes
    Neighbor ipv6 MPLS Label Capability Negotiation:
    Neighbor AS4 Capability Negotiation:
    Outbound Policy Group:
       ID: 4, Use Count: 1
    BFD:Disabled
       Byte Sent:   3204, Received: 3166
       Local host:  2000::2, Local  Port: 179
       Remote host: 2000::1, Remote Port: 8047
    Maintenance Mode : Disabled
    G-Shut: Disabled
       Remote host: 98.0.0.1, Remote Port: 179
```

show ipv6 bgp neighbors advertised-routes

Displays the routes that the device has advertised to the neighbor during the current BGP4+ session.

Syntax

show ipv6 bgp neighbors [*ipv6-addr* | *ipv4-addr*] **advertised-routes** [*ipv6-addr* **/** *mask-bits*]

show ipv6 bgp neighbors [*ipv6-addr* | *ipv4-addr*] [**detail**] [*ipv6-addr* **/** *mask-bits*] [**vrf** *vrf-name*]

show ipv6 bgp neighbors [*ipv6-addr* | *ipv4-addr*] **vrf** *vrf-name*

Parameters

ipv6-addr

IPv6 address of the neighbor in dotted-decimal notation.

ipv4-addr

IPv4 address of the neighbor in dotted-decimal notation.

detail

Displays details of advertised routes.

ipv6-addr/ mask-bits

The IPv6 address range and the number of mask bits in CIDR notation of the network to which routes are advertised for.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example displays the details of advertised routes.

```
device# show ipv6 bgp neighbors 123::3 advertised-routes

       There are 5 routes advertised to neighbor 123::3
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
       Prefix             Next Hop        MED        LocPrf     Weight Status
1      110:110:110::/64   123::2           0                     0      BE
         AS_PATH: 222 111
2      110:110:110:1::/64 123::2           0                     0      BE
         AS_PATH: 222 111
3      110:110:110:2::/64 123::2           0                     0      BE
         AS_PATH: 222 111
4      110:110:110:3::/64 123::2           0                     0      BE
         AS_PATH: 222 111
```

```
5      110:110:110:4::/64 123::2           0                    0      BE
         AS_PATH: 222 111
```

This example shows ipv6 bgp neighbors 150.1.1.2 advertised routes

```
SLX# show ipv6 bgp neighbors 150.1.1.2 advertised routes
There are 4 routes advertised to neighbor 150.1.1.2
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL x:BEST-EXTERNAL
RPKI State: V - VALID, I - INVALID, N - NOT FOUND ? - Unknown
       Prefix         Next Hop         MED         LocPrf Weight       RPKI State
Status
1        1::1/128      ::ffff:150.1.1.1               0     100 32768   N BL AS_PATH:
2        2::2/128      ::ffff:150.1.1.1               0     100 32768   N BL AS_PATH:
3        3::3/128      ::ffff:150.1.1.1               0     100 32768   N BL AS_PATH:
4        4001::/64     ::ffff:150.1.1.1               0     100 32768   N BL AS_PATH:
           S5#
```

show ipv6 bgp neighbors flap-statistics

Displays the route flap statistics for routes received from or sent to a BGP4+ neighbor.

Syntax

show ipv6 bgp neighbors [*ipv6-addr* | *ipv4-addr*] **flap-statistics** [**vrf** *vrf-name*]

Parameters

ipv6-addr

IPv6 address of the neighbor, in dotted-decimal notation, to displays the route flap statistics for.

ipv4-addr

IPv4 address of the neighbor, in dotted-decimal notation, to displays the route flap statistics for.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

This example shows IPv6 route flap statistics for routes.

```
SLX# show ipv6 bgp neighbors 2000:db8::01:01 flap-statistics
Total number of flapping routes: 0
```

show ipv6 bgp neighbors last-packet-with-error

Displays information about the last packet that contained an error from any of a device's neighbors.

Syntax

show ipv6 bgp neighbors [*ipv6-addr* | *ipv4-addr*] **last-packet-with-error** [**decode**] [**vrf** *vrf-name*]

Parameters

ipv6-addr

IPv6 address of a neighbor in dotted-decimal notation.

ipv4-addr

IPv4 address of a neighbor in dotted-decimal notation.

decode

Decodes last packet that contained an error from any of a device's neighbors.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example shows sample output from the **show ipv6 bgp neighbors last-packet-with-error** command when no packet from a specified neighbor contained an error.

```
device# show ipv6 bgp neighbors 123::3 last-packet-with-error

 Received Message Length: 45
 BGP Message:
  0xffffffff  0xffffffff  0xffffffff  0xffffffff  0x002d0104
  0x014b00b4  0x09090909  0x10020601  0x04020000  0x01020202
  0x00020280  0x00

 BGP Header
  Marker:   0xffffffff  0xffffffff  0xffffffff  0xffffffff
  Message Length: (0x002d) 45
  Message Type: (0x01) OPEN

 OPEN Message
 Version: (0x04) 4
 AS Number: (0x014b) 331
 Hold Time: (0x00b4) 180
 BGP Identifier: (0x09090909) 9.9.9.9
 Optional Parameter length: (0x10) 16

 OPEN message optional parameters
```

```
 Parameter Type: (0x02) Capability
 Parameter Length: (0x06) 6
  Capability Type: (0x01) MULTIPROTOCOL EXTENSIONS
  Capability Length: (0x04) 4
  AFI: (0x0200) Unknown(512)
  Reserved: (0x00) 0
  SAFI: (0x01) Unicast

 Parameter Type: (0x02) Capability
 Parameter Length: (0x02) 2
  Capability Type: (0x02) ROUTE REFRESH(new)
  Capability Length: (0x00) 0

 Parameter Type: (0x02) Capability
 Parameter Length: (0x02) 2
  Capability Type: (0x80) ROUTE REFRESH(old)
  Capability Length: (0x00) 0
```

show ipv6 bgp neighbors received

Displays Outbound Route Filters (ORFs) received from BGP4+ neighbors of the device.

Syntax

show ipv6 bgp neighbors [*ipv6-addr* | *ipv4-addr*] **received**

show ipv6 bgp neighbors [*ipv6-addr* | *ipv4-addr*] **received detail** [**vrf** *vrf-name*]

show ipv6 bgp neighbors [*ipv6-addr* | *ipv4-addr*] **received prefix-filter** [**vrf** *vrf-name*]

show ipv6 bgp neighbors [*ipv6-addr* | *ipv4-addr*] **received vrf** *vrf-name*]

Parameters

ipv6-addr

IPv6 address of a neighbor in dotted-decimal notation.

ipv4-addr

IPv4 address of a neighbor in dotted-decimal notation.

detail

Displays detailed information for ORFs received from BGP4+ neighbors of the device.

vrf *vrf-name*

Specifies a VRF instance.

prefix-filter

Displays the results for ORFs that are prefix-based.

Modes

Privileged EXEC mode

Examples

The following example shows sample output from the **show ipv6 bgp neighbors received** command when the prefix-filter keyword is used.

```
device# show ipv6 bgp neighbors 2001:db8:93e8:cc00::1 received prefix-filter
```

show ipv6 bgp neighbors received-routes

Lists all route information received in route updates from BGP4+ neighbors of the device since the soft-reconfiguration feature was enabled.

Syntax

show ipv6 bgp neighbors [*ipv6-addr* | *ipv4-addr*] **received-routes** [**detail**] [**vrf** *vrf-name*]

Parameters

ipv6-addr

IPv4 address of a neighbor in dotted-decimal notation.

detail

Displays detailed route information.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example displays the received routes from the BGP neighbor 160:160:160::10.

```
device# show ipv6 bgp neighbors 160:160:160::10 received-routes

       There are 5 received routes from neighbor 160:160:160::10
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix             Next Hop        MED        LocPrf     Weight Status
1      110:110:110::/64   160:160:160::10  0         100        0      BE
         AS_PATH: 111
2      110:110:110:1::/64 160:160:160::10  0         100        0      BE
         AS_PATH: 111
3      110:110:110:2::/64 160:160:160::10  0         100        0      BE
         AS_PATH: 111
4      110:110:110:3::/64 160:160:160::10  0         100        0      BE
         AS_PATH: 111
5      110:110:110:4::/64 160:160:160::10  0         100        0      BE
         AS_PATH: 111
```

show ipv6 bgp neighbors rib-out-routes

Displays information about BGP4+ outbound RIB routes.

Syntax

show ipv6 bgp neighbors [*ipv6-addr* | *ipv4-addr*] **rib-out-routes** [*ipv6-addr / mask*] [**vrf** *vrf-name*]

show ipv6 bgp neighbors [*ipv6-addr* | *ipv4-addr*] **rib-out-routes detail** [*ipv6-addr / mask*] [**vrf** *vrf-name*]

show ipv6 bgp neighbors [*ipv6-addr* | *ipv4-addr*] **rib-out-routes detail** [**vrf** *vrf-name*]

show ipv6 bgp neighbors [*ipv6-addr* | *ipv4-addr*] **rib-out-routes** [**vrf** *vrf-name*]

Parameters

ipv6-addr

IPv6 address of a neighbor in dotted-decimal notation.

ipv4-addr

IPv4 address of a neighbor in dotted-decimal notation.

vrf *vrf-name*

Specifies a VRF instance.

detail

Displays detailed RIB route information. Detail information for RIB routes can be fetched for a specific range of IPv6 addresses and for specific VRFs.

Modes

Privileged EXEC mode

Examples

This example shows sample output from the **show ipv6 bgp neighbors rib-out-routes** command.

```
device# show ipv6 bgp neighbors 123::3 rib-out-routes

       There are 5 RIB_out routes for neighbor 123::3
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST E:EBGP I:IBGP L:LOCAL
       Prefix             Next Hop        MED        LocPrf     Weight Status
1      110:110:110::/64   160:160:160::10  0         100        0      BE
         AS_PATH: 111
2      110:110:110:1::/64 160:160:160::10  0         100        0      BE
         AS_PATH: 111
3      110:110:110:2::/64 160:160:160::10  0         100        0      BE
         AS_PATH: 111
4      110:110:110:3::/64 160:160:160::10  0         100        0      BE
```

```
          AS_PATH: 111
5       110:110:110:4::/64 160:160:160::10  0         100        0      BE
          AS_PATH: 111
```

show ipv6 bgp neighbors routes

Lists a variety of route information received in UPDATE messages from BGP4+ neighbors.

Syntax

show ipv6 bgp neighbors [*ipv6-addr* | *ipv4-addr*] **routes** [**vrf** *vrf-name*]

show ipv6 bgp neighbors [*ipv6-addr* | *ipv4-addr*] **routes** [**best** | **not-installed-best** | **unreachable** [**vrf** *vrf-name*]]

show ipv6 bgp neighbors [*ipv6-addr* | *ipv4-addr*] **routes detail** [**best** | **not-installed-best** | **unreachable** [**vrf** *vrf-name*]]

show ipv6 bgp neighbors [*ipv6-addr* | *ipv4-addr*] **routes detail** [**vrf** *vrf-name*]

Parameters

ipv6-addr

IPv6 address of a neighbor in dotted-decimal notation.

ipv4-addr

IPv4 address of a neighbor in dotted-decimal notation.

best

Displays routes received from the neighbor that are the best BGP4+ routes to their destination.

not-installed-best

Displays routes received from the neighbor that are the best BGP4+ routes to their destination but were not installed in the route table because the device received better routes from other sources.

unreachable

Displays routes that are unreachable because the device does not have a valid OSPF or static route to the next hop.

vrf *vrf-name*

Specifies a VRF instance.

detail

Displays detailed information for the specified route types.

Modes

Privileged EXEC mode

Examples

This example shows sample output from the **show ipv6 bgp neighbors routes** command when the best keyword is used.

```
device# show ipv6 bgp neighbor 2001:db8::106 routes best
```

show ipv6 bgp neighbors routes-summary

Lists all route information received in UPDATE messages from BGP4+ neighbors.

Syntax

show ipv6 bgp neighbors [*ipv6-addr* | *ipv4-addr*] **routes-summary** [**vrf** *vrf-name*]

Parameters

ipv6-addr

IPv6 address of a specified route in dotted-decimal notation.

ipv4-addr

IPv4 address of a specified route in dotted-decimal notation.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Output

The **show ipv6 bgp neighbors routes-summary** command displays the following information.

Output field	Description
IP Address	The IPv6 address of the neighbor
Routes Received	How many routes the device has received from the neighbor during the current BGP4+ session: • Accepted or Installed - Indicates how many of the received routes the device accepted and installed in the BGP4+ route table. • Filtered or Kept - Indicates how many routes were filtered out, but were nonetheless retained in memory for use by the soft reconfiguration feature. • Filtered - Indicates how many of the received routes were filtered out.
Routes Selected as BEST Routes	The number of routes that the device selected as the best routes to their destinations.
BEST Routes not Installed in IPv6 Forwarding Table	The number of routes received from the neighbor that are the best BGP4+ routes to their destinations, but were nonetheless not installed in the IPv6 route table because the device received better routes from other sources (such as OSPFv3, or static IPv6 routes).

Output field	Description
Unreachable Routes	The number of routes received from the neighbor that are unreachable because the device does not have a valid OSPFv3, or static IPv6 route to the next hop.
History Routes	The number of routes that are down but are being retained for route flap dampening purposes.
NLRIs Received in Update Message	The number of routes received in Network Layer Reachability (NLRI) format in UPDATE messages: • Withdraws - The number of withdrawn routes the device has received. • Replacements - The number of replacement routes the device has received.
NLRIs Discarded due to	Indicates the number of times the device discarded an NLRI for the neighbor due to the following reasons: • Maximum Prefix Limit - The device's configured maximum prefix amount had been reached. • AS Loop - An AS loop occurred. An AS loop occurs when the BGP4+ AS-path attribute contains the local AS number. • Invalid Nexthop Address - The next hop value was not acceptable. • Duplicated Originator_ID - The originator ID was the same as the local router ID. • Cluster_ID - The cluster list contained the local cluster ID, or contained the local router ID (see above) if the cluster ID is not configured.
Routes Advertised	The number of routes the device has advertised to this neighbor: • To be Sent - The number of routes the device has queued to send to this neighbor. • To be Withdrawn - The number of NLRIs for withdrawing routes the device has queued up to send to this neighbor in UPDATE messages.

Output field	Description
NLRIs Sent in Update Message	The number of NLRIs for new routes the device has sent to this neighbor in UPDATE messages: • Withdraws - The number of routes the device has sent to the neighbor to withdraw. • Replacements - The number of routes the device has sent to the neighbor to replace routes the neighbor already has.
Peer Out of Memory Count for	Statistics for the times the device has run out of BGP4+ memory for the neighbor during the current BGP4+ session: • Receiving Update Messages - The number of times UPDATE messages were discarded because there was no memory for attribute entries. • Accepting Routes(NLRI) - The number of NLRIs discarded because there was no memory for NLRI entries. This count is not included in the Receiving Update Messages count. • Attributes - The number of times there was no memory for BGP4+ attribute entries. • Outbound Routes (RIB-out) - The number of times there was no memory to place a "best" route into the neighbor's route information base (Adj-RIB-Out) for routes to be advertised. • Outbound Routes Holder - For debugging purposes only.

Examples

This example shows sample output from the **show ipv6 bgp neighbors routes-summary** command.

```
SLX# show ipv6 bgp neighbors routes-summary
    Total number of BGP Neighbors: 2
1   IP Address: 3001::2
Routes Accepted/Installed:2,  Filtered/Kept:0,  Filtered:0
   Routes Selected as BEST Routes:0
      BEST Routes not Installed in IP Forwarding Table:0
   Unreachable Routes (no IGP Route for NEXTHOP):0
   History Routes:0

NLRIs Received in Update Message:2,  Withdraws:0 (0),  Replacements:0
   NLRIs Discarded due to
      Maximum Prefix Limit:0, AS Loop:0
      Maximum Add-paths per Prefix per Peer Limit:0
      Invalid Nexthop:0, Invalid Nexthop Address:0.0.0.0
      Invalid Confed aspath:0, maxas-limit aspath:0
      Duplicated Originator_ID:0, Cluster_ID:0

Routes Advertised:2,  To be Sent:0,  To be Withdrawn:0
NLRIs Sent in Update Message:2,  Withdraws:0,  Replacements:0

Peer Out of Memory Count for:
   Receiving Update Messages:0, Accepting Routes(NLRI):0
   Attributes:0, Outbound Routes(RIB-out):0 Outbound Routes Holder:0

2   IP Address: 4001::2
Routes Accepted/Installed:2,  Filtered/Kept:0,  Filtered:0
   Routes Selected as BEST Routes:0
      BEST Routes not Installed in IP Forwarding Table:0
   Unreachable Routes (no IGP Route for NEXTHOP):0
```

```
   History Routes:0

NLRIs Received in Update Message:2,  Withdraws:0 (0),  Replacements:0
   NLRIs Discarded due to
      Maximum Prefix Limit:0, AS Loop:0
      Maximum Add-paths per Prefix per Peer Limit:0
      Invalid Nexthop:0, Invalid Nexthop Address:0.0.0.0
      Invalid Confed aspath:0, maxas-limit aspath:0
      Duplicated Originator_ID:0, Cluster_ID:0

Routes Advertised:2,  To be Sent:0,  To be Withdrawn:0
NLRIs Sent in Update Message:2,  Withdraws:0,  Replacements:0

Peer Out of Memory Count for:
   Receiving Update Messages:0, Accepting Routes(NLRI):0
   Attributes:0, Outbound Routes(RIB-out):0 Outbound Routes Holder:0
```

show ipv6 bgp peer-group

Displays peer-group information.

Syntax

show ipv6 bgp peer-group *peer-group-name* [**vrf** *vrf-name*]

Parameters

peer-group-name

Specifies a peer group name.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

Only the parameters that have values different from their defaults are listed.

Examples

This example shows sample output from the **show ipv6 bgp peer-group** command.

```
device# show ipv6 bgp peer-group

1   BGP peer-group is pg
      Address family : IPV4 Unicast
        activate
      Address family : IPV6 Unicast
        no activate
    Members:
       IP Address: 1.1.1.1, AS: 100
       IP Address: 1::1, AS: 100

2   BGP peer-group is pg6
      Address family : IPV4 Unicast
        activate
      Address family : IPV6 Unicast
        no activate
    Currently there are no members.
```

show ipv6 bgp routes

Displays BGP4+ route information that is filtered by the table entry at which the display starts.

Syntax

show ipv6 bgp routes [*num* | *ipv6-address/prefix* | **age** *num* | **as-path-access-list** *name* | **best** | **cidr-only** | **community-access-list** *name* | **community-reg-expression** *expression* | **detail** | **local** | **neighbor** *ipv6-addr* | **nexthop** *ipv6-addr* | **no-best** | **not-installed-best** | **prefix-list** *string* | **regular-expression** *name* | **route-map** *name* | **summary** | **unreachable**] [**vrf** *vrf-name*]

Parameters

num

Table entry at which the display starts.

ipv6-address/prefix

Table entry at which the display starts.

age

Displays BGP4+ route information that is filtered by age.

as-path-access-list *name*

Displays BGP4+ route information that is filtered by autonomous system (AS)-path access control list (ACL). The name must be between 1 and 32 ASCII characters in length.

best

Displays BGP4+ route information that the device selected as best routes.

cidr-only

Displays BGP4+ routes whose network masks do not match their class network length.

community-access-list *name*

Displays BGP4+ route information for an AS-path community access list. The name must be between 1 and 32 ASCII characters in length.

community-reg-expression *expression*

Displays BGP4+ route information for an ordered community-list regular expression.

detail

Displays BGP4+ detailed route information.

local

Displays BGP4+ route information about selected local routes.

neighbor *ip-addr*

Displays BGP4+ route information about selected BGP neighbors.

nexthop *ip-addr*

Displays BGP4+ route information about routes that are received from the specified next hop.

no-best

Displays BGP4+ route information that the device selected as not best routes.

not-installed-best

Displays BGP4+ route information about best routes that are not installed.

prefix-list *string*

Displays BGP4+ route information that is filtered by prefix list. The string must be between 1 and 32 ASCII characters in length.

regular-expression *name*

Displays BGP4+ route information about routes that are associated with the specified regular expression.

route-map *name*

Displays BGP4+ route information about routes that use the specified route map.

summary

Displays BGP4+ summary route information.

unreachable

Displays BGP4+ route information about routes whose destinations are unreachable through any of the BGP4+ paths in the BGP4+ route table.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example shows sample input from the **show ipv6 bgp routes** command.

```
device# show ipv6 bgp routes

Total number of BGP Routes: 1
Status A:AGGREGATE B:BEST b:NOT-INSTALLED-BEST C:CONFED_EBGP D:DAMPED
       E:EBGP H:HISTORY I:IBGP L:LOCAL M:MULTIPATH m:NOT-INSTALLED-MULTIPATH
       S:SUPPRESSED F:FILTERED s:STALE
       Prefix             Next Hop        MED        LocPrf     Weight Status
1      107:1:1::/64       ::              0          100        32768  BL
         AS_PATH:
```

This example shows sample input from the **show ip bgp routes** command when the **summary** keyword is used.

```
device# show ipv6 bgp routes summary

  Total number of BGP routes (NLRIs) Installed     : 1
```

```
  Distinct BGP destination networks                : 1
  Filtered bgp routes for soft reconfig            : 0
  Routes originated by this router                 : 1
  Routes selected as BEST routes                   : 1
  Routes Installed as BEST routes                  : 1
  BEST routes not installed in IP forwarding table : 0
  Unreachable routes (no IGP route for NEXTHOP)    : 0
  IBGP routes selected as best routes              : 0
  EBGP routes selected as best routes              : 0
  BEST routes not valid for IP forwarding table    : 0
```

show ipv6 bgp routes community

Displays BGP4+ route information that is filtered by community and other options.

Syntax

show ipv6 bgp routes community { *num* | **internet** | **local-as** | **no-advertise** | **no-export** } [**vrf** *vrf-name*]

Parameters

community

Displays routes filtered by a variety of communities.

num

Specific community member.

internet

Displays routes for the Internet community.

local-as

Displays routes for a local sub-AS within the confederation.

no-advertise

Displays routes with this community that cannot be advertised to any other BGP4+ devices at all.

no-export

Displays routes for the community of sub-ASs within a confederation.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example shows output from the **show ipv6 bgp routes community** command when the **internet** keyword is used.

```
device# show ipv6 bgp routes community internet
```

show ipv6 bgp routes large-community

Displays information for all BGP4+ routes with large-community attributes matching the specified value.

Syntax

show ipv6 bgp routes [**detail**] **large-community** *ADMIN:OPER1:OPER2* [**vrf** *vrf-name*]

Modes

Privileged EXEC mode

Parameters

detail

Optionally displays detailed information for all BGP4+ routes with large-community attributes matching the specified value. If you omit this keyword, brief information is displayed.

ADMIN

A four-octet namespace identifier for a BGP Large-Communities Global Administrator.

OPER1

A four-octet operator-defined value for BGP Large-Communities Local Data Part 1.

OPER2

A four-octet operator-defined value for BGP Large-Communities Local Data Part 2.

vrf *vrf-name*

Specifies a VRF instance.

Examples

The following is an example command.

```
device# show ipv6 bgp routes large-community 1:2:3
```

show ipv6 bgp routes large-community access-list

Displays information for all BGP4+ routes matching the large community access list.

Syntax

show ipv6 bgp routes [**detail**] **large-community access-list**
large_community_ACL [**vrf** *vrf-name*]

Modes

Privileged EXEC mode

Parameters

detail

Optionally displays detailed information for all BGP4+ routes matching the specified large community access list. If you omit this keyword, brief information is displayed.

large_community_ACL

Name of the large community defined in a standard or extended large community access list

vrf *vrf-name*

Specifies a VRF instance.

Examples

The following example displays brief information of all BGP4+ routes with large community attributes that match the large community access-list, lcstdacl1.

```
device# show ipv6 bgp routes large-community access-list lcstdacl1
```

show ipv6 bgp routes large-community reg-expression

Displays information for all BGP4+ routes with large-community attributes matching the specified regular expression (REGEX).

Syntax

show ipv6 bgp routes [**detail**] **large-community reg-expression** *regex_value*

Modes

Privileged EXEC mode

Parameters

detail

Optionally displays detailed information for all BGP4+ routes with large-community attributes matching the specified REGEX. If you omit this keyword, brief information is displayed.

regex_value

REGEX value.

Examples

The following example displays the BGP4+ routes that match the specified REGEX value.

```
device# show ipv6 bgp routes large-community reg-expression _456778*
```

show ipv6 bgp summary

Displays BGP information such as the local autonomous system number (ASN), maximum number of routes supported, and some BGP4+ statistics.

Syntax

show ipv6 bgp summary [**vrf** *vrf-name*]

Parameters

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

This example displays summary BGP4+ information.

```
device# show ipv6 bgp summary

  BGP4 Summary
  Router ID: 10.10.10.10   Local AS Number: 2040
  Confederation Identifier: not configured
  Confederation Peers:
  Maximum Number of IP ECMP Paths Supported for Load Sharing: 1
  Number of Neighbors Configured: 1040, UP: 4
  Number of Routes Installed: 3079574, Uses 483493118 bytes
  Number of Routes Advertising to All Neighbors: 107925658 (17078048 entries), Uses
1297931648 bytes
  Number of Attribute Entries Installed: 1296243, Uses 230731254 bytes
  '+': Data in InQueue '>': Data in OutQueue '-': Clearing
  '*': Update Policy 'c': Group change 'p': Group change Pending
  'r': Restarting 's': Stale '^': Up before Restart '<': EOR waiting
  '$': Learning-Phase (for Delayed Route Calculation)
  '#': RIB-in Phase
  Neighbor Address  AS#         State     Time     Rt:Accepted Filtered Sent     ToSend
  1:2::3            100         CONN      0h 0m18s    0        0        0        1
```

The $: Learning-Phase (for Delayed Route Calculation) notation denotes that the BGP peer with this notation is learning bulk route updates. More than one peer can be in Learning-Phase. BGP BEST-Path selection is delayed until all the peers complete Learning-Phase. A peer can be in Learning-Phase only if BGP delayed route calculation feature is enabled and in specific scenarios described in the **init-route-calc-delay** command.

The # : RIB-IN phase notation denotes that a peer is learning bulk route updates. When one or more peer is in RIB-IN phase, BGP provides high preference for learning incoming route-updates and less preference for advertising routes (to outbound peers). An incoming route-update can possibly cause a BGP BEST-path change and

eventually re-compute RIB-OUT for outbound peers. Slowing down RIB-OUT until all peers complete learning route updates will improve BGP performance. This feature is enabled by default and does not require additional configuration. Unlike BGP delayed route calculation, BGP BEST-Path selection is not delayed in this Phase.

This example displays summary information about dynamically created BGP neighbors.

```
Neighbor Address  AS#         State     Time     Rt:Accepted Filtered Sent     ToSend
 *2000:1:1:1::2     100         ESTAB   0h4m28s       0        0        0        0
 *fe80::629c:9fff:fede:f46
                    100         ESTAB   0h4m28s       0        0        0        0
```

The following is the output of the IPv6 BGP Summary command.

```
SLX# show ipv6 bgp summary

  BGP4 Summary
  Router ID: 172.31.254.35   Local AS Number: 4200000000
  Confederation Identifier: not configured
  Confederation Peers:
  Maximum Number of IP ECMP Paths Supported for Load Sharing: 1
  Number of Neighbors Configured: 0, UP: 0
  Number of Routes Installed: 0
  Number of Routes Advertising to All Neighbors: 0 (0 entries)
  Number of Attribute Entries Installed: 0
  d: Dynamically created based on a listen range command
  Dynamically created neighbors: 0/100(max)
  A: Auto Discovered Neighbors using LLDP
  Auto Neighbors Count: 0
  '+': Data in InQueue '>': Data in OutQueue '-': Clearing
  '*': Update Policy 'c': Group change 'p': Group change Pending
  'r': Restarting 's': Stale '^': Up before Restart '<': EOR waiting
  '$': Learning-Phase (for Delayed Route Calculation)
  '#': RIB-in Phase
  'D': Dampening enabled
  Neighbor Address    AS#            State        Time        Rt:Accepted    Filtered
Sent    ToSend
  11:11::2            100            ESTAB        1h43m33s    2            0
2        0
```

show ipv6 counters interface

Displays ipv6 statistics for an interface.

Syntax

show ipv6 counters interface [**ethernet** *slot/plot* | **loopback** *loopback-number* | **port-channel** *number* | **ve** *ve-number*]

Parameters

interface

Specifies an interface.

ethernet *slot/plot*

Specifies physical Ethernet interface and a valid slot and port on it.

loopback *loopback-number*

Specifies the loopback interface.

port-channel *number*

Specifies a port-channel.

ve *ve-number*

Specifies the virtual Ethernet (ve) number.

Modes

Privileged EXEC mode

Examples

The following is an example of the **show ipv6 counters interface** command output.

```
device# show ipv6 counters interface ethernet 1/1

 Interface Ethernet 1/1 IPv6 statistics (ifindex 406896641)
```

show ipv6 dhcp relay address interface

Displays IPv6 DHCP Relay addresses configured on supported interfaces.

Syntax

show ipv6 dhcp relay address interface [**ethernet** *slot/port* | **ve** *interface number*]

Parameters

ethernet

Specifies the ethernet interface.

slot

Specifies a valid slot number. For devices that do not support line cards, specify **0**.

port

Specifies a valid port number.

ve

Specifies the Ve interface.

interface number

Specifies the Ve interface number.

Modes

Privileged EXEC mode

Examples

The following example displays IPv6 DHCP relay addresses configured per interface.

```
device# show ipv6 dhcp relay address interface ethernet 3/21

Interface               Relay Address                          VRF Name
Outgoing Interface
---------               -------------                          -------------
-----------------------
Eth 3/21                4001::101                              default-vrf
Eth 3/21                fe80::8
blue                         Ve 100
```

show ipv6 dhcp relay delegated-prefixes

Displays the DHCPv6 delegated prefixes for a specific vrf.

Syntax

```
show ipv6 dhcp relay delegated-prefixes [ {all-vrfs}|{[ vrf vrf-
   name ] [ ipv6-prefix | client-id client-ipv6-ip-address | interface
   { ethernet slot/port | ve ve-id | po po-id } ] } ]
```

Parameters

all-vrfs

Specifies all VRFs.

vrf *vrf-name*

Specifies a VRF.

ipv6-prefix

Specifies the IPv6 prefix in this format: X:X::X:X/M

client-id *client-ip-address*

Displays the IPv6 prefixes for this specific client.

interface { **ethernet** *slot/port* | **ve** *ve-id* | **po** *po-id* }

Configures the interface for which to display the Prefix Delegation information.

ethernet *slot/port*

Configures the ethernet slot/port for displaying Prefix Delegation information.

ve *ve-id*

Configures the VE for displaying Prefix Delegation information.

po *po-id*

Configures the port-channel interface for displaying Prefix Delegation information.

Modes

Privileged EXEC mode

Usage Guidelines

None.

Examples

The following example shows how to display the DHCPv6 delegated prefixes for specific VRF.

```
SLX-Router#show ipv6 dhcp relay delegated-prefixes
Delegated Prefixes Table - 2 entries VRF: default-vrf
IPv6 Prefix           Client              Interface     Expire Time
1122:abb::/48         101:10:1::1         Eth 1/2        3h24m10s
1265:abc::/48         101:10:1::5         Eth 1/2        0m28s
SLX-Router#
SLX-Router#show ipv6 dhcp relay delegated-prefixes vrf red
IPv6 DHCP Relay Delegated Prefixes Table - 2 entries VRF: red
IPv6 Prefix          Client               Interface        Expire Time
1329:aaa::/48        103:10:1::8          Eth 1/3        3h24m10s
1fe:bbb::/48         104:10:1::6          Eth 1/4        0m28s
```

show ipv6 dhcp relay prefix-delegation-information

Displays the DHCPv6 Relay prefix delegation information for all interfaces where DHCPv6 Relay is enabled.

Syntax

show ipv6 dhcp relay prefix-delegation-information

Parameters

prefix-delegation-information

Displays the DHCPv6 Relay prefix delegation information for those interfaces where DHCPv6 Relay is enabled.

Modes

Privileged EXEC Mode

Output

The command displays the following information:

Output field	Description
Interface	The name of the interface where DHCPv6 Relay is enabled.
Current	The configured value for DHCPv6 Relay prefix delegation.
Maximum	The maximum configurable prefix delegation entries.
Admin Distance	The administrative distance for this network.

Examples

The following example shows the output for the command.

```
 SLX#show ipv6 dhcp relay prefix-delegation-information
DHCPv6 Relay Prefix Delegation Notification Information:
Interface   Current     Maximum     Admin Distance
ve 100      20          20000       10
ve 101      4000        20000       10
ve 102      0           20000       10
ve 103      0           20000       10
ve 104      0           20000       10
```

show ipv6 dhcp relay statistics

Displays statistics for DHCPv6 packets and DHCPv6 PD packets counts.

Syntax

show ipv6 dhcp relay statistics

Modes

Privileged EXEC mode

Usage Guidelines

The **show ipv6 dhcp relay statistics** command displays the following information about the IP DHCP Relay function for IP DHCP Relay addresses configured on the device:

- Number of DHCP Error packets dropped.
- Number of DHCP SOLICIT, REQUEST, CONFIRM, RENEW, REBIND, RELEASE, DECLINE, INFORMATION-REQUEST, RELAY-FORWARD, RELAY-REPLY packets received.
- Number of DHCP RELAY-FORWARD, REPLY packets sent.

Examples

The following example displays statistics for the device.

```
device# show ipv6 dhcp relay statistics

DHCPv6 Relay Statistics:
------------------------
Packets dropped : 0
    Error : 0
Packets received : 112144
    SOLICIT : 20020
    REQUEST : 20052
    CONFIRM : 0
    RENEW : 0
    REBIND : 0
    RELEASE : 16000
    DECLINE : 0
    INFORMATION-REQUEST : 0
    RELAY-FORWARD : 0
    RELAY-REPLY : 56072
    PD-SOLICIT : 1
    PD-REQUEST : 1
    PD-CONFIRM : 0
    PD-RENEW : 0
    PD-REBIND : 0
    PD-RELEASE : 1
    PD-DECLINE : 0
    PD-INFORMATION-REQUEST : 0
    PD-RELAY-FORWARD : 0
    PD-RELAY-REPLY : 1
Packets sent : 112144
```

```
    RELAY-FORWARD : 56072
    REPLY : 56072
    PD-RELAY-FORWARD : 2
    PD-REPLY : 2
```

show ipv6 interface

Displays details of IPv6 interfaces.

Syntax

show ipv6 interface [**brief** | **ethernet** *slot/port* | **loopback** *loopback-port-number* | **port-channel** *number* | **ve** *ve_id*]

Parameters

brief

Displays brief interface information.

ethernet

Specifies Ethernet interface.

slot

Specifies a valid slot number. For devices that do not support line cards, specify **0**.

port

Specifies a valid port number.

loopback *loopback-port-number*

Specifies the loopback interface. The range is from 1 to 255.

port-channel *number*

Specifies a port-channel.

ve *ve-id*

Specifies the VE ID of a virtual Ethernet (VE) interface. The range is from 1 to 4096.

Modes

Privileged EXEC mode

Interface configuration mode

Examples

The following example displays the output of the **show ipv6 interface** command with an Ethernet interface specified.

```
device# show ipv6 interface ethernet 2/25
 Ethernet 2/25 is up protocol is up
 IPv6 Address: 2025:2525:aaaa::1/64  Primary  Confirmed
 IPv6 Address: 2500:ffee:1234::12/64  Secondary  Confirmed
 IPv6 Address: 2500:ffee:1234::14/64  Secondary  Confirmed
 IPv6 Address: 2500:ffee:1234::16/64  Secondary  Confirmed
 IPv6 Address: fe80::748e:f8ff:fe09:e10d/128  Link-local  Confirmed
 IPv6 multicast groups locally joined:
    ff02::1
    ff02::2    ff02::1:ff00:1    ff02::1:ff00:12
    ff02::1:ff00:14    ff02::1:ff00:16    ff02::1:ff09:e10d
```

```
IPv6 MTU: 1500
Vrf : default-vrf
```

show ipv6 mld groups

Displays information about learned groups for a specified bridge domain, interface, VLAN, MCT (Multi-Chassis Trunking) cluster, or CCEP (Cluster Client Edge Port) client.

Syntax

show ipv6 mld groups detail[*ipv6 address* [**bridge-domain** *bd id* |**interface** [**ethernet** | **port-channel**] *interface name* | **vlan** *vlan id* |**cluster** *cluster id* |**client** *client id*]

Parameters

detail

Displays the MLD v2 INCLUDE,EXCLUDE source list for the group.

ipv6 address

Specifies the address for which to show group information

bridge-domain

Specifies the bridge domain for which to show group information.
bd id

Specifies the ID of the bridge domain.

interface

Specifies the interface for which to show group information.
ethernet *interface name*

Specifies the Ethernet name.

port channel *interface name*

Specifies the port channel name.

vlan

Specifies the VLAN for which to show group information.
vlan id

Specifies the ID of the VLAN.

cluster

Specifies the MCT cluster for which to show group information.
cluster id

Specifies the ID of the cluster.

client

Specifies the CCEP client for which to show group information.
client id

Specifies the ID of the client.

Modes

Privileged EXEC mode

Examples

The following example shows typical output for a VLAN.

```
device# show ipv6 mld groups vlan 100
Total number of groups: 1
MLD Connected Group Membership
Group Address          Interface        Uptime        Expires     Last Reporter
ff28::1                Vlan 100         00:02:03       Never      Static
Member Port: Eth 0/1
```

The following example shows typical output for a bridge domain.

```
device# show ipv6 mld groups bridge-domain 10
Total number of groups: 1
MLD Connected Group Membership
Group Address          Interface        Uptime        Expires     Last Reporter
ff38::2                bridgedomain10   00:00:34      Never      Static
Member Port: Eth 0/2.200
```

show ipv6 mld snooping

Displays snooping information for the specified VLAN or bridge domain.

Syntax

show ipv6 mld snooping [**vlan** *vlan id* | **bridge-domain** *bd id*]

Parameters

vlan

Specifies the VLAN for which to see snooping information.
vlan id

Specifies the ID of the VLAN.

bridge-domain

Specifies the bridge domain for which to see snooping information.
bd id

Specifies the ID of the bridge domain.

Modes

Privileged EXEC mode

Examples

The following example shows typical output for a bridge domain.

```
device# show ipv6 mld snooping bridge-domain 10
Bridge-domain ID: 10
 Multicast Router ports: Eth 0/44.200
 Querier - disabled
 MLD Operation mode: MLDv2
 Is Fast-Leave Enabled : Disabled Max Response time = 10
 Last Member Query Interval = 10 Query interval = 125
 Number of Multicast Groups: 0
 Group: ff28::1
 Member Ports: Eth 0/44.200
```

show ipv6 mld snooping mrouter

Displays multicast (mrouter) port-related information for the specified VLAN or bridge domain.

Syntax

show ipv6 mld snooping mrouter [**vlan** *vlan id* | **bridge-domain** *bd id*]

Parameters

vlan

Specifies the VLAN for which to see mrouter information.
vlan id

Specifies the ID of the VLAN.

bridge-domain

Specifies the bridge domain for which to see mrouter information.
bd id

Specifies the ID of the bridge domain.

Modes

Privileged EXEC mode

Examples

The following example shows typical mrouter information for a VLAN.

```
device# show ipv6 mld snooping mrouter vlan 100
Vlan          Interface       Expires (Sec)
100           Eth 0/1         Never
```

The following example shows typical mrouter information for a bridge domain.

```
device# show ipv6 mld snooping mrouter bridge-domain 10
BD            Interface           Expires (Sec)
100           Eth 0/2.200         298
```

show ipv6 mld statistics

Displays MLD packet statistics for the specified VLAN, interface, or bridge domain.

Syntax

show ipv6 mld statistics [**bridge-domain** *bd id* | **interface** [**ethernet** | **port-channel**] *interface name* |**vlan** *vlan id*]

Parameters

bridge-domain

Specifies the bridge domain for which you want to see statistics.
bd id

Specifies the ID of the bridge domain.

interface

Specifies the interface for which you want to see statistics.
ethernet *interface name*

Specifies the Ethernet name.

port-channel *interface name*

Specifies the port channel name.

vlan

Specifies the VLAN for which you want to see statistics.
vlan id

Specifies the ID of the VLAN.

Modes

Privileged EXEC mode

Examples

The following example shows typical output for a bridge domain.

```
device# show ipv6 mld statistics bridge-domain 100
MLD packet statistics for Bridge-Domain 100:
MLD Message Type         Edge-Received     Edge-Sent    Edge-Rx-Errors
General Query            1                      0                 0
Group Specific Query     0                      0                 0
V1 Membership Report     0                      1                 0
V2 Membership Report     0                      0                 0
Group Leave              0                      0                 0
```

The following example shows typical output for a VLAN.

```
device# show ipv6 mld statistics vlan 12
MLD packet statistics for vlan 12:
MLD Message Type         Edge-Received     Edge-Sent     Edge-Rx-Errors
General Query            0                        0                  0
Group Specific Query     0                        0                  0
```

```
V1 Membership Report     0                    0                    0
V2 Membership Report     0                    0                    0
Group Leave              0                    0                    0
PIM Hello           0               0             0
```

show ipv6 multicast snooping

Shows the status of MLD snooping and IPv6 PIM snooping on a VLAN or bridge domain.

Syntax

show ipv6 multicast snooping [**vlan**| **bridge-domain**] *id*

Parameters

vlan

Specifies the VLAN for which you want to show snooping status.

bridge-domain

Specifies the bridge domain for which you want to show snooping status.

id

Specifies the ID of the VLAN or bridge domain.

Modes

Privileged EXEC mode

Examples

The following example shows the snooping status for a VLAN.

```
device# show ipv6 multicast snooping vlan 10
Vlan id            : 10
MLD  snooping      : Enabled
IPv6 PIM  snooping : Enabled
MLD  Version       : MLDv1
```

show ipv6 multicast snooping mcache

Displays the IPv6 multicast forwarding cache for a VLAN or a bridge domain.

Syntax

show ipv6 multicast snooping mcache [**vlan**| **bridge-domain**] *id*

Parameters

vlan

Specifies the VLAN for which you want to show the forwarding cache.

bridge-domain

Specifies the bridge domain for which you want to show the forwarding cache.

id

Specifies the ID of the VLAN or bridge domain.

Modes

Privileged EXEC mode

Examples

The following example shows the forwarding cache for a VLAN.

```
show ipv6 multicast snooping mcache vlan 100
Flags : V1|V2 : MLD Receiver, P_G : PIM (*,G) Join, P_SG: PIM (S,G) Join
                BR : PIM Blocked RPT
 Vlan ID : 100
 -------------
1     (*, ff04:3000:4000::2 )  00:21:48    NumOIF: 1
        Outgoing Ports:
                eth0/14        Flags: 0x84 ( V1)  00:21:48/202s
2     (*, ff08:1001:2001::1 )  00:27:09    NumOIF: 1
        Outgoing Ports:
                eth0/14        Flags: 0x84 ( V1)  00:27:09/131s
3     (*, ff0e:1000:2000::1 )  00:27:09    NumOIF: 1
        Outgoing Ports:
                eth0/14        Flags: 0x84 ( V1)  00:27:09/131s
```

show ipv6 nd

Displays the router advertisement information.

Syntax

show ipv6 nd interface [**ethernet** *slot/plot* | **prefix** | **ve** *ve-number* | **vrf** *vrf-name*]

Parameters

interface

Specifies an interface.

ethernet *slot/plot*

Specifies physical Ethernet interface and a valid slot and port on it.

prefix

Displays prefix information.

ve *ve-number*

Specifies the virtual Ethernet (ve) number.

vrf *vrf-name*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following is an example of the **show ipv6 nd** command output.

```
device# show ipv6 nd interface ethenet 3/5
ICMPv6 ND Interfaces for VRF  default-vrf
  IPv6 address:  2ffe::1
  Router-Advertisement active timers:
    Last Router-Advertisement sent: 00:01:25
    Next Router-Advertisement sent in: 00:07:06
  Router-Advertisement parameters:
    Periodic interval:  200 to 600 seconds
    Send 'Managed Address Configuration' flag: false
    Send 'Other Stateful Configuration' flag: false
    Send 'Current Hop Limit' field: 64
    Send 'MTU' option value: 1500
    Send 'Router Lifetime' field: 1800 secs
    Send 'Reachable Time' field: 0 ms
    Send 'Retrans Timer' field: 0 ms
    Suppress RA: false
    Suppress MTU in RA: false
    Suppress All RA: false
  Neighbor-Solicitation parameters:
    NS retransmit interval: 1 secs
    DAD Attempts: 2
```

```
   DAD expiry: 1 secs
Neighbor Cache Expiry: 14400 secs
```

show ipv6 nd suppression-cache

Displays IPv6 neighbor discovery (ND)-suppression information.

Syntax

show ipv6 nd suppression-cache [**summary**]

show ipv6 nd suppression-cache bridge-domain *bridge-domain-id*

show ipv6 nd suppression-cache vlan *vlan-id*

Parameters

summary

Specifies summary format.

bridge-domain *bridge-domain-id*

Specifies one or more bridge domain IDs. To specify a range of IDs, insert a hyphen between the beginning and ending integers (for example, 5-16). To specify individual IDs and ranges of IDs, separate them with commas (for example: 1,5-7,55). Do not insert spaces after commas. You can enter a maximum of 253 characters.

vlan *vlan-id*

Specifies one or more VLAN IDs. To specify a range of IDs, insert a hyphen between the beginning and ending integers (for example, 5-16). To specify individual IDs and ranges of IDs, separate them with commas (for example: 1,5-7,55). Do not insert spaces after commas. You can enter a maximum of 253 characters.

Modes

Privileged EXEC mode

Output

The **show ipv6 nd suppression-cache** command displays the following information:

Output field	Description
Vlan/Bd	Displays the VLAN (V) ID or bridge-domain (B) ID.
IP	Displays the IPv6 address.
Mac	Displays the MAC address.
Interface	Displays the interface type and ID. "Tu" represents a tunnel interface, followed by the end-point IP. "Nsh" indicates that the ARP is learned through MCT peer node, followed by the cluster peer interface.

Output field	Description
Age	In hh:mm:ss format, displays the time since the most recent renewal of a dynamic entry. For a static entry, displays "Never".
Flags	Displays "L" (locally learned adjacency), "R" (remote learned adjacency), or RS (remote static adjacency).

Examples

The following example displays the results of the basic form of this command.

```
device# show ipv6 nd suppression-cache
Flags: L  - Locally Learnt Adjacency
       R  - Remote Learnt Adjacency
       RS - Remote Static Adjacency
Number of Locally Learnt Adjacency: 0
Number of Remotely Learnt Adjacency: 810

Vlan/Bd IP                          Mac            Interface                   Age     Flags
-------------------------------------------------------------------------------------------
4006(V) fd80:113:114:1:4006::114  609c.9fb1.1401 Tu 61441 (114.114.114.114) Never    RS
4006(V) fd80:113:114:1:4006::1001 00ef.4006.3601 Eth 1/4                     00:00:17 L
4006(V) fd80:113:114:1:4006::1002 00ef.4006.3602 Eth 1/4                     00:00:17 L
4006(V) fe80::1                   00ef.4006.3601 Eth 1/4                     00:16:16 L
4006(V) fe80::2                   00ef.4006.3602 Eth 1/4                     00:16:16 L
4006(V) fe80::629c:9fff:feb1:1401 609c.9fb1.1401 Tu 61441 (114.114.114.114) Never    RS
4007(V) fd80:113:114:1:4007::1001 00ef.4007.4601 Tu 61441 (114.114.114.114) Never    R
4007(V) fd80:113:114:1:4007::1002 00ef.4007.4602 Tu 61441 (114.114.114.114) Never    R
0081(B) 20:102::8                 887e.25d3.180b Tu 32771 (1.89.0.2)         Never    RS
                                                 Tu 32775 (1.89.0.5)
0081(B) 20.102::2                 f463.95a1.0406 Po 31.1901                  Never    R
```

show ipv6 nd suppression-statistics

Displays IPv6 neighbor discovery (ND)-suppression statistics.

Syntax

show ipv6 nd suppression-statistics

show ipv6 nd suppression-statistics bridge-domain *bridge-domain-id*

show ipv6 nd suppression-statistics vlan *vlan-id*

Parameters

bridge-domain *bridge-domain-id*

Specifies one or more bridge domain IDs. To specify a range of IDs, insert a hyphen between the beginning and ending integers (for example, 5-16). To specify individual IDs and ranges of IDs, separate them with commas (for example: 1,5-7,55). Do not insert spaces after commas. You can enter a maximum of 253 characters.

vlan *vlan-id*

Specifies a VLAN interface.

Modes

Privileged EXEC mode

Output

The **show ipv6 nd suppression-statistics** command displays the following information:

Output field	Description
Vlan/Bd	Displays the VLAN (V) ID or bridge-domain (B) ID.
Forwarded	Displays the number of packets forwarded.
Suppressed	Displays the number of packets suppressed.
Remote-arp Proxy	Displays the number of packets for which the device has sent proxy-ARP replies.

Examples

The following example displays the results of the basic form of this command.

```
device# show ipv6 nd suppression-statistics
Vlan/Bd         Forwarded     Suppressed    Remote-arp Proxy
-------------------------------------------------------------
110 (V)         0             117           0
254 (V)         3             10            0
```

show ipv6 nd suppression-status

Displays the IPv6 neighbor discovery (ND)-suppression status.

Syntax

show ipv6 nd suppression-status

show ipv6 nd suppression-status bridge-domain *bridge-domain-id*

show ipv6 nd suppression-status vlan *vlan-id*

Parameters

bridge-domain *bridge-domain-id*

Specifies one or more bridge domain IDs. To specify a range of IDs, insert a hyphen between the beginning and ending integers (for example, 5-16). To specify individual IDs and ranges of IDs, separate them with commas (for example: 1,5-7,55). Do not insert spaces after commas. You can enter a maximum of 253 characters.

vlan *vlan-id*

Specifies one or more VLAN IDs. To specify a range of IDs, insert a hyphen between the beginning and ending integers (for example, 5-16). To specify individual IDs and ranges of IDs, separate them with commas (for example: 1,5-7,55). Do not insert spaces after commas. You can enter a maximum of 253 characters.

Modes

Privileged EXEC mode

Output

The **show ipv6 nd suppression-status** command displays the following information:

Output field	Description
Vlan/Bd	Displays the VLAN (V) ID or bridge-domain (B) ID.
Configuration	Displays "Enabled" or "Disabled".
Evpn-Register	Displays "Yes" if the VLAN is extended through EVPN or "No" if it is not extended.
Operation	Displays "Active" or "Inactive".

Examples

The following example displays the results of the basic form of this command.

```
device# show ipv6 nd suppression-status
Vlan/Bd          Configuration   Evpn-Register   Operation
```

```
------------------------------------------------------------
4003 (V)         Enabled         Yes             Active
4005 (V)         Disabled        No              Inactive
4006 (V)         Enabled         Yes             Active
4007 (V)         Enabled         Yes             Active
4090 (V)         Disabled        No              Inactive
```

show ipv6 neighbor

Displays the IPv6 neighbor discovery (ND) entries.

Syntax

show ipv6 neighbor

show ipv6 neighbor { **dynamic** | **static** } [**summary**] [**vrf** *vrf-name*]

show ipv6 neighbor ethernet *slot* **/** *port* [**vrf** *vrf-name*]

show ipv6 neighbor { *ipv6-address* | **ve** *vlan_id* | **summary** } [**vrf** *vrf-name*]

show ipv6 neighbor vrf *vrf-name*

Parameters

ipv6-address

Restricts the display to the entries for the specified IPv6 address. Specify this parameter in hexadecimal using 16-bit values between colons as documented in RFC 2373.

ethernet *slot/port*

Restricts the display to the entries for the specified Ethernet interface.

static

Displays the static IPv6 neighbors.

Type

Displays the dynamic IPv6 neighbors .

summary

Displays the summary of IPv6 neighbors.

ve *ve-num*

Restricts the display to the entries for the specified VE interface. The range is from 1 to 4096.

vrf *vrf-name*

Displays the IPv6 neighbor information for the specified Virtual Routing/Forwarding (VRF) instance.

Modes

Privileged EXEC mode

Output

The **show ipv6 neighbor** command displays the following information:

Output field	Description
Address	Displays the IP address.
Mac-address	Displays the MAC address or "UnResolved".
L3 Interface	Displays the physical or VE interface.
L2 Interface	Displays the Layer 2 interface. Supported values: • (Physical interface): "Eth *slot* **/** *port*" • (Port-channel): "Po" • (VxLAN): "Tu" • "PW": VPLS Pseudo-wire • "UnResolved"
Vlan / BD	Displays the VLAN or the BD for the neighbor entry. VLANs are indicated with a (V) and BDs with (B)
Age	In hh:mm:ss format, displays the time since the most recent renewal of a dynamic entry. For a static entry, displays "Never".
Type	Displays the neighbor discovery (ND) type. Supported values: • "Dynamic" • "BGP-EVPN": Entries learned through the BGP-EVPN control plane • "BGP-Sticky": Entries learned through the BGP-EVPN control plane—with the "sticky" attribute (static or MY-IP at the originator). • "LeakNd": A neighbor entry leaked from another VRF. • "PreNd": ND triggered by other than the data traffic, for example, by the static route. • "Static"

Examples

The following example illustrates the output of the **show ipv6 neighbor** command without keywords.

```
device# show ipv6 neighbor
Total Entries in VRF default-vrf : 8000
Address                   Mac-address      L3 Intf    L2 Intf              Vlan/BD  Age       Type
-------------------------------------------------------------------------------------------------
100:1:2::1                887e.25d3.d10b   Ve 4002    Eth 0/50.2           2(B)     00:05:45  Dynamic
100:1:3::1                887e.25d3.d10b   Ve 4003    Eth 0/50.3           3(B)     00:06:18  Dynamic
100:1:4::1                887e.25d3.d10b   Ve 4004    Eth 0/50.4           4(B)     00:05:42  Dynamic
10:1:1:2::2               0010.9400.2eeb   Ve 2       Eth 0/37             2(V)     00:09:23  Dynamic
10:1:1:3::2               0010.9400.2eec   Ve 3       Eth 0/37             3(V)     00:09:23  Dynamic
10:1:1:4::2               0010.9400.2eed   Ve 4       Eth 0/37             4(V)     00:09:23  Dynamic
```

The following example displays the output of the **show ipv6 neighbor summary** option.

```
device# show ipv6 neighbor summary
Static Entries                  : 1
Dynamic Entries                 : 5
Leaked Entries                  : 2
Pre-arp Entries                 : 1
Remote(Mct/Evpn) Entries        : 0
Remote(Mct/Evpn) Sticky Entries : 28
Total Entries                   : 37
```

show ipv6 ospf

Displays a summary of the OSPFv3 configuration in the device.

Syntax

show ipv6 ospf [**vrf** *name*]

Parameters

vrf *name*

Specifies the name of the VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

Examples

The following example shows sample output from the command.

```
device# show ipv6 ospf
==========================================================================
OSPFv3 Global Information
==========================================================================

router-id                      : 127.158.208.0
admin-state                    : DISABLE
version                        : 3
area-bdr-rtr-state             : FALSE
as-bdr-rtr-state               : FALSE
as-scope-lsa-count             : 0
lsa-checksum                   : 0
originate-new-lsas             : 0
rx-new-lsas                    : 0
ext-lsa-count                  : 0
Helper mode                    : enabled
Graceful restart time       : Enabled with restart interval: 120,
```

show ipv6 ospf area

Displays the OSPFv3 area table in a specified format.

Syntax

show ipv6 ospf area [*A.B.C.D*] [*decimal*] [**vrf** *vrfname*]

Parameters

A.B.C.D

Area address in dotted decimal format.

decimal

Area address in decimal format. Valid values range from 0 to 2147483647.

vrf vrf *name*

Specifies a non-default VRF instance.

Modes

Privileged EXEC mode

Examples

The following example shows sample output from the **show ipv6 ospf area** command when no arguments or keywords are used.

```
device# show ipv6 ospf area
```

show ipv6 ospf database

Displays lists of information about different OSPFv3 link-state advertisements (LSAs).

Syntax

show ipv6 ospf database [**advrtr** *A.B.C.D* | **extensive** | **grace** | **link-id** *decimal* | **prefix** *ipv6-addr*] [**vrf** *vrfname*]

show ipv6 ospf database [**as-external** | **inter-prefix** | **inter-router** | **intra-prefix** | **link** [*decimal*] | **network** | **router** | **type-7**] [**advrtr** *A.B.C.D* | **link-id** *decimal*] [**vrf** *vrfname*]

show ipv6 ospf database scope { **area** { *A.B.C.D* | *decimal* } | **as** | **link** } [**vrf** *vrfname*]

show ipv6 ospf database summary [**all-vrfs** | **vrf** *vrfname*]

Parameters

advrtr *A.B.C.D*

Displays LSAs by Advertising Router Id in dotted decimal format.

extensive

Displays detailed lists of LSA information.

grace

Displays grace LSA information.

link-id *decimal*

Link-state ID that differentiates LSAs. Valid values range from 1 through 4294967295.

prefix

Display LSAs that contain a prefix.

ipv6-addr

Specifies an IPv6 address.

vrf vrf *name*

Specifies a non-default VRF instance.

as-external

Displays information about external LSAs.

inter-prefix

Displays information about inter area prefix LSAs.

inter-router

Displays information about inter area router LSAs.

intra-prefix

Displays information about intra area prefix LSAs.

link *decimal*

Displays information about the link LSAs.

network

Displays information about network LSAs.

router

Displays information about router LSAs.

type-7

Displays information about the not so stubby area (NSSA) external LSAs.

scope

Displays LSA information by LSA scope.

area

Displays LSAs by scope within a specified area.

as

Displays autonomous system (AS) LSAs by scope.

link

Displays link LSAs by scope.

summary

Displays LSA summary information.

all-vrfs

Specifies all VRFs.

Modes

Privileged EXEC mode

Examples

The following is sample output from the **show ipv6 ospf database as-external** command using the **link-id** keyword:

```
device# show ipv6 ospf database as-external link-id 5
```

The following is sample output from the **show ipv6 ospf database inter-prefix** command using the **link-id** keyword:

```
device# show ipv6 ospf database inter-prefix link-id 5
```

The following is sample output from the **show ipv6 ospf database network** command:

```
device# show ipv6 ospf database network
```

The following is sample output from the **show ipv6 ospf database router** command:

```
device# show ipv6 ospf database router
```

The following is sample output from the **show ipv6 ospf database type-7** command:

```
device# show ipv6 ospf database type-7
```

The following is sample output from the **show ipv6 ospf database scope** command using the **area** keyword:

```
device# show ipv6 ospf database scope area 0
```

show ipv6 ospf interface

Displays interface information for all or specific OSPFv3-enabled interfaces.

Syntax

show ipv6 ospf interface brief [**all-vrfs** | **vrf** *vrf-name*]

show ipv6 ospf interface [**ethernet** *slot/port* | **loopback** *number* | **port-channel** *number* | **ve** *vlan_id*]

show ipv6 ospf interface [**vrf** *vrf-name*]

Parameters

brief

Displays summary information.

all-vrfs

Displays the information for all VRF instances.

vrf *vrf-name*

Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

ethernet *slot/port*

Specifies an Ethernet slot and port.

loopback *number*

Specifies a loopback port number. Valid values range from 1 through 255.

port-channel *number*

Specifies a port-channel.

ve *vlan_id*

Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

Modes

Privileged EXEC mode

Usage Guidelines

Examples

The following is sample output from the **show ipv6 ospf interface** command when no arguments or keywords are used.

The following is sample output from the **show ipv6 ospf interface** command the **brief** keyword is used.

show ipv6 ospf memory

Displays information about OSPFv3 memory usage.

Syntax

show ipv6 ospf memory [**vrf** *vrfname*]

Parameters

vrf *vrfname*

Displays the information for the specified VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

Examples

The following is sample output from the **show ipv6 ospf memory vrf** *vrf-name* command:

```
device# show ipv6 ospf memory vrf vrf-1
   Total Dynamic Memory Allocated for this instance : 87046288 bytes
global shared memory pool for all instances
   Memory Type               Size       Allocated  Max-alloc  Alloc-Fails
   MTYPE_OSPF6_AREA          1100       1024       1065       0
   MTYPE_OSPF6_AREA_RANGE    52         0          16         0
   MTYPE_OSPF6_SUMMARY_ADDRE 36         0          16         0
   MTYPE_OSPF6_IF            396        2048       2625       0
   MTYPE_OSPF6_NEIGHBOR      24916      2048       2098       0
   MTYPE_OSPF6_ROUTE_NODE    36         71666      72415      0
   MTYPE_OSPF6_ROUTE_INFO    52         71666      80537      0
   MTYPE_OSPF6_PREFIX        24         0          16         0
   MTYPE_OSPF6_LSA           252        76787      133135     0
   MTYPE_OSPF6_VERTEX        196        5120       5327       0
   MTYPE_OSPF6_SPFTREE       60         1024       1056       0
   MTYPE_OSPF6_NEXTHOP       32         5134       8192       0
   MTYPE_OSPF6_EXTERNAL_INFO 52         0          1024       0
   MTYPE_THREAD              68         14703      15192      0
   MTYPE_OSPF6_LINK_LIST     44         6849444    7050698    0
   MTYPE_OSPF6_LINK_NODE     28         170996     265654     0
   MTYPE_OSPF6_LSA_RETRANSMI 20         0          25598      0
Global Memory Pool Usage for all instances : 415468328 bytes
global Heap memory for all instances
   Memory Type               Size       Allocated  Max-alloc  Alloc-Fails
   MTYPE_OSPF6_TOP           41104      1024       1024       0
   MTYPE_OSPF6_LSA_HDR       416        76787      107723     0
   MTYPE_OSPF6_RMAP_COMPILED 0          0          0          0
   MTYPE_OSPF6_OTHER         96         132591     137421     0
   MTYPE_THREAD_MASTER       200        1024       1024       0
---------------------
```

```
Packet Tx thread Info
---------------------
Queue Id[0]: Enqueued[291763] Dequeued [291763]
Queue Id[1]: Enqueued[13108] Dequeued [13108]
Send Failed Packets - 0
device#
```

show ipv6 ospf neighbor

Displays detailed or summary OSPFv3 neighbor information.

Syntax

show ipv6 ospf neighbor [**all-vrfs** | **vrf** *vrf-name*]

show ipv6 ospf neighbor detail [**vrf** *vrf-name*]

show ipv6 ospf neighbor interface [**ethernet** *slot/port* | **loopback** *number* | **port-channel** *number* | **ve** *vlan_id*]

show ipv6 ospf neighbor router-id *A.B.C.D* [**vrf** *vrf-name*]

Parameters

all-vrfs

Specifies all VRF instances.

vrf *vrf-name*

Specifies a non-default VRF instance.

detail

Displays detailed neighbor information.

interface

Displays OSPFv3 interface information.

ethernet *slot/port*

Specifies an Ethernet slot and port.

loopback *number*

Specifies a loopback port number. Valid values range from 1 through 255.

port-channel *number*

Specifies a port-channel.

ve *vlan_id*

Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

router-id *A.B.C.D*

Specifies neighbor information for the specified router ID (in dotted decimal format).

Modes

Privileged EXEC mode

Examples

The following example shows sample output from the **show ipv6 ospf neighbor** command when no arguments or keywords are used.

```
device# show ipv6 ospf neighbor
Total number of neighbors in all states: 1
Number of neighbors in state Full      : 1

RouterID        Pri State  DR              BDR             Interface     State   QCount
1.4.4.4         1 Full     100.5.5.5       1.4.4.4         Eth 1/13      DR      0
device#
```

The following example shows sample output from the **show ipv6 ospf neighbor detail** command when no arguments or keywords are used.

```
device# show ipv6 ospf neighbor detail
Total number of neighbors in all states: 1
Number of neighbors in state Full      : 1

RouterID        Pri State  DR              BDR             Interface     State   QCount
1.4.4.4         1 Full     100.5.5.5       1.4.4.4         Eth 1/13      DR      0
                Option: 00-00-00    Timer: 692
BFD State: NONE, BFD HoldoverInterval(sec):Configured: 0 Current: 0
device#
```

show ipv6 ospf redistribute route

Displays all IPv6 routes or a specified IPv6 route that the device has redistributed into OSPFv3.

Syntax

show ipv6 ospf redistribute route *A.B.C.D:M* [**vrf** *vrf-name*]

show ipv6 ospf redistribute route [**vrf** *vrf-name*]

Parameters

A.B.C.D:M

Specifies an IPv6 address.

vrf *vrfname*

Specifies the name of a VRF instance.

Modes

Privileged EXEC mode

Examples

The following is sample output from the **show ipv6 ospf redistribute route** command when no arguments or keywords are used:

```
device# show ipv6 ospf redistribute route
```

show ipv6 ospf routes

Displays OSPFv3 routes.

Syntax

show ipv6 ospf routes *A.B.C.D:M* [**vrf** *vrfname*]

show ipv6 ospf routes [**vrf** *vrfname*]

Parameters

A.B.C.D:M

Specifies a destination IPv6 address.

vrf *vrfname*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Examples

The following example displays OSPFv3-calculated routes.

```
device# show ipv6 ospf routes
```

show ipv6 ospf spf

Displays OSPFv3 SPF node, table, and tree information.

Syntax

show ipv6 ospf spf { **node** | **table** | **tree** } [**area** { *A.B.C.D* | *decimal* }] [**vrf** *vrfname*]

Parameters

node

Displays OSPFv3 node information.

table

Specifies a SPF table.

tree

Specifies a SPF tree.

area

Specifies an area.

A.B.C.D

Area address in dotted decimal format.

decimal

Area address in decimal format.

vrf *vrfname*

Specifies an non-default VRF instance.

Examples

The following example shows sample output from the **show ipv6 ospf spf** command when the **node** keyword is used.

```
device# show ipv6 ospf spf node
```

show ipv6 ospf summary

Displays summary information for all OSPFv3 instances.

Syntax

show ipv6 ospf summary [**all-vrfs** | **all-vrfs total** | **vrf** *vrfname*]

Parameters

all-vrfs

Specifies all VRF instances. If this option is not used, details for the default VRF are shown in the output.

vrf *vrfname*

Specifies a non-default VRF instance. If this option is not used, details for the default VRF are shown in the output.

all-vrfs total

Displays the cumulative summary of OSPF information with the total numbers for all of the VRF intances. If this option is not used, details for the default VRF are shown in the output. If this option is not used, details for the default VRF are shown in the output.

Modes

Privileged EXEC mode

Examples

The following example shows sample default VRF output from the **show ipv6 ospf summary** command when no arguments or keywords are used.

```
device# show ipv6 ospf summary
Seq Instance        Intfs   Nbrs    Nbrs-Full LSAs    Routes
1   default-vrf     0       0       0         0       0
```

The following example shows sample output from the **show ipv6 ospf summary all-vrfs total** command.

```
device# show ipv6 ospf summary all-vrfs total

----------------------------------------
         IPv6 OSPF Summary Total
----------------------------------------
Number of instances: 1024
Number of interfaces: 2048
Number of neighbors: 2048
Number of neighbors in FULL state: 2048
Number of LSAs: 76786
```

```
Number of Routes: 67570
device#
```

show ipv6 ospf virtual-links

Displays information about all OSPFv3 virtual links or specified links.

Syntax

show ipv6 ospf virtual-links brief [**vrf** *vrfname*]

show ipv6 ospf virtual-links [**vrf** *vrfname*]

Parameters

brief

Displays summary information.

vrf *vrfname*

Specifies a non-default VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

Examples

The following is sample output from the **show ipv6 ospf virtual-links** command when no arguments or keywords are used:

```
device# show ipv6 ospf virtual-links
```

show ipv6 ospf virtual-neighbor

Displays information about OSPFv3 virtual neighbors.

Syntax

show ipv6 ospf virtual-neighbor brief [**vrf** *vrfname*]

show ipv6 ospf virtual-neighbor [**vrf** *vrfname*]

Parameters

brief

Displays summary information.

vrf *vrfname*

Specifies a nondefault VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

Examples

The following example shows sample output from the **show ipv6 ospf virtual-neighbor** command when no arguments or keywords are used.

```
device# show ipv6 ospf virtual-neighbor
```

show ipv6 pim anycast-rp

Displays information about the Anycast rendezvous point (RP).

Syntax

show ipv6 pim anycast-rp

Modes

Privileged EXEC mode

Examples

The following example shows typical output for the command.

```
device# show ipv6 pim anycast-rp
Number of Anycast RP: 2
Anycast RP :2003:1::1
Prefix Name :AnyCastRPList-1
Peer Addresses :
2002:1:2::1
2002:1:5::1
2002:1:8::1
Anycast RP :2003:2::1
Prefix Name :AnyCastRPList-2
Peer Addresses :
2001:2:5:25::5
2001:2:8:28::8
2001:2:8:28::2
2001:5:8:58::5
2001:2:5:25::2
2001:5:8:58::8
```

show ipv6 pim bsr

Displays bootstrap router (BSR) information.

Syntax

show ipv6 pim bsr

Modes

Privileged EXEC mode

Usage Guidelines

This command displays BSR information, including whether the PIM router is the elected or candidate BSR. It also displays information about the candidate rendezvous point (RP).

Examples

The following example shows typical output for the command.

```
device# show ipv6 pim bsr
PIMv2 Bootstrap information :
------------------------------------------------------------------
  This system is the Elected BSR
  BSR address: 1234::5. Hash Mask Length 32. Priority 0.
  Next bootstrap message in 00:00:50
  Configuration:
    Candidate Lo 1 (Address 1234::5). Hash Mask Length 32. Priority 0.
Next Candidate-RP-advertisment in 00:00:50
  RP: 1234::5
    group prefixes:
    ff08:: / 16
    ff05:: / 16
  Candidate-RP-advertisement period: 60
```

show ipv6 pim group

Displays a list of PIM multicast groups.

Syntax

show ipv6 pim group

Modes

Privileged EXEC mode

Usage Guidelines

This command displays a list of PIM multicast groups and the local interface that is connected to the receivers of a group.

Examples

This example shows typical output for the command.

```
device# show ipv6 pim group
Total number of groups: 3
1    Group ff04:3000:4000::2
     Group member at  Ve100: Ve100
2    Group ff08:1001:2001::1
     Group member at  Ve200: Ve200
3    Group ff0e:1000:2000::1
     Group member at  eth 0/1: eth 0/1
```

show ipv6 pim interface

Displays IPv6 PIM status and configuration information for an interface.

Syntax

show ipv6 pim interface [{ ethernet |ve |loopback} *interface-num*]

Parameters

`ethernet`

Specifies an Ethernet interface for which to show information.
interface-num

Specifies the interface name in the slot or port.

`ve`

Specifies a virtual Ethernet interface for which to show information.
interface-num

Specifies the VE number.

`loopback`

Specifies a loopback interface for which to show information.
interface-num

Specifies the loopback number.

Modes

Privileged EXEC mode

Usage Guidelines

The **show ipv6 pim interface** form of this command displays interface information for the node on which you execute the command.

The **show ipv6 pim interface ve** version of this command displays information about the VE interface on the node on which you execute the command.

The **show ipv6 pim interface ethernet** version of this command displays information about the Ethernet interface on the node on which you execute the command.

The **show ipv6 pim interface loopback** version of this command displays information about the loopback interface on the node on which you execute the command.

Examples

This example shows typical output for the **show ipv6 pim interface** version of this command.

```
device# show ipv6 pim interface
------------+-------------------------------+----+-----
+-------------------------------------------+---+--------|--------------------
Interface    |Local                          |Ver
|Mode |Designated                    Router       |TTL| DR     |        Vrf
             |Address                        |
|     |Address                       Port         |Thr| Prio   |        Name
------------+-------------------------------+----+-----
+-------------------------------------------+---+--------|--------------------
Eth 0/6       fe80::629c:9fff:fe5a:ee1c
v2    SM    fe80::da84:66ff:feea:3b1f     None          1   1       default-vrf
Eth 0/47      fe80::629c:9fff:fe5a:ee45
v2    SM    Itself                        None          1   1       default-vrf
Ve20          fe80::629c:9fff:fe5a:ee15      v2
SM    fe80::7aa6:e1ff:fe45:9815     None          1   1       default-vrf
Ve40          fe80::629c:9fff:fe5a:ee15      v2
SM    fe80::748e:f8ff:fe05:7801     None          1   1       default-vrf
Ve41          fe80::629c:9fff:fe5a:ee15      v2
SM    fe80::748e:f8ff:fe05:7801     None          1   1       default-vrf
Ve700         fe80::629c:9fff:fe5a:ee15      v2
SM    Itself                        None          1   1       default-vrf
```

show ipv6 pim mcache

Displays route entries in the multicast cache.

Syntax

show ipv6 pim mcache [[*ipv6-address-1* | *ipv6-address-2*] | **ecmp** |]

Parameters

ip-address-1

Specifies the Group/Source IPv6 address.

ip-address-2

Specifies the Source/Group IPv6 address.

ecmp

Specifies IPv6 PIM equal-cost multi-path (ECMP) routing information.

Modes

Privileged EXEC mode

Examples

The following example shows typical output for the command.

```
device# show ipv6 pim mcache
IP Multicast Mcache Table
Entry Flags    : sm  - Sparse Mode, ssm - Source Specific Multicast
                 RPT - RPT Bit, SPT - SPT Bit, LSrc - Local Source
                 LRcv - Local Receiver, RegProbe - Register In Progress
                 RegSupp - Register Suppression Timer, Reg - Register Complete
                 needRte - Route Required for Src/RP, JDUp - Join Desire Upstream
Interface Flags: IM - Immediate, IH - Inherited, WA - Won Assert
                 MJ - Membership Join, MI - Membership Include, ME - Membership Exclude
                 BR - Blocked RPT, BA - Blocked Assert, BF - Blocked Filter
                 BI - Blocked IIF, UJ - Unintended Join oif
Total entries in mcache: 2
1    (*, ff0e:1000:2000::1) RP 1234::32 in Eth 0/8, Uptime 00:16:18
     Sparse Mode, RPT=1 SPT=0 Reg=0 RegSupp=0 RegProbe=0 JDUp=1 LSrc=0 LRcv=1
     upstream neighbor=fe80::2e0:cff:fe03:a (2008::32)
     AgeSltMsk: 0     num_oifs = 1
           Ve100(00:16:18/0) Flags: MJ
     Flags (0x01260480)
         sm=1 needRte=0
2    (1010::100, ff0e:1000:2000::1) in Eth 0/8, Uptime 00:09:27
     Sparse Mode, RPT=0 SPT=1 Reg=0 RegSupp=0 RegProbe=0 JDUp=1 LSrc=0 LRcv=1
     upstream neighbor=fe80::2e0:cff:fe03:a (2008::32)
     AgeSltMsk: 1 KAT timer value: 240
     num_oifs = 1
           Ve100(00:09:27/0) Flags: MJ
     Flags (0x510680f4)
         sm=1 needRte=0
```

show ipv6 pim neighbor

Displays information about active neighbors for a PIM router.

Syntax

show ipv6 pim neighbor [**interface** {**ethernet** | **ve**} *interface-num*]

Parameters

interface

Specifies an interface for which to display neighbor information.

ethernet *interface-num*

Specifies an Ethernet interface name in the slot or port.

ve *interface-num*

Specifies a virtual Ethernet interface number.

Modes

Privileged EXEC mode

Usage Guidelines

The **show ipv6 pim neighbor** form of this command displays neighbor information for the node on which you execute the command.

The **show ipv6 pim neighbor interface ve** form of this command displays neighbor information for the VE interface on the node on which you execute the command.

The **show ipv6 pim neighbor interface ethernet** form of this command displays neighbor information for the Ethernet interface on the node on which you execute the command.

Examples

This example shows typical output for the **show ipv6 pim neighbor** form of the command.

```
device# show ipv6 pim neighbor
Total Number of Neighbors : 4
Port         Phy_Port     Neighbor                                  Holdtime Age
UpTime  Priority
                                                                    sec      sec      Dd
HH:MM:SS
Eth 0/6      Eth 0/6      fe80::da84:66ff:feea:3b1f                 105      16
01:32:17         1
                         +2001:6:8:68::6
Ve20         Ve20         fe80::7aa6:e1ff:fe45:9815                 105      19
01:42:21         1
                         +2001:5:8:58::5
Ve40         Ve40         fe80::748e:f8ff:fe05:7801                 105      10       7d
```

```
07:10:24         1
                         +2001:2:8:28::2
Ve41         Ve41         fe80::748e:f8ff:fe05:7801              105      10       7d
07:10:23         1
                         +2001:8:2:82::2
```

show ipv6 pim rp-candidate

Displays information about the candidate rendezvous point (RP).

Syntax

show ipv6 pim rp-candidate

Modes

Privileged EXEC mode

Usage Guidelines

This command displays information about the candidate RP and its group mappings.

Examples

The following example shows typical output for the command.

```
device# show ipv6 pim rp-candidate
Next Candidate-RP-advertisment in 00:00:10
  RP: 1234::5
    group prefixes:
    ff08:: / 16
    ff05:: / 16
  Candidate-RP-advertisement period: 60
```

show ipv6 pim rp-hash

Displays the rendezvous points (RP) for a PIM-SM (Sparse Mode) group.

Syntax

show ipv6 pim rp-hash *group-addr*

Parameters

group-addr

Specifies the IPv6 address of the PIM-SM group.

Modes

Privileged EXEC mode

Usage Guidelines

This command displays the learned or configured RPs for the indicated PIM-SM group.

Examples

This example shows the RP for the FF05:10::10:20 group.

```
device# show ipv6 pim rp-hash ff0e:1000:2000::1
RP: 1234::32, v2
    Info source: 1234::5, via bootstrap
```

show ipv6 pim rp-map

Displays the mapping of group addresses to rendezvous point (RP) addresses.

Syntax

show ipv6 pim rp-map

Modes

Privileged EXEC mode

Examples

The following example shows typical output for the command.

```
device# show ipv6 pim rp-map
Number of group-to-RP mappings: 3

     Group address       RP address
----------------------------------------
1    ff04:3000:4000::2   1234::1234
2    ff08:1001:2001::1   1234::5
3    ff0e:1000:2000::1   1234::32
```

show ipv6 pim rp-set

Displays the rendezvous point (RP) set list.

Syntax

show ipv6 pim rp-set

Modes

Privileged EXEC mode

Usage Guidelines

This command shows information for all learned or configured RPs.

Examples

This example shows typical output for the command.

```
device# show ipv6 pim rp-set
Vrf Instance : default-vrf
---------------------------
Static RP
---------
 Static RP count: 1
   RP: 1234::1234
Number of group prefixes Learnt from BSR: 3
Group prefix = ff05::      # RPs: 1
      RP 1: 1234::5    priority=0    age=30    holdtime=150
Group prefix = ff08::      # RPs: 1
      RP 1: 1234::5    priority=0    age=30    holdtime=150
Group prefix = ff0e::      # RPs: 1
      RP 1: 1234::32    priority=0    age=40    holdtime=150
```

show ipv6 pim rpf

Displays the Reverse Path Forwarding (RPF) for a specified address.

Syntax

show ipv6 pim rpf *src-ipv6-addr* [*grp-ipv6-addr*]

Parameters

src-ipv6-addr

Specifies the IPv6 source or RP address for RPF.

grp-ipv6-addr

(Optional) Specifies the IPv6 group address.

Modes

Privileged EXEC mode

Usage Guidelines

This command displays the port that PIM regards as the best reverse path for the specified address.

Examples

This example shows typical output for the command.

```
device# show ipv6 pim rpf 1234:32
upstream nbr fe80::2e0:cff:fe03:a on Eth 0/8
```

show ipv6 pim settings

Displays settings such as neighbor timeout and hello interval.

Syntax

show ipv6 pim settings

Modes

Privileged EXEC mode

Examples

The following example shows typical output for the command.

```
device# show ipv6 pim settings

vrf : default-vrf
Maximum mcache           : 32768     Current Count             : 0
Hello interval           : 30        Neighbor timeout          : 105
Join/Prune interval      : 60        Inactivity interval       : 180
Hardware drop enabled    : 1         Prune wait interval       : 3
Register Suppress Time   : 60        Register Probe Time       : 10
Register Stop Delay      : 0         Register Suppress interval: 0
SSM Enabled              : No        SPT Threshold             : 1
Route Precedence         : uc-non-default uc-default none
```

show ipv6 pim traffic

Displays traffic statistics on each IPv6 PIM-enabled interface.

Syntax

show ipv6 pim traffic

Modes

Privileged EXEC mode

Examples

The following example shows typical output for the command.

```
device# show ipv6 pim traffic
Port         |HELLO               |JOIN                |PRUNE               |
ASSERT              |GRAFT/REGISTER     |REGISTER-STOP      |BSR-MSGS            |RPC-MSGS
             |Rx         Tx       |Rx         Tx       |Rx         Tx       |Rx
Tx        |Rx         Tx       |Rx         Tx       |Rx         Tx       |Rx         Tx
-----------+---------+---------+---------+---------+---------+---------+---------+---------
+---------+---------+---------+---------+---------+---------+---------+---------+---------
Eth 0/6      197       201       490       0         0         0         0
0         0         0         0         0         0         0         0         0
Eth 0/47     0         21087     0         0         0         0         0
0         0         0         0         0         0         0         0         0
Ve20         219       220       1068      108       0         214       0
0         0         643       428       0         0         0         0         0
Ve40         21034     21035     18264     64000     57        31535     0
0         73972     41170     61336     36982     0         0         0         0
Ve41         21032     21037     4         12        16        450       0
14913     4         0         0         0         0         0         0         0
Ve700        0         21086     0         0         0         0         0
0         0         0         0         0         0         0         0         0
```

show ipv6 prefix-list

Displays IPv6 prefix-lists.

Syntax

show ipv6 prefix-list *prefix-list-name*

Parameters

prefix-list-name

Specifies an IPv6 prefix list name.

Modes

Privileged EXEC mode

Usage Guidelines

The *prefix-list-name* parameter restricts the display to the specified prefix list. Specify the name of the prefix list that you want to display.

Output

The **show ipv6 prefix-list** command displays the following information:

Examples

The following example shows how to display IPv6 prefix lists.

```
device# show ipv6 prefix-lists
ipv6 prefix-list routesfor2001: 2 entries
     seq 5 permit 2001::/16
     seq 10 permit 2001:db8::/32
```

show ipv6 route

Displays the router advertisement information.

Syntax

show ipv6 route [**all** | **bgp** | **connected** | **import** *source-name* | **nexthop** *nexthop-id* | **ospf** | **static** | **summary** | **system-summary**] *vrf-name*

show ipv6 route [**isis** | **slot** *line-card-number* | **static** | **system-summary** | **vrf** *number*]

Parameters

all

Specifies all routes.

bgp

Specifies BGP routes.

connected

Displays the directly connected routes.

import *source-name*

Specifies import routes and the source VRF name

isis

Specifies routes learned from the Intermediate System to Intermediate System (IS-IS) protocol.

nexthop *nexthop-id*

Displays the route nexthop table.

ospf

Specifies OSPF routes.

slot *line-card-number*

Specifies the IPv6 route information on a slot for the specified line card number.

static

Specifies static IPv6 routes.

summary

Displays the route summary.

system-summary

Displays the system-level summary for IPv6 routes.

vrf-name

The name of the VRF context.

vrf *number*

Specifies a VRF instance.

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported only on Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices. For a complete list of devices, see "Supported Hardware".

Routes of type *DHCPv6* show tag value *10*.

Examples

The following is an example of the **show ipv6 route** command output.

```
SLX# show ipv6 route
IPv6 Routing Table for VRF "default-vrf"
Total number of IPv6 routes: 13
'*' denotes best ucast next-hop
'[x/y]' denotes [preference/metric]

1200:1201::/64, attached
    *via ::, Eth 2/45, [0/0], 45m29s, direct, tag 0
1200:1201::1:1/128, attached
    *via ::, Eth 2/45, [0/0], 45m29s, local, tag 0
1200:1202::/64, attached
    *via ::, Ve 2, [0/0], 45m26s, direct, tag 0
1200:1202::1:1/128, attached
    *via ::, Ve 2, [0/0], 45m26s, local, tag 0
2221::/32
    *via 1200:1201::1:2, Eth 2/45, [100/10], 11m41s, static, tag 300
2222::/48
    *via fe80::205:33ff:fee6:a531, Eth 2/45, [1/1], 43m44s, static, tag 0
2222::1/128
    *via fe80::205:33ff:fee6:a531, Eth 2/45, [110/1], 0m7s, ospfv3, intra, tag 0
2223::/64
    *via 1200:1202::1:2, Ve 2, [1/1], 3m45s, static, tag 0
2224::1/128
    *via fe80::205:33ff:fee6:a501, Ve 2, [1/1], 43m41s, static, tag 0
fe80::/10, attached
    *via ::, , [0/0], 6h30m, local, tag 0
ff00::/8, attached
    *via ::, Null0, [0/0], 6h30m, local, tag 0
2043:0:0:1::1/64,
     via fe80::1, Ve 5, [10/1], 1h4m, dhcpv6, tag 10
2043:0:0:2::1/64,
     via fe80::1, Ve 6, [10/1], 1h4m, dhcpv6, tag 10
```

show ipv6 static route

Displays information about IPv6 static routes.

Syntax

show ipv6 static route [*ipv6prefix* | **vrf** *vrf-name*]

Parameters

ipv6prefix

The IPv6 prefix in the *A:B::/length* format.

vrf vrf-name

The name of the VRF context.

Modes

Privileged EXEC mode

Examples

The following example displays the IPv6 static route information for the default VRF.

```
device# show ipv6 static route
IPv6 Configured Static Routes for VRF "default-vrf"

3002:7::/64-> 1200:3::1:2 preference: 1
   nh_vrf (default-vrf)

3002:9::/64-> 1200:4::1:2 preference: 1
   nh_vrf (default-vrf)
device#
```

show ipv6 vrrp

Displays information about IPv6 VRRP and VRRP-E sessions.

Syntax

show ipv6 vrrp

show ipv6 vrrp *VRID* [**detail** | **summary**]

show ipv6 vrrp detail

show ipv6 vrrp summary [**vrf** { *vrf-name* | **all** | **default-vrf** }]

show ipv6 vrrp interface { **ethernet** *slot*/*port* | **port-channel** *number* | **ve** *vlan_id* } [**detail** | **summary**]

Parameters

VRID

The virtual group ID about which to display information. The range is from 1 through 16.

detail

Displays all session information in detail, including session statistics.

summary

Displays session-information summaries.

vrf

Specifies a VRF instance or all VRFs.

vrf-name

Specifies a VRF instance. For the default vrf, enter **default-vrf**.

all

Specifies all VRFs.

interface

Displays information for an interface that you specify.

ethernet *slot port*

Specifies a valid, physical Ethernet interface with a slot and port number.

port-channel *number*

Specifies a port-channel interface.

ve *vlan_id*

Specifies the VE VLAN number.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display information about IPv6 VRRP and VRRP-E sessions, either in summary or full-detail format. You can also specify a particular virtual group ID, or an interface for which to display VRRP output.

Note
IPv6 VRRP-E supports only the VE interface type.

To display information for IPv6 VRRP sessions using the default VRF, you can use the **show ipv6 vrrp summary** syntax (with no additional parameters).

To display information for the default or a named VRF, you can use the **show ipv6 vrrp summary vrf** syntax with the *vrf-name* option.

To display information about all VRFs, use the **show ipv6 vrrp summary vrf all** syntax.

Examples

The following example displays information about all IPv6 VRRP sessions on the device.

```
device# show ipv6 vrrp

Total number of VRRP session(s)   : 2

VRID 14
  Interface: Ve 2018;  Ifindex: 1207961570
  Mode: VRRP
  Admin Status: Enabled
  Description :
  Address family: IPv6
  Version: 3
  Authentication type: No Authentication
  State: Master
  Session Master IP Address: Local
  Virtual IP(s): fe80::1
  Configured Priority: unset (default: 100); Current Priority: 100
  Advertisement interval: 1000 milli sec  (default: 1000 milli sec)
  Preempt mode: ENABLE  (default: ENABLE)
  Hold time: 0 sec  (default: 0 sec)
  Trackport:
    Port(s)                   Priority  Port Status
    =======                   ========  ===========
  Statistics:
    Advertisements: Rx: 0, Tx: 35
    Neighbor Advertisements: Tx: 1

VRID 15
  Interface: Ve 2019;  Ifindex: 1207961571
  Mode: VRRP
  Admin Status: Enabled
  Description :
  Address family: IPv6
  Version: 3
  Authentication type: No Authentication
  State: Master
  Session Master IP Address: Local
  Virtual IP(s): fe80::1
```

```
  Configured Priority: unset (default: 100); Current Priority: 100
  Advertisement interval: 1000 milli sec  (default: 1000 milli sec)
  Preempt mode: ENABLE  (default: ENABLE)
  Hold time: 0 sec  (default: 0 sec)
  Trackport:
    Port(s)                   Priority  Port Status
    =======                   ========  ===========
  Statistics:
    Advertisements: Rx: 0, Tx: 448
    Neighbor Advertisements: Tx: 1
```

The following example displays IPv6 VRRP information in detail for a specific virtual group ID of 19, including session statistics.

```
device# show ipv6 vrrp 19 detail

Total number of VRRP session(s)   : 1
VRID 15
  Interface: Ve 2019;  Ifindex: 1207961571
  Mode: VRRPE
  Admin Status: Enabled
  Description :
  Address family: IPv6
  Version: 3
  Authentication type: No Authentication
  State: Backup
  Session Master IP Address: fe80::205:33ff:fe79:fb1e
  Virtual IP(s): 2001:2019:8192::1
  Virtual MAC Address: 02e0.5200.2513
  Configured Priority: unset (default: 100); Current Priority: 100
  Advertisement interval: 1 sec  (default: 1 sec)
  Preempt mode: DISABLE  (default: DISABLED)
  Advertise-backup: ENABLE  (default: DISABLED)
  Backup Advertisement interval: 60 sec  (default: 60 sec)
  Short-path-forwarding: Enabled
  Revert-Priority: unset; SPF Reverted: No
  Hold time: 0 sec  (default: 0 sec)
  Master Down interval: 4 sec
  Trackport:
    Port(s)                   Priority  Port Status
    =======                   ========  ===========
  Global Statistics:
  ==================
    Checksum Error : 0
    Version Error  : 0
    VRID Invalid   : 0
  Session Statistics:
  ===================
    Advertisements             : Rx: 103259, Tx: 1721
    Neighbor Advertisements             : Tx: 0
    Session becoming master    : 0
    Advts with wrong interval  : 0
    Prio Zero pkts             : Rx: 0, Tx: 0
    Invalid Pkts Rvcd          : 0
    Bad Virtual-IP Pkts        : 0
    Invalid Authenticaton type : 0
    Invalid TTL Value          : 0
    Invalid Packet Length      : 0
    VRRPE backup advt sent     : 1721
    VRRPE backup advt recvd    : 0
```

The following example displays summary information for IPv6 VRRP statistics on the default VRF. (This command is equivalent to **show ipv6 vrrp summary vrf default-vrf**.)

```
device# show ipv6 vrrp summary

Total number of VRRP session(s)   : 1
Master session count  : 1
Backup session count  : 0
Init session count    : 0

VRID  Session  Interface  Admin   Current   State    Short-path  Revert    SPF
                          State   Priority           Forwarding  Priority  Reverted
====  =======  =========  =====   ========  =====    ==========  ========  ========
15    VRRPE    Ve 2019    Enabled 100       Master   Enabled     unset     No
```

The following example displays summary information for IPv6 VRRP statistics on the VRF named red.

```
device# show ipv6 vrrp summary vrf red

Total number of VRRP session(s)   : 1
Master session count  : 1
Backup session count  : 0
Init session count    : 0

VRID  Session  Interface  Admin   Current   State    Short-path  Revert    SPF
                          State   Priority           Forwarding  Priority  Reverted
====  =======  =========  =====   ========  =====    ==========  ========  ========
14    VRRPE    Ve 2018    Enabled 100       Master   Enabled     unset     No
```

The following example displays summary information for IPv6 VRRP statistics on all VRFs.

```
device# show ipv6 vrrp summary vrf all

Total number of VRRP session(s)   : 2
Master session count  : 2
Backup session count  : 0
Init session count    : 0

VRID  Session  Interface  Admin   Current   State    Short-path  Revert    SPF
                          State   Priority           Forwarding  Priority  Reverted
====  =======  =========  =====   ========  =====    ==========  ========  ========
14    VRRPE    Ve 2018    Enabled 100       Master   Enabled     unset     No
15    VRRPE    Ve 2019    Enabled 100       Master   Enabled     unset     No
```

The following example displays information for IPv6 VRRP-E tracked networks.

```
device# show ipv6 vrrp detail

Total number of VRRP session(s)   : 1

VRID 2
  Interface: Ve 100;  Ifindex: 1207959652
  Mode: VRRPE
  Admin Status: Enabled
  Description :
  Address family: IPv6
  Version: 3
  Authentication type: No Authentication
  State: Master
  Session Master IP Address: Local
```

```
Virtual IP(s): 2001:2019:8192::1
Virtual MAC Address: 02e0.5225.1002
Configured Priority: unset (default: 100); Current Priority: 100
Advertisement interval: 1 sec  (default: 1 sec)
Preempt mode: DISABLE  (default: DISABLED)
Advertise-backup: DISABLE  (default: DISABLED)
Backup Advertisement interval: 60 sec  (default: 60 sec)
Short-path-forwarding: Disabled
Revert-Priority: unset; SPF Reverted: No
Hold time: 0 sec  (default: 0 sec)
Master Down interval: 4 sec
Trackport:
  Port(s)                   Priority  Port Status
  =======                   ========  ===========

Tracknetwork:
  Network(s)                Priority  Status
  =========                 ========  ==========
  2001::/64                 20        Up

Global Statistics:
==================
  Checksum Error : 0
  Version Error  : 0
  VRID Invalid   : 0

Session Statistics:
===================
  Advertisements             : Rx: 0, Tx: 132
  Neighbor Advertisements           : Tx: 66
  Session becoming master    : 1
  Advts with wrong interval  : 0
  Prio Zero pkts             : Rx: 0, Tx: 0
  Invalid Pkts Rvcd          : 0
  Bad Virtual-IP Pkts        : 0
  Invalid Authenticaton type : 0
  Invalid TTL Value          : 0
  Invalid Packet Length      : 0
  VRRPE backup advt sent     : 0
  VRRPE backup advt recvd    : 0
```

show isis

Displays general IS-IS information.

Syntax

show isis

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Output

The **show isis** command displays the following information:

Output field	Description
IS-IS Routing Protocol Operation State	The operating state of IS-IS. Possible states include the following: • Enabled - IS-IS is enabled. • Disabled - IS-IS is disabled.
IS-Type	The intermediate system type. Possible types include the following: • Level 1 only - The device routes traffic only within the area in which it resides. • Level 2 only - The device routes traffic between areas of a routing domain. • Level 1-2 - The device routes traffic within the area in which it resides and between areas of a routing domain.
System ID	The unique IS-IS router ID. Typically, the device's base MAC address is used as the system ID.
Manual area address(es)	Area address(es) of the device.
Level-1-2 Database State	The state of the Level 1-2 Database: • On • Off
Administrative Distance	The current setting of the IS-IS administrative distance.
Maximum Paths	The number of paths IS-IS can calculate and install in the forwarding table
Default redistribution metric	The value of the default redistribution metric, which is the IS-IS cost of redistributing the route into IS-IS.
Number of Routes redistributed into IS-IS	The number of routes distributed into IS-IS.
Level-1 Auth-mode	One of the following authentication modes set for Level-1 on the router: • None • md5 • cleartext
Level-2 Auth-mode	One of the following authentication modes set for Level-2 on the router: • None • md5 • cleartext
Metric Style Supported for Level-1	The following values are supported: • Wide - Wide Metric Style

Output field	Description
	• Narrow - Narrow Metric Style
Metric Style Supported for Level-2	The following values are supported: • Wide - Wide Metric Style • Narrow - Narrow Metric Style
IS-IS Partial SPF Optimizations	This parameter can contain one of the following values: • Enabled • Disabled
Timers: L1 or L2 SPF:	These values are displayed individually for IS-IS levels 1 and 2.
max-wait	The maximum time gap that occurs between running of SPF calculations. It is the value configured as the spf-max-wait variable in the**spf-interval** command.
Init-wait	The initial time gap between an SPF event and the first running of SPF. This value reflects the spf-initial-time variable that is configured using the **spf-interval** command.
Second-wait	The interval between the first running of SPF and the first recalculation of the SPF tree. If this optional value is configured, it is doubled with each recalculation of the SPF tree until the value is equal to the max-wait value This value reflects the spf-second-wait variable that is configured using the **spf-interval** command.
SPF run status.	This field is not specifically labeled but is displayed directly under the SPF timers. It can any of the three values shown below: • SPF is running • SPF will run in *sec* where the *sec* variable is a value in seconds until the next time that SPF will be run. • SPF is not scheduled
Timers: PSPF:	
max-wait	The maximum time gap that occurs between running of PSPF calculations. It is the value configured as the max-wait value in the**partial-spf-interval** command.
Init-wait	The initial time gap between the wait time after an LSP change until the first PSPF calculation. This value reflects the initial-wait variable that is configured using the **partial-spf-interval** command.
Second-wait	The wait time between the first and second PSPF calculations. If this optional value is configured, it is doubled with each PSPF recalculation until the value is equal to the max-wait value

Output field	Description
	This value reflects the second-wait variable that is configured using the **partial-spf-interval** command.
PSPF run status.	This field is not specifically labeled but is displayed directly under the PSPF timers. It can any of the three values shown below: • PSPF is running • PSPF will run in *sec* where the *sec* variable is a value in seconds until the next time that PSPF will be run. • PSPF is not scheduled
Timers: LSP:	
max-lifetime	The maximum number of seconds an unrefreshed LSP can remain in the device's LSP database. The default value is 1000 sec.
refresh-interval	The maximum number of seconds that a device waits between sending updated LSPs to its IS-IS neighbors. The default value is 1 sec.
gen-interval	The minimum number of seconds that a device waits between sending updated LSPs to its IS-IS neighbors. The default value is 10 sec.
retransmit-interval	The amount of time the device waits before it retransmits LSPs. The default value is 5 sec.
lsp-interval	The rate of transmission (in milliseconds) of the LSPs. The default rate is 33 ms.
Timers: SNP:	
csnp-interval	How often the designated IS sends a CSNP to the broadcast interface. The default value is 10 sec.
psnp-interval	How often the IS sends a PSNP. The default value is 2 sec.
Global Hello Padding	This value can be: • Enabled • Disabled
Global Hello Padding For Point to Point Circuits	This value can be: • Enabled • Disabled
Ptpt Three Way HandShake Mechanism	This value can be: • Enabled • Disabled
IS-IS Traffic Engineering Support	This value can be: • Enabled

Output field	Description
	• Disabled
BFD	This value can be: • Enabled • Disabled
Interfaces with IPv4 IS-IS configured	Interfaces on which IPv4 IS-IS is configured.

Examples

The following example displays sample output from the **show isis** command.

```
device# show isis

 IS-IS Routing Protocol Operation State: Enabled
 IS-Type: Level-1-2
 System Id: 768e.f805.5812
 Manual area address(es): 11
 Level-1-2 Database State:  On
 Administrative Distance 115
 Maximum Paths 8
 Default redistribution metric 0
 Default link metric for level-1 0 (conf)/ 10 (adv)
 Default link metric for level-2 0 (conf)/ 10 (adv)
 Protocol Routes Redistributed into IS-IS:  None
 Number of Routes Redistributed into IS-IS: 0
 Level-1 Auth-mode: None
 Level-2 Auth-mode: None
 Metric Style Supported for Level-1: Narrow
 Metric Style Supported for Level-2: Narrow
 Graceful-Restart Helper Support: Enabled
 ISIS Partial SPF Optimizations: Enabled
 Timers:
    L1 SPF: Max-wait 5s Init-wait 5000ms Second-wait 5000ms
    L2 SPF: Max-wait 5s Init-wait 5000ms Second-wait 5000ms
        L1 SPF is not scheduled
        L2 SPF is not scheduled
    PSPF: Max-wait 5000ms Init-wait 2000ms Second-wait 5000ms
        PSPF is not scheduled
    LSP: max-lifetime 1200s refresh-interval 900s gen-interval 10s
        retransmit-interval 5s, lsp-interval 33ms
    SNP: csnp-interval 10s psnp-interval 2s
 Global Hello Padding: Enabled
 Global Hello Padding For Point to Point Circuits: Enabled
 Ptpt Three Way HandShake Mechanism: Enabled
 BGP Ipv4 Converged: False  BGP Ipv6 Converged: False
 IS-IS Traffic Engineering Support: Disabled
  No ISIS Shortcuts Configured
 BFD: Disabled, BFD HoldoverInterval: 0
 NSR: Disabled
 LSP-SYNC: Not Globally Enabled
```

show isis config

Displays the global IS-IS configuration commands that are in effect on the device.

Syntax

show isis config

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The running-config does not list the default values. Only commands that change a setting or add configuration information are displayed.

Examples

The following example displays sample output from the **show isis config** command.

```
device# show isis config

router isis
 net 11.768e.f805.5812.00
 address-family ipv4 unicast
!

 address-family ipv6 unicast
!
```

show isis counts

Displays IS-IS error statistics.

Syntax

```
show isis counts
```

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Output

The **show isis counts** command displays the following information:

Output field	Description
Area Mismatch	The number of times the device interface was unable to create a Level-1 adjacency with a neighbor because the device interface and the neighbor did not have any areas in common.
Max Area Mismatch	The number of times the device received a PDU whose value for maximum number of area addresses did not match the device's value for maximum number of area addresses.
System ID Length Mismatch	The number of times the device received a PDU whose ID field was a different length than the ID field length configured on the device.
LSP Sequence Number Skipped	The number of times the device received an LSP with a sequence number that was more than 1 higher than the sequence number of the previous LSP received from the same neighbor.
LSP Max Sequence Number Exceeded	The number of times the device attempted to set an LSP sequence number to a value higher than the highest number in the CSNP sent by the Designated IS.
Level-1 Database Overload	The number of times the Level-1 state on the device changed from Waiting to On or from On to Waiting. • Waiting to On - This change can occur when the device recovers from a previous Level-1 LSP database overload and is again ready to receive new LSPs. • On to Waiting - This change can occur when the device's Level-1 LSP database is full and the device receives an additional LSP, for which there is no room.
Level-2 Database Overload	The number of times the Level-2 state on the device changed from Waiting to On or from On to Waiting. • The change from Waiting to On can occur when the device recovers from a previous Level-2 LSP database overload and is again ready to receive new LSPs.

Output field	Description
	• The change from On to Waiting can occur when the device's Level-2 LSP database is full and the device receives an additional LSP, for which there is no room.
Our LSP Purged	The number of times the device received an LSP that was originated by the device itself and had age zero (aged out).
PDU Drop Count	
CSNP Auth Failures	The number of CSNP Authentication failures recorded for Level-1 and Level-2. This counter will only be displayed if it has a value greater than zero.
PSNP Auth Failures	The number of PSNP Authentication failures recorded for Level-1 and Level-2. This counter appears only if it has a value greater than 0.
HELLO Auth Failures	The number of HELLO Authentication failures recorded for Level-1 and Level-2. This counter will only be displayed if it has a value greater than zero.
Adjacency not found	The number of PDUs dropped at both Level-1 and Level-2 because there is no valid adjacency on the interface where they were received. This counter will only be displayed if it has a value greater than zero.
Adjacency Level Mismatch	The number of PDUs dropped at both Level-1 and Level-2 because the adjacency from which the PDU is received has a different level than the PDU level. This counter will only be displayed if it has a value greater than zero.
IS Level Mismatch	The number of PDUs dropped at both Level-1 and Level-2 because the IS-IS router level mismatches with the PDU level received. This counter will only be displayed if it has a value greater than zero.
Length Too Short	The number of PDUs dropped at both Level-1 and Level-2 because the received PDU length is less than the standard PDU header length. This counter will only be displayed if it has a value greater than zero.
Length Too Long	The number of PDUs dropped at both Level-1 and Level-2 because the received PDU length is greater than the MTU of the link. This counter will only be displayed if it has a value greater than zero.
Max Area Check Failure	The number of PDUs dropped at both Level-1 and Level-2 because the received PDU has a maximum area count different than what is configured on this IS-IS router. This counter will only be displayed if it has a value greater than zero.
Zero Checksum	The number of PDUs dropped at both Level-1 and Level-2 because the received PDU has a zero checksum. This counter will only be displayed if it has a value greater than zero.
Checksum Mismatch	The number of PDUs dropped at both Level-1 and Level-2 because the received PDU has a checksum different than the computed checksum on the received PDU. This counter will only be displayed if it has a value greater than zero.
Invalid Length	The number of PDUs dropped at both Level-1 and Level-2 because the received PDU has a different length than what is advertised in

Output field	Description
	the PDU header. This counter will only be displayed if it has a value greater than zero.

Examples

The following example displays sample output from the **show isis counts** command.

```
device# show isis counts

 Area Mismatch: 0
 Max Area Mismatch: 0
 System ID Length Mismatch: 0
 LSP Sequence Number Skipped: 0
 LSP Max Sequence Number Exceeded: 0
 Level-1 Database Overload: 0
 Level-2 Database Overload: 0
 Our LSP Purged: 0
```

show isis database

Displays information about the entries in the LSP database.

Syntax

show isis database lsp-id

show isis database detail [**level1** | **level2**]

show isis database level1

show isis database level2

show isis database summary

Parameters

lsp-id

Specifies a link-state packet (LSP) in HHHH.HHHH.HHHH.HH-HH format, for example, 3333.3333.3333.00-00, or by entering a name, for example, XMR.00-00.

detail

Specifies detailed information.

level1

Specifies Level 1 packets only.

level2

Specifies Level 2 packets only.

summary

Specifies summarized information.

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Output

The **show isis database** command displays the following information:

Output field	Description
LSPID	The LSP ID, which consists of the source ID (6 bytes), the pseudonode (1 byte), and LSPID (1 byte). **Note:** If the address has an asterisk (*) at the end, this indicates that the LSP is locally originated.
LSP Seq Num	The sequence number of the LSP.
LSP Checksum	The checksum calculated by the device that sent the LSP and used by the device to verify that the LSP was not corrupted during transmission over the network.
LSP Holdtime	The maximum number of seconds during which the LSP will remain valid. **Note:** The IS that originates the LSP sets the timer for the LSP. As a result, LSPs do not all have the same amount of time remaining when they enter the device's LSP database.
ATT	A 4-bit value extracted from bits 4 - 7 in the Attach field of the LSP.
P	The value in the Partition option field of the LSP. The field can have one of the following values: • 0 - The IS that sent the LSP does not support partition repair. • 1 - The IS that sent the LSP supports partition repair.
OL	The value in the LSP database overload field of the LSP. The field can have one of the following values: • 0 - The overload bit is off. • 1 - The overload bit is on, indicating that the IS that sent the LSP is overloaded and should not be used as a IS-IS transit router for that level.
NLPID	The Network Layer Protocol Identifier (NLPID), which specifies the protocol the IS that sent the LSP is using. Usually, this value is "CC(IP)".
IP address	The IP address of the interface that sent the LSP. The device can use this address as the next hop in routes to the addresses listed in the rows below.
Destination addresses	The rows of information below the IP address row are the destinations advertised by the LSP. The device can reach these destinations by using the IP address listed above as the next hop. Each destination entry contains the following information: • Metric - The value of the default metric, which is the IS-IS cost of using the IP address above as the next hop to reach this destination.

Output field	Description
	• Device type - The device type at the destination. The type can be one of the following: ◦ End System - The device is an ES. ◦ IP-Internal - The device is an ES within the current area. The IP address and subnet mask are listed. ◦ IS - The device is another IS. The NET (NSAP address) is listed. ◦ IP-Extended - Same as IP-Internal, except the device uses the extended TLV fields described in draft-ietf-isis-traffic-02.txt to carry the information. ◦ IS-Extended - Same as IS, except the device uses the extended TLV fields described in draft-ietf-isis-traffic-02.txt to carry the information.
Flooding to *num* interface:	Identifies the number of interfaces on which the specific LSP entry will be flooded and identifies the interfaces.
Acking to *num* interface:	Identifies the number of interfaces on which the specific LSP entry will be acknowledged and identifies the interfaces.

Examples

The following is sample output for the **show isis database** command when no argument or keyword is used.

```
device# show isis database

IS-IS Level-1 Link State Database
LSPID                             Seq Num    Checksum  Holdtime ATT/P/OL
R1.00-00*                         0x00000030 0x163a    394      0/0/0
IS-IS Level-2 Link State Database
LSPID                             Seq Num    Checksum  Holdtime ATT/P/OL
R1.00-00*                         0x00000030 0xc865    394      0/0/0
```

The following is sample output for the **show isis database** command when the **detail** keyword is used.

```
device# show isis database detail

IS-IS Level-1 Link State Database
LSPID                             Seq Num    Checksum  Holdtime ATT/P/OL
R1.00-00*                         0x00000038 0x0642    1095     0/0/0
   Area Address:  11
   NLPID:  IP
   Hostname:  R1
   Metric:  10       IP-Internal 1.2.3.4/32          Up: 0
   Metric:  10       IP-Internal 11.2.1.16/30        Up: 0
   Metric:  10       IP-Internal 11.2.1.0/30         Up: 0
   Metric:  10       IP-Internal 11.2.1.8/30         Up: 0
   Metric:  10       IP-Internal 11.2.1.4/30         Up: 0
   Metric:  10       IP-Internal 11.2.1.12/30        Up: 0
   Metric:  10       IP-Internal 11.2.1.24/30        Up: 0
   Metric:  10       IP-Internal 11.2.1.20/30        Up: 0
   Metric:  10       IP-Internal 11.2.1.32/30        Up: 0
   Metric:  10       IP-Internal 11.2.1.28/30        Up: 0
   Metric:  10       IP-Internal 11.2.1.36/30        Up: 0
```

```
   Metric:  10       IS 76:8e:f8:5:58:12. 2
   Metric:  10       IS 76:8e:f8:5:58:12. 3
   Metric:  10       IS 76:8e:f8:5:58:12. 4
   Metric:  10       IS 76:8e:f8:5:58:12. 5
   Metric:  10       IS 76:8e:f8:5:58:12. 6
   Metric:  10       IS 76:8e:f8:5:58:12. 7
…
```

show isis hostname

Displays the router-name-to-system-ID mapping table entries for an IS-IS device.

Syntax

show isis hostname

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example displays sample output from the **show isis hostname** command.

```
device# show isis hostname

Total number of entries in IS-IS Hostname Table: 1
   System ID       Hostname            * = local IS
-----------------------------------------------------
  * 768e.f805.5812  R1
```

show isis interface

Displays information about IS-IS interfaces for a device.

Syntax

show isis interface

show isis interface brief

show isis interface ethernet *slot/port*

show isis interface loopback *number*

show isis interface port-channel *number*

show isis interface ve *vlan_id*

Parameters

brief

Specifies a brief summary of IP interface IS-IS interface information.

ethernet *slot* **/** *port*

Specifies an Ethernet slot and port.

loopback *number*

Specifies a loopback interface. Valid values range from 1 through 255.

port-channel *number*

Specifies a port-channel interface.

ve *vlan_id*

Specifies a virtual Ethernet (VE) interface. Valid values range from 1 through 4096.

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Output

The **show isis interface** command displays the following information:

Output field	Description
Total number of IS-IS interfaces	The number of interfaces on which IS-IS is enabled.
Interface	The interface number to which the information listed below applies.
Circuit State	The state of the circuit, which can be one of the following: • DOWN • UP
Circuit Mode	The IS-IS type in use on the circuit. The mode can be one of the following: • LEVEL-1 • LEVEL-2 • LEVEL-1-2
Circuit Type	The type of IS-IS circuit running on the interface. The circuit type can be one of the following: • BCAST (broadcast). • PTP (Point-to-Point)
Passive State	The passive state determines whether the interface is allowed to form an IS-IS adjacency with the IS at the other end of the circuit. The state can be one of the following: • FALSE - The passive option is disabled. The interface can form an adjacency with the IS at the other end of the link. • TRUE - The passive option is enabled. The interface cannot form an adjacency, but can still advertise itself into the area.
Circuit Number	The ID that the instance of IS-IS running on the interface applied to the circuit between this interface and the interface at the other end of the link.
MTU	The maximum length supported for IS-IS PDUs sent on this interface.
Level-1 Auth-mode	One of the following authentication modes set for Level-1 on the router: • None • md5 • cleartext
Level-2 Auth-mode	One of the following authentication modes set for Level-2 on the router: • None • md5 • cleartext This parameter is not displayed for interfaces that are configured with a Point-to-Point circuit type. This is because separate Level-2 Hello messages are not sent on Point-

Output field	Description
	to-Point interfaces. Consequently, "Hello Interval", "Hello Multiplier", and "Authentication" parameters should always be configured in the Level-1 mode for Point-to-Point interfaces.
Level-1 Metric	The default-metric value that the device inserts in IS-IS Level-1 PDUs for this interface.
Level-1 Priority	The priority of this IS to be elected as the Designated IS for Level-1 in this broadcast network.
Level-1 Hello Interval	The number of seconds the software waits between sending Level-1 hello PDUs to the IS at the other end of the circuit.
Level-1 Hello Multiplier	The number by which the software multiplies the hello interval to calculate the hold time set in Level-1 Hello PDUs sent on the circuit.
Level-1 Designated IS	The NET of the Level-1 Designated IS.
Level-1 DIS Changes	The number of times the NET of the Level-1 Designated IS has changed.
Level-2 Metric	The default-metric value that the device inserts in IS-IS Level-2 PDUs for this interface.
Level-2 Priority	The priority of this IS to be elected as the Designated IS for Level-2 in this broadcast network.
Level-2 Hello Interval	The number of seconds the software waits between sending Level-2 Hello messages to the IS at the other end of the circuit.
Level-2 Hello Multiplier	The number by which the software multiplies the hello interval to calculate the hold time set for Level-2 Hello PDUs sent on this circuit. This parameter is not displayed for interfaces that are configured with a Point-to-Point circuit type. This is because separate Level-2 Hello messages are not sent on Point-to-Point interfaces. Consequently, "Hello Interval", "Hello

Output field	Description
	Multiplier", and "Authentication" parameters should always be configured in the Level-1 mode for Point-to-Point interfaces.
Level-2 Designated IS	The NET of the Level-2 Designated IS.
Level-2 DIS Changes	The number of times the NET of the Level-2 Designated IS has changed.
Next IS-IS LAN Level-1 Hello	Number of seconds before next Level-1 Hello PDU will be transmitted by the device.
Next IS-IS LAN Level-2 Hello	Number of seconds before next Level-2 Hello PDU will be transmitted by the device.
Number of active Level-1 adjacencies	The number of ISs with which this interface has an active Level-1 adjacency.
Number of active Level-2 adjacencies	The number of ISs with which this interface has an active Level-2 adjacency.
Circuit State Changes	The number of times the state of the circuit has changed.
Circuit State Adjacencies Changes	The number of times an adjacency has started or ended on this circuit.
Rejected Adjacencies	The number of adjacency attempts by other ISs rejected by the device.
Circuit Authentication L1 failures	The number of times the device rejected a circuit because the authentication did not match the authentication configured for Level 1 on the device.
Circuit Authentication L2 failures	The number of times the device rejected a circuit because the authentication did not match the authentication configured for Level 2 on the device. This parameter is not displayed for interfaces that are configured with a Point-to-Point circuit type. This is because separate Level-2 Hello messages are not sent on Point-to-Point interfaces. Consequently, "Hello Interval", "Hello Multiplier", and "Authentication" parameters should always be configured in the Level-1 mode for Point-to-Point interfaces.
Bad LSP	The number of times the interface received a bad LSP from an IS at the other end of the circuit. The following conditions can cause an LSP to be bad: • Invalid checksum • Invalid length • Invalid lifetime value
Control Messages Sent	The number of IS-IS control PDUs sent on this interface.
Control Messages Received	The number of IS-IS control PDUs received on this interface.
Hello Padding:	The Hello Padding configuration, which can be: • Enabled • Disabled
IP Enabled	If set to TRUE, the IP protocol is enabled for this circuit.
IP Address and Subnet	The IP address and subnet mask for this interface.

Output field	Description
Mask	
IPv6 Enabled	If set to TRUE, the IPv6 protocol is enabled for this circuit.
IPv6 Address and Subnet Mask	The IPv6 address and subnet mask for this interface.
Ipv6 Link-Local Addresses	The IPv6 link local address for this interface.
MPLS TE Enabled:	If set to TRUE, MPLS Traffic Engineering protocol is enabled for this circuit.
BFD Enabled:	If set to TRUE, BiDirectional Forwarding Detection is enabled for this circuit.

Examples

The following example displays information about IS-IS interfaces for a device.

```
device# show isis interface
Total number of IS-IS Interfaces: 11

Interface: Ve 301
   Circuit State: UP Circuit Mode: Level 1-2
   Circuit Type: BCAST Passive State: FALSE
   Circuit Number: 2, MTU: 1500
   Level-1 Auth-mode: NONE
   Level-2 Auth-mode: NONE
   Level-1 Metric: 10, Level-1 Priority: 64
   Level-1 Hello Interval: 10, Level-1 Hello Multiplier: 3
   Level-1 Designated IS: R1-02 Level-1 DIS Changes: 2
   Level-2 Metric: 10, Level-2 Priority: 64
   Level-2 Hello Interval: 10, Level-2 Hello Multiplier: 3
   Level-2 Designated IS: R1-02 Level-2 DIS Changes: 2
   Next IS-IS LAN Level-2 Hello in 11 seconds
   Number of active Level-2 adjacencies: 0
   Next IS-IS LAN Level-1 Hello in 1 seconds
   Number of active Level-1 adjacencies: 0
   Circuit State Changes: 1 Circuit Adjacencies State Changes: 0
   Rejected Adjacencies: 0
   Circuit Authentication L1 failures: 0
   Circuit Authentication L2 failures: 0
   Bad LSPs: 0
   Control Messages Sent: 7577 Control Messages Received: 0
   Hello Padding: Enabled
   IP Enabled: TRUE
   IP Addresses:
     11.2.1.1/30
   IPv6 Enabled: FALSE
   MPLS TE Enabled: FALSE
   BFD Enabled: FALSE
   LDP-SYNC: Disabled, State:

Interface: Ve 302
   Circuit State: UP Circuit Mode: Level 1-2
   Circuit Type: BCAST Passive State: FALSE
   Circuit Number: 3, MTU: 1500
   Level-1 Auth-mode: NONE
   Level-2 Auth-mode: NONE
```

```
   Level-1 Metric: 10, Level-1 Priority: 64
   Level-1 Hello Interval: 10, Level-1 Hello Multiplier: 3
   Level-1 Designated IS: R1-03 Level-1 DIS Changes: 2
   Level-2 Metric: 10, Level-2 Priority: 64
   Level-2 Hello Interval: 10, Level-2 Hello Multiplier: 3
   Level-2 Designated IS: R1-03 Level-2 DIS Changes: 2
   Next IS-IS LAN Level-2 Hello in 2 seconds
   Number of active Level-2 adjacencies: 0
   Next IS-IS LAN Level-1 Hello in 4 seconds
   Number of active Level-1 adjacencies: 0
   Circuit State Changes: 1 Circuit Adjacencies State Changes: 0
   Rejected Adjacencies: 0
   Circuit Authentication L1 failures: 0
   Circuit Authentication L2 failures: 0
   Bad LSPs: 0
   Control Messages Sent: 7600 Control Messages Received: 0
   Hello Padding: Enabled
   IP Enabled: TRUE
   IP Addresses:
     11.2.1.5/30
   IPv6 Enabled: FALSE
   MPLS TE Enabled: FALSE
   BFD Enabled: FALSE
   LDP-SYNC: Disabled, State:
…
```

The following example displays summarized information about IS-IS interfaces for a device.

```
device# show isis interface brief

Total number of IS-IS Interfaces: 11
Interface       Type  State Mode Passive MTU  UpAdj DIS  StateChg  AdjStateChg
Ve 301          BCAST UP    L12  FALSE   1500 0     None 1         0
Ve 302          BCAST UP    L12  FALSE   1500 0     None 1         0
Ve 303          BCAST UP    L12  FALSE   1500 0     None 1         0
Ve 304          BCAST UP    L12  FALSE   1500 0     None 1         0
Ve 305          BCAST UP    L12  FALSE   1500 0     None 1         0
Ve 306          BCAST UP    L12  FALSE   1500 0     None 1         0
Ve 307          BCAST UP    L12  FALSE   1500 0     None 1         0
Ve 308          BCAST UP    L12  FALSE   1500 0     None 1         0
Ve 309          BCAST UP    L12  FALSE   1500 0     None 1         0
Ve 310          BCAST UP    L12  FALSE   1500 0     None 1         0
Lo 1            BCAST UP    L12  TRUE    0    0     None 1         0
```

show isis neighbors

Displays IS-IS neighbor information.

Syntax

show isis neighbor [**detail**]

Parameters

detail

Specifies detailed information.

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Output

The **show isis neighbors** command displays the following information:

Output field	Description
Total number of IS-IS Neighbors	The number of ISs with which the device has formed IS-IS adjacencies.
System ID	The System ID of the neighbor or the hostname of the neighbor.
Interface	The device port or virtual interface attached to the neighbor.
SNPA	The Subnetwork Point of Attachment (SNPA), which is the MAC address of the device port or virtual interface attached to the neighbor.
State	The state of the adjacency with the neighbor. The state can be one of the following: • DOWN - The adjacency is down. • INIT - The adjacency is being established and is not up yet. • UP - The adjacency is up.
Holdtime	The neighbor's advertised hold time.
Type	The IS-IS type of the adjacency. The type can be one of the following: • ISL1 - Level-1 IS • ISL2 - Level-2 IS • ES - ES **Note:** The device forms a separate adjacency for each IS-IS type. Thus, if the device has both types of IS-IS adjacencies with the neighbor, the display contains a separate row of information for each adjacency.
Pri	The priority of this IS to be elected as the Designated IS in this broadcast network.
StateChgeTime	The amount of time that has passed since the adjacency last changed state.
Protocol	The routing protocol supported by the neighbor. The protocol can be one of the following: • MT-ISIS - Multi-Topology is enabled on the neighbor. • ISIS - Multi-Topology is not enabled on the neighbor.

The **show isis neighbors detail** command displays the following information:

Output field	Description
Total number of IS-IS Neighbors	The number of ISs with which the device has formed IS-IS adjacencies.
System ID	The System ID of the neighbor or the hostname of the neighbor.
Interface	The device port or virtual interface attached to the neighbor.
SNPA	The Subnetwork Point of Attachment (SNPA), which is the MAC address of the device port or virtual interface attached to the neighbor.
State	The state of the adjacency with the neighbor. The state can be one of the following: • DOWN - The adjacency is down. • INIT - The adjacency is being established and is not up yet. • UP - The adjacency is up.
Holdtime	The neighbor's advertised hold time.
Type	The IS-IS type of the adjacency. The type can be one of the following: • ISL1 - Level-1 IS • ISL2 - Level-2 IS • ES - ES **Note:** The device forms a separate adjacency for each IS-IS type. Thus, if the device has both types of IS-IS adjacencies with the neighbor, the display contains a separate row of information for each adjacency.
Pri	The priority of this IS to be elected as the Designated IS in this broadcast network.
StateChgeTime	The amount of time that has passed since the adjacency last changed state.
3-Way Handshake TLV received	The received 3-way handshake TLV for the interface.
Area Address (es)	The address of the area.
Protocols Supported	The topology supported by the neighbor.
IP Address	The IP address assigned to the neighbor interface.
Adj Usage L1	The adjacency level used by the neighbor.
circuit ID	The ID of the IS-IS circuit running on the neighbor interface.
Protocol	The routing protocol supported by the neighbor. The protocol can be one of the following: • MT-ISIS - Multi-Topology is enabled on the neighbor. • ISIS- Multi-Topology is not enabled on the neighbor.

Examples

The following example displays information about IS-IS neighbors.

```
device# show isis neighbors
```

show isis routes

Displays the routes in the IS-IS route table.

Syntax

show isis routes [*ip-address subnet-mask* | *ip-address/prefix*]

Parameters

ip-address subnet-mask

Specifies an IP address and network mask.

ip-address/prefix

Specifies an IP address and prefix.

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Output

The **show isis routes** command displays the following information:

Output field	Description
Total number of IS-IS routes	The total number of routes in the device's IS-IS route table. The total includes Level-1 and Level-2 routes.
Destination	The IP destination of the route.
Mask	The subnet mask for the destination address.
Cost	The IS-IS default metric for the route, which is the cost of using this route to reach the next-hop router to this destination.
Type	The route type, which can be one of the following: • L1 - Level-1 route • L2 - Level-2 route
Tag	The tag value associated with the route.
Path	The path number in the table. The IS-IS route table can contain multiple equal-cost paths to the same destination, in which case the paths are numbered consecutively. When IP load sharing is enabled, the device can load balance traffic to the destination across the multiple paths.
Next Hop IP	The IP address of the next-hop interface to the destination.
Interface	The device interface (port or virtual interface) attached to the next hop.
Flags	Values used by technical support for troubleshooting.

Examples

The following is sample output for the **show isis routes** command when no argument or keyword is used.

```
device# show isis routes
```

show isis spf-log

Displays IS-IS link-state packet (LSP) logging information.

Syntax

show isis spf-log

show isis spf-log detail

show isis spf-log level-1 [**detail**]

show isis spf-log level-2 [**detail**]

Parameters

detail

Specifies detailed information.

level-1

Specifies Level 1 packets only.

level-2

Specifies Level 2 packets only.

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Output

The **show isis spf-log** command displays the following information:

Output field	Description
When	When (in hours: minutes : seconds) a full SPF calculation occurred. The last 20 occurrences are logged.
Duration	The time required to complete this SPF run, Elapsed time is normal clock time (not CPU time). Other options for this field are: • Running - the SPF is still running and the duration will be updated after the SFP has run. • Pending - the event is pending and another SPF will be run once the currently executing SPF has completed.
Nodes	The number of routers and pseudonodes (LANs) that make up the topology calculated in this SPF run.
Count	The number of events that triggered this SPF run. When a topology change has occurred, multiple link-state packets (LSPs) are received in a short time. Since a router waits about 5 seconds before running a full SPF run, it can include all new information. This count includes the number of events (such as receiving new LSPs) that occurred while the router was waiting the 5 second interval before running full SPF.
Last Trigger LSP	When a full SPF calculation is triggered by the arrival of a new LSP, the router stores the LSP ID. The LSP ID can provide a clue about the source of routing instability in an area. If multiple LSPs in a single level are causing SPF runs, only the LSP ID of the last received LSP is recorded.
Triggers	The reason that a full SPF calculations was triggered.
Alternate Route Check	PSPF deleted an IPv4 or IPv6 route. Full SPF must run to find the alternate route.
Route Change in L1 SPF Run	The L1 SPF run added or deleted an IPv4 or IPv6 route. The L2 SPF must run to accommodate this change.
LSP Purged	An LSP was purged. A full SPF calculation must process this change.
LSP Added	A new LSP has appeared in the database. A full SPF calculation is needed to process this new LSP.
Summary Address Change	A summary address configuration change has occurred.
Adjacency State Change	An adjacency was added or deleted.
Admin Distance Change	The administrative distance configuration has changed.
LSP Header Change	The LSP header (attached or overload bits) is changed.
IS Neighbor TLV Change	An IS neighbor TLV was added or deleted in an LSP.
Area Address TLV Change	The area address TLV changed.
Interface IP Address	The IP address configuration changed.

Output field	Description
Change	
IP Address TLV Change	An IP address TLV changed in the LSP.
IPv6 Address TLV Change	An IPv6 address TLV changed in the LSP.
IS-IS Level Change	The IS-IS level configuration changed.
Interface Metric Change	The IS-IS interface metric configuration changed.
LSP Changed - PSPF Disabled	The LSP changed and PSPF is disabled.
LSP Overload Bit Change	The overload bit in the LSP header changed.
Interface State Change	The interface state changed to up or down.
Redist Prefix-List Change	The redistribution list configuration changed.
Redist Policy Change	The redistribution policy configuration changed.
Maximum Path Change	The IS-IS maximum path configuration changed.
IP Load Sharing Change	The IP load sharing configuration changed.
User Cleared IS-IS Route	The user cleared a specific IS-IS route.
User Cleared IS-IS Routes	The user cleared all IS-IS routes.
Neighbor NLPID Change	NLPID set is changed in received hellos.
ISIS Enable	IS-IS was enabled.
ISTCT_SPF Computation	The user issued the **disable-incremental-stct-spf-opt** command.
User Cleared IS-IS All	The user issued the **clear isis all** command.
Interface Config Change	ISIS was enabled or disabled on a port.
User Trigger	The user issued the **clear isis spf-trigger** command.
Recompute InterLeve Routes	The neighbor IS-type is changed either from L1 to L12 or L12 to L1
Exited Overload State	IS-IS exited from an overload condition.

Examples

The following is sample output for the **show isis spf-log** command.

```
device# show isis spf-log
ISIS Level-1 SPF Log
 When      Duration Nodes Count Last-Trigger-LSP         Trigger
  10h34m13s 0ms      1     10    R1.00-00             Interface State Change
  10h34m38s 0ms      1     2     R1.00-00             Interface Config Change
  10h34m43s 0ms      1     18    R1.00-00             Interface Config Change
  10h34m48s 0ms      1     5     R1.00-00             Interface State Change
ISIS Level-2 SPF Log
 When      Duration Nodes Count Last-Trigger-LSP         Trigger
  10h34m13s 0ms      1     10    R1.00-00             Interface State Change
  10h34m38s 0ms      1     2     R1.00-00             Interface Config Change
```

```
  10h34m43s 0ms      1     18    R1.00-00             Interface Config Change
  10h34m48s 0ms      1     5     R1.00-00             Interface State Change
```

The following is sample output for the **show isis spf-log** command when the **detail** keyword is used.

```
device# show isis spf-log detail

ISIS Level-1 SPF Log
 When      Duration Nodes Count Last-Trigger-LSP         Trigger
  12h18m45s 0ms      1     10    R1.00-00             Interface State Change
  Ipv4 Route updates: 0 Ipv6 Route updates: 0
        First Trigger: 12h18m50s Ve 305 State Changed to Up
  12h19m10s 0ms      1     2     R1.00-00             Interface Config Change
  Ipv4 Route updates: 0 Ipv6 Route updates: 0
        First Trigger: 12h19m15s Ve 310 State Changed to Down
  12h19m15s 0ms      1     18    R1.00-00             Interface Config Change
  Ipv4 Route updates: 0 Ipv6 Route updates: 0
        First Trigger: 12h19m18s Ve 301 State Changed to Down
  12h19m20s 0ms      1     5     R1.00-00             Interface State Change
  Ipv4 Route updates: 0 Ipv6 Route updates: 0
        First Trigger: 12h19m25s LSP R1.00-00 Area Address TLV Changed
ISIS Level-2 SPF Log
 When      Duration Nodes Count Last-Trigger-LSP         Trigger
  12h18m45s 0ms      1     10    R1.00-00             Interface State Change
  Ipv4 Route updates: 0 Ipv6 Route updates: 0
        First Trigger: 12h18m50s Ve 305 State Changed to Up
  12h19m10s 0ms      1     2     R1.00-00             Interface Config Change
  Ipv4 Route updates: 0 Ipv6 Route updates: 0
        First Trigger: 12h19m15s Ve 310 State Changed to Down
  12h19m15s 0ms      1     18    R1.00-00             Interface Config Change
  Ipv4 Route updates: 0 Ipv6 Route updates: 0
        First Trigger: 12h19m18s Ve 301 State Changed to Down
  12h19m20s 0ms      1     5     R1.00-00             Interface State Change
…
```

The following is sample output for the **show isis spf-log** command when the **level-1** keyword is used.

```
device# show isis spf-log level-1
ISIS Level-1 SPF Log
 When      Duration Nodes Count Last-Trigger-LSP         Trigger
  12h19m40s 0ms      1     10    R1.00-00             Interface State Change
  12h20m5s 0ms      1     2     R1.00-00             Interface Config Change
  12h20m10s 0ms      1     18    R1.00-00             Interface Config Change
  12h20m15s 0ms      1     5     R1.00-00             Interface State Change
```

show isis traffic

Displays information about IS-IS packet counts.

Syntax

show isis traffic

Modes

Privileged EXEC mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Output

The **show isis traffic** command displays the following information:

Output field	Description
Level-1 Hellos	The number of Level-1 hello PDUs sent and received by the device.
Level-2 Hellos	The number of Level-2 hello PDUs sent and received by the device.
Level-1 LSP	The number of Level-1 link-state PDUs sent and received by the device.
Level-2 LSP	The number of Level-2 link-state PDUs sent and received by the device.
Level-1 CSNP	The number of Level-1 Complete Sequence Number PDUs (CSNPs) sent and received by the device.
Level-2 CSNP	The number of Level-2 CSNPs sent and received by the device.
Level-1 PSNP	The number of Level-1 Partial Sequence Number PDUs (PSNPs) sent and received by the device.
Level-2 PSNP	The number of Level-2 PSNPs sent and received by the device.

Examples

The following is sample output for the **show isis traffic** command.

```
device# show isis traffic

                            Message Received     Message Sent
 Level-1 Hellos             0                    44912
 Level-2 Hellos             0                    44927
 PTP Hellos                 0                    0
 Level-1 LSP                0                    0
 Level-2 LSP                0                    0
 Level-1 CSNP               0                    0
 Level-2 CSNP               0                    0
 Level-1 PSNP               0                    0
 Level-2 PSNP               0                    0
```

show selinux status

This command displays the SE Linux status for this SLX-OS device.

Syntax

show selinux status

Modes

Privilege Execution Mode

Output

The following information is displayed:

Output field	Description
SE Linux status	This field shows whether the SE Linux module is enabled or disabled on the system.
SE Linuxfs mount	This field shows the SE Linux temporary file system mount point.
SE Linux root directory	This field shows the location where all the SE Linux configuration files are stored.
Loaded policy name	This field shows the type of SE Linux policy that is currently loaded.
Current mode	This field shows current active SE Linux mode
Mode from config file	This field shows the mode from the `selinux config file (/etc/selinux/config)`.
Policy MLS status	This field shows the current status of MLS policy, which is enabled by default.
Policy deny_unknown status	This field shows the current status of the `deny_unknown flag` flag in the policy, which is set to allowed by default.
Memory protection checking	This field shows whether SE Linux checks the protection requested by the application or the protection that is applied by the kernel for `mmap` and `mprotect` calls.
Max kernel policy version	This field shows the current version of the SE Linux policy.

Examples

The following example shows the use of this command to view the current SE Linux status.

```
SLX # show selinux status
SE Linux status:                enabled
SE Linuxfs mount:               /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             mls
Current mode:                   permissive
```

```
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      31
```

show system internal bgp evpn nhid

Single NHID with Multiple tunnels for Aliasing scenario.

Examples

The following example shows the single NHID with Multiple tunnels for Aliasing scenario.

```
*** show system internal bgp evpn nhid ***
NHID Tunnel Encap ULabel Ref Installed Status Node ESI-Node
0x71100001 10.10.10.10 VXLAN 0x7c008003 TRUE TRUE Up 0x036edbd0 NA
0x71100002 30.30.30.30 VXLAN 0x7c008004 TRUE TRUE Up 0x036edce0 NA 0x71100003 10.10.10.10
VXLAN 0x7c008003 TRUE TRUE Up 0x036eddf0 0x036ed570 30.30.30.30 VXLAN 0x7c008004 TRUE
TRUE Up 0x036eddf0 0x036ed570 [ECMP]
```

show mac-address-table

Multiple tunnel entries can be present per MAC entry if the MAC is reachable via multiple tunnels.

Examples

The following example shows the multiple tunnel entries can be present per MAC entry if the MAC is reachable via multiple tunnels.

```
sw# show mac-address-table
Type Code - CCL:Cluster Client Local MAC
CCR:Cluster Client Remote MAC
CR:Cluster Remote MAC
VlanId/BDId Mac-address Type State Ports/LIF/PW/T 30 (V) 0010.9400.0102 EVPN Active Tu
32771 (1.1.1.1) Tu 32772 (2.2.2.2)
30 (V) 0010.9400.0202 EVPN Active Tu 32771 (1.1.1.1)
30 (V) 0010.9400.0302 EVPN Active Tu 32771 (1.1.1.1)
```

Following table captures the difference between Simplified MCT and EVPN MH naming convention:

MAC naming in Simplified MCT	Equivalent MAC naming in EVPN-MH
CCL	ES-Local
CCR	ES-Remote
Static-CCL	Static-ESL
Dynamic-CCL	ES-Local
Static-CCR	Static-ESR

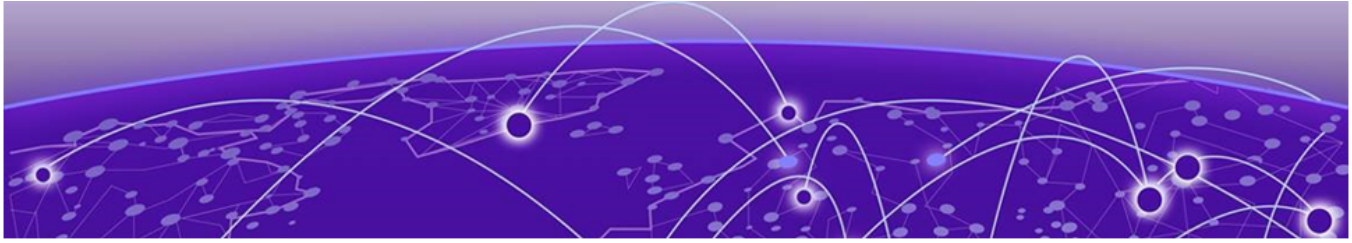
show ip arp suppression-cache

Multiple tunnel entries can be present per ARP.

Examples

The following example shows the multiple tunnel entries can be present per ARP.

```
sw# show ip arp suppression-c
Flags: L - Locally Learnt Adjacency
R - Remote Learnt Adjacency
RS - Remote Static Adjacency
Number of Locally Learnt Adjacency : 0
Number of Remotely Learnt Adjacency: 2794
Vlan/Bd IP Mac Interface Age Flags
-------------------------------------------------------------------------------------------
---------
0001 (B) 20.100.0.1 f46e.959f.2c27 Po 17.1801 Never R 0001 (B) 20.100.0.8 887e.25d3.180b
Tu 32771 (1.89.0.2) Never RS Tu 32775 (1.89.0.5)
```



Show J through Show Z

show lacp on page 2130
show license on page 2131
show link-oam info on page 2133
show link-oam info detail on page 2134
show link-oam statistics on page 2136
show link-oam statistics detail on page 2137
show lldp on page 2139
show lldp interface on page 2140
show lldp neighbors on page 2142
show lldp statistics on page 2145
show loop-detection on page 2146
show mac-address-table on page 2149
show management-heartbeat manager on page 2150
show media on page 2151
show media interface on page 2152
show media optical-monitoring interface on page 2155
show media tunable-optic-sfpp on page 2158
show monitor on page 2160
show mpls autobw-template on page 2162
show mpls autobw-threshold-table on page 2163
show mpls bypass-lsp on page 2164
show mpls dynamic-bypass interface on page 2167
show mpls interface on page 2168
show mpls ldp on page 2169
show mpls lsp on page 2172
show mpls policy on page 2180
show mpls rsvp on page 2181
show mpls rsvp interface on page 2183
show mpls rsvp session on page 2186
show mpls statistics on page 2194
show mpls te database on page 2197
show mvrp on page 2199
show mvrp attributes on page 2200
show mvrp interface on page 2202

show mvrp statistics on page 2204
show netconf on page 2206
show netconf capabilities on page 2207
show notification stream on page 2208
show ntp status on page 2209
show ntp status association detail on page 2210
show ntp status associations on page 2212
show overlay-gateway on page 2214
show onieversion on page 2216
show policy-map on page 2217
show port-channel on page 2221
show port-channel load-balance on page 2223
show port port-channel ethernet on page 2225
show port-security on page 2226
show process cpu on page 2229
show process info on page 2231
show process memory on page 2232
show qos cpu cfg on page 2234
show qos cpu info on page 2237
show qos flowcontrol interface on page 2238
show qos interface all on page 2240
show qos interface on page 2244
show qos interface port-channel on page 2247
show qos interface ve on page 2254
show qos maps on page 2256
show qos maps cos-mutation on page 2259
show qos maps cos-traffic-class on page 2261
show qos maps dscp-cos on page 2262
show qos maps dscp-mutation on page 2263
show qos maps dscp-traffic-class on page 2264
show qos maps traffic-class-cos on page 2266
show qos maps traffic-class-dscp on page 2267
show qos-mpls maps dscp-exp on page 2268
show qos-mpls maps exp-dscp on page 2269
show qos-mpls maps exp-traffic-class on page 2270
show qos tx-queue interface on page 2271
show rmon on page 2272
show rmon history on page 2274
show remote-attestation on page 2275
show rollback checkpoint on page 2276
show rollback diff checkpoint on page 2278
show rollback feature-status on page 2279

show rollback log on page 2280
show rollback patch checkpoint on page 2281
show rollback status on page 2282
show route-map on page 2284
show run router mpls cspf-group on page 2287
show running-config on page 2288
show running-config aaa on page 2289
show running-config aaa accounting on page 2290
show running-config aaa authorization on page 2291
show running-config aaa authorization command on page 2292
show running-config access-list overlay type vxlan on page 2293
show running-config arp on page 2294
show running-config control-plan ip subnet-rate-limit on page 2296
show running-config dpod on page 2297
show running-config event-handler on page 2298
show running-config ip access-list on page 2300
show running-config ip receive on page 2301
show running-config ipv6 on page 2302
show running-config ipv6 access-list on page 2304
show running-config keychain on page 2305
show running-config lag hash on page 2306
show running-config ldap-server on page 2308
show running-config mac access-list on page 2309
show running-config password-attributes on page 2310
show running-config radius-server on page 2312
show running-config rmon on page 2313
show running-config role on page 2314
show running-config rule on page 2315
show running-config sflow on page 2317
show running-config ssh on page 2318
show running-config ssh server on page 2319
show running-config ssh server key-exchange on page 2321
show running-config system-monitor on page 2322
show running-config telemetry collector on page 2324
show running-config telemetry profile on page 2325
show running-config telemetry profile (MPLS) on page 2327
show running-config telemetry profile (queue) on page 2329
show running-config telemetry server on page 2331
show running-config username on page 2332
show sflow on page 2334
show span path session on page 2336
show spanning-tree on page 2337

show ssh client status on page 2339
show ssh server status on page 2340
show startup-config on page 2341
show statistics access-list on page 2342
show statistics access-list overlay type vxlan on page 2346
show statistics bridge-domain on page 2347
show statistics vlan on page 2349
show statistics vpn on page 2351
show storm-control on page 2352
show support on page 2354
show system maintenance on page 2355
show system maintenance rate-monitoring on page 2356
show system monitor tm on page 2357
show tech-support on page 2358
show telemetry client-cert on page 2361
show telemetry collector name on page 2362
show telemetry collector summary on page 2363
show telemetry server status on page 2364
show telnet server status on page 2365
show threshold monitor on page 2366
show threshold monitor ecmp on page 2368
show threshold monitor host on page 2369
show threshold monitor nexthop on page 2371
show threshold monitor route on page 2373
show threshold monitor sfp on page 2375
show tm voq-stat ingress-device all discards on page 2378
show tm voq-stat ingress-device all egress-port ethernet on page 2380
show tm voq-stat ingress-device all max-buffer-util on page 2382
show tm voq-stat ingress-device all max-queue-depth on page 2383
show tm voq-stat ingress-device ethernet on page 2385
show tm voq-stat slot on page 2388
show topology-group on page 2390
show tpm on page 2391
show tpvm on page 2393
show tpvm config on page 2396
show tpvm config password-policy on page 2398
show tunnel on page 2400
show udld on page 2402
show udld interface on page 2403
show udld statistics on page 2405
show users on page 2406
show version on page 2407

show vlan brief on page 2409
show vlan detail on page 2411
show vrf on page 2412
show vrrp on page 2415
show ztp status on page 2420

show lacp

Displays Link Aggregation Control Protocol (LACP) statistics.

Syntax

show lacp { **counter** [*port-channel*] | **sys-id** }

Parameters

counter

Displays LACP statistics for all port-channel interfaces.
port-channel

Displays counters for a specified port channel interface.

sys-id

Displays LACP statistics by system ID.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the LACP statistics for each port-channel interface for all port-channel interfaces or a single port-channel interface, or by system ID.

Examples

The following example displays the local system ID:

```
device# show lacp sys-id

% System 8000,00-05-1e-76-1a-a6
```

show license

Displays license information.

Syntax

show license [**eula** | **id**]

Command Default

Displays the licenses installed on the device.

Parameters

eula

Specifies the EULA statement.

id

Specifies the license ID and information.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display general license information, the license ID, and the EULA text.

The EULA text can be displayed using the **show license eula** command.

Examples

The following example displays the EULA text.

```
device# show license eula
Use of the features enabled via the "license eula accept" CLI requires a license to
be purchased within 30 days. By accepting the EULA you indicate that you
have read and accept the Extreme End User License Agreement found at the following URL.
[https://learn.extremenetworks.com/rs/641-VMV-602/images/Extreme-Networks-End-User-
License-Agreement.pdf].
```

The following example displays the SAU license when the EULA is accepted.

```
device# show license
Chassis:
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Advanced Features license
Feature name:ADVANCED_FEATURES
License is Trust Based
```

```
EULA acceptance date: Thu Nov 24 23:58:11 2016
```

The following example displays the device license ID.

```
device# show license id
LocationLicense ID
================================================
Chassis10:00:00:05:1E:38:7F:CE
```

show link-oam info

Displays the link OAM information.

Syntax

show link-oam info

Modes

Privileged EXEC mode

Output

The **show link-oam info** command displays the following information:

Output field	Description
Ethernet Port	Indicates the ethernet port where the EFM-OAM is enabled.
Link Status	Indicates whether the physical link is operational (up) or has any fault (down).
OAM Status	Indicates the status of OAM on the link between the local and remote DTEs. The status is enabled if the OAM client is satisfied with the local and remote settings.
Mode	Indicates whether the DTE is in active or passive modes. Active DTEs can start the discovery process and passive DTEs can only respond.
Local Stable	Indicates the reception of the remote DTE state information and is satisfied with the remote OAM settings.
Remote Stable	Indicates the reception of the local DTE state information at the remote DTE and is satisfied with the local OAM settings.

Examples

The following example displays sample output from the **show link-oam info** command.

```
device#show link-oam info
Ethernet Link Status     OAM Status      Mode       Local Stable    Remote Stable
1/1      up              up              active     satisfied       satisfied
1/2      up              up              passive    satisfied       satisfied
1/3      up              up              active     satisfied       satisfied
1/4      up              init            passive    unsatisfied     unsatisfied
1/5      down            down            passive    unsatisfied     unsatisfied
1/6      down            down            passive    unsatisfied     unsatisfied
1/7      down            down            passive    unsatisfied     unsatisfied
```

show link-oam info detail

Displays the detailed dump of the link OAM internal state for all ports.

Syntax

show link-oam info detail

Modes

Privileged EXEC mode

Output

The **show link-oam info detail** command displays the following information:

Output field	Description
Local information	Displays the local information.
Remote information	Displays the remote information.

Examples

This example displays the detailed dump of Link OAM statistics for all ports:

```
device# show link-oam info detail
OAM information for Ethernet port: 2/1
        +link-oam mode:        active
        +link status:          up
        +oam status:           init
        Local information
                multiplexer action:  forward
                parse action:        forward
                stable:              unsatisfied
                state:               activeSend
                dying-gasp:          false
                critical-event:      false
                link-fault:          false
        Remote information
                multiplexer action:  forward
                parse action:        forward
                stable:              unsatisfied
                dying-gasp:          false
                critical-event:      false
                link-fault:          false

OAM information for Ethernet port: 2/2
        +link-oam mode:        passive
        +link status:          down
        +oam status:           init
        Local information
                multiplexer action:  forward
                parse action:        forward
                stable:              unsatisfied
                state:               down
                dying-gasp:          false
```

```
                critical-event:      false
                link-fault:          false
        Remote information
                multiplexer action:  forward
                parse action:        forward
                stable:              unsatisfied
                dying-gasp:          false
                critical-event:      false
                link-fault:          false
```

show link-oam statistics

Display the link OAM statistics.

Syntax

show link-oam statistics

Modes

Privileged EXEC mode

Output

The **show link-oam statistics** command displays the following information:

Output field	Description
Ethernet Port	Indicates the ethernet port where the EFM-OAM is enabled.
Tx PDUs	Indicates the number of PDUs transmitted.
Rx PDUs	Indicates the number of PDUs received.

Examples

The following example displays sample output from the **show link-oam statistics** command.

```
device# show link-oam statistics
Ethernet Tx PDUs    Rx PDUs
2/1          93          92
2/2             45          46
```

show link-oam statistics detail

Displays the detailed dump of Link OAM statistics for all ports.

Syntax

show link-oam statistics detail

Modes

Privileged EXEC mode

Output

The **show link-oam statistics detail** command displays the following information:

Output field	Description
Tx statistics	Details the data transmitted.
Rx statistics	Details the date received.

Examples

This example displays the detailed dump of Link OAM statistics for all ports:

```
device# show link-oam statistics detail
OAM statistics for Ethernet port: 1/1
        Tx statistics
                information OAMPDUs:                    587
                loopback control OAMPDUs:               0
                variable request OAMPDUs:               0
                variable response OAMPDUs:              0
                unique event notification OAMPDUs:      0
                duplicate event notification OAMPDUs:   0
                organization specific OAMPDUs:          0
                link-fault records:                     0
                critical-event records:                 0
                dying-gasp records:                     0
        Rx statistics
                information OAMPDUs:                    442
                loopback control OAMPDUs:               0
                variable request OAMPDUs:               0
                variable response OAMPDUs:              0
                unique event notification OAMPDUs:      0
                duplicate event notification OAMPDUs:   0
                organization specific OAMPDUs:          0
                unsupported OAMPDUs:                    0
                link-fault records:                     0
                critical-event records:                 0
                dying-gasp records:                     0
                discarded TLVs:                         0
                unrecognized TLVs:                      0
OAM statistics for Ethernet port: 1/2
        Tx statistics
                information OAMPDUs:                    440
                loopback control OAMPDUs:               0
```

```
                variable request OAMPDUs:              0
                variable response OAMPDUs:             0
                unique event notification OAMPDUs:     0
                duplicate event notification OAMPDUs:  0
                organization specific OAMPDUs:         0
                link-fault records:                    0
                critical-event records:                0
                dying-gasp records:                    0
        Rx statistics
                information OAMPDUs:                   441
                loopback control OAMPDUs:              0
                variable request OAMPDUs:              0
                variable response OAMPDUs:             0
                unique event notification OAMPDUs:     0
                duplicate event notification OAMPDUs:  0
                organization specific OAMPDUs:         0
                unsupported OAMPDUs:                   0
                link-fault records:                    0
                critical-event records:                0
                dying-gasp records:                    0
                discarded TLVs:                        0
                unrecognized TLVs:                     0
```

show lldp

Displays Link Layer Discovery Protocol (LLDP) configuration information.

Syntax

show lldp

Modes

Privileged EXEC mode

Examples

The following example displays LLDP configuration information.

```
device# show lldp

LLDP Global Information
  system-name: SLX
  system-description: Extreme SLX9540 Switch/Router
  description:
  State:                    Enabled
  Mode:                     Receive/Transmit
  Advertise transmitted:    30 seconds
  Hold time for advertise: 120 seconds
  Tx Delay Timer:           1 seconds
  Transmit TLVs:            Chassis ID              Port ID
                            TTL                     Port Description
                            System Name             IEEE DCBx
                            BGP Auto NBR
  DCBx iSCSI Priority Values: none
```

show lldp interface

Displays the LLDP status on the specified interface.

Syntax

show lldp interface [**ethernet** *slot/port*]

Parameters

ethernet

Use this parameter to specify an Ethernet interface, followed by the slot or port number. For devices that do not support line cards, specify 0 for the slot.

slot

Specifies a valid slot number. 0 is the only valid entry.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

If the **ethernet** *slot/port* parameter is not specified, this command displays the LLDP status information received on all the interfaces.

Examples

To display all the LLDP ethernet interface information, enter the following:

```
device# show lldp interface ethernet ?
Description: The list of Ethernet interfaces.
Possible completions:
  0/1
  0/2
  0/3
  0/4
  0/5
  0/6
  0/8
  0/9
  0/10
  0/11
  0/12
  0/13
  0/14
  0/15
  0/16
  0/17
  0/18
```

```
  0/19
  0/20
  0/21
  0/22
  0/23
```

To display the LLDP interface information for a specified ethernet interface, enter the following:

```
device# show lldp interface ethernet 1/18
LLDP information for Eth 1/18
  State:                   Enabled
  Mode:                    Receive/Transmit
  Advertise Transmitted:   30 seconds
  Hold time for advertise: 120 seconds
  Tx Delay Timer:          1 seconds
  Transmit TLVs:           Chassis ID              Port ID
                           TTL                     Port Description
                           System Name
```

show lldp neighbors

Displays Link Layer Discovery Protocol (LLDP) Type Length Value (TLV) information for all neighboring devices on a specific interface.

Syntax

show lldp neighbors interface ethernet *slot/port* [**detail**]

Parameters

interface ethernet

Causes the display of LLDP information about an Ethernet interface.

slot

Specifies a valid slot number. Must be 0 if the switch does not contain slots.

port

Specifies a valid port number.

detail

Specifies the display of detailed LLDP neighbor information.

Modes

Privileged EXEC mode

Examples

The following example shows how to display LLDP neighbor information for a specific interface (Ethernet 0/18).

```
device# show lldp neighbors interface ethernet 1/18
Local Port  Dead Interval  Remaining Life  Remote Port ID   Remote Port Descr Chassis
ID       Tx  Rx   System Name
Eth 1/18      120            115             Ethernet 2/25    Eth 2/25
768e.f807.6000   655 654  SLX
```

The following example displays detailed LLDP neighbor information for a specific interface (Ethernet 0/18).

```
device# show lldp neighbors interface ethernet 0/18 detail

Neighbors for Interface Eth 0/18

MANDATORY TLVs
==============
Local Interface: Eth 0/18  (Local Interface MAC: 768e.f805.5816)
Remote Interface: Ethernet 0/25 (Remote Interface MAC: 768e.f807.610d)
Dead Interval: 120 secs
Remaining Life : 118 secs
Chassis ID: 768e.f807.6000
LLDP PDU Transmitted: 656  Received: 655

OPTIONAL TLVs
```

```
==============
Port Interface Description: Eth 0/25
System Name: SLX

DCBX TLVs
===========

BGP Auto NBR TLV
============
Remote AS number: 2250
Remote peer address: 10.5.5.2
```

This example displays the LLDP neighbors and their details.

```
device(config-cee-map-default)# do show lldp neighbors
Local Port    Dead Interval  Remaining Life  Remote Port ID                  Remote
Port Descr                 Chassis ID       Tx           Rx           System Name
Eth 0/33      120            111             Ethernet 0/33                   Eth
0/33                          d8c4.9780.f41c   10           10           NH-Leaf2

Total no. of Records: 1

device(config-cee-map-default)# do show lldp neighbors detail
Neighbors for Interface Eth 0/33

MANDATORY TLVs
===============
Local Interface: Eth 0/33  (Local Interface MAC: d8c4.9780.f53d)
Remote Interface: Ethernet 0/33 (Remote Interface MAC: d8c4.9780.f43e)
Dead Interval: 120 secs
Remaining Life : 105 secs
Chassis ID: d8c4.9780.f41c
LLDP PDU Transmitted: 10  Received: 10

OPTIONAL TLVs
==============
Port Interface Description: Eth 0/33
System Name: NH-Leaf2
Remote Protocols Advertised:  Link Aggregation
Remote VLANs Configured:
      VLAN ID:    1  VLAN Name: default
      VLAN ID:    5  VLAN Name: VLAN0005
      VLAN ID:   10  VLAN Name: VLAN0010
      VLAN ID:   50  VLAN Name: VLAN0050
      VLAN ID:  500  VLAN Name: VLAN0500
Port Vlan Id: 1
Port & Protocol Vlan Flag: Supported,  Not enabled
Port & Protocol Vlan Id: 0

DCBX TLVs
===========
Version : CEE
DCBX Ctrl OperVersion: 0  MaxVersion: 0  SeqNo: 2 AckNo: 2
DCBX ETS OperVersion: 0  MaxVersion: 0  Enabled: 1  Willing: 0 Error: 0
Enhanced Transmission Selection (ETS)
  Priority-Group ID Map:
    Priority : 0  1  2  3  4  5  6  7
    Group ID : 0  0  0  0  0  0  0  0
  Group ID Bandwidth Map:
    Group ID  :   0   1   2   3   4   5   6   7
    Percentage:   0   0   0   0   0   0   0   0
    Number of Traffic Classes supported: 8
DCBX PFC OperVersion: 0  MaxVersion: 0  Enabled: 1  Willing: 0 Error: 0
```

```
Priority-based Flow Control (PFC)
     Enabled Priorities: none
     Number of Traffic Class PFC supported: 8
LAN LLS OperVersion: 0  MaxVersion: 0  Enabled: 1  Willing: 0 Error: 0
LAN  Logic Link Status: Up


8021 DCBX TLVs
==============
Version : IEEE 8021
8021 ETS Recommendation:

Enhanced Transmission Selection (ETS)
  Priority-Group ID Map:
    Priority : 0  1  2  3  4  5  6  7
    Group ID : 0  0  0  0  0  0  0  0
  Group ID Bandwidth Map:
    Group ID  :   0   1   2   3   4   5   6   7
    Percentage:   0   0   0   0   0   0   0   0
    Number of Traffic Classes supported: 8

  TSA Assignment Map:
    Group ID  :   0   1   2   3   4   5   6   7
    TSA   :       2   2   2   2   2   2   2   2

8021 PFC configuration Willing: 0 MBC: 0
Priority-based Flow Control (PFC)
     Enabled Priorities: none
     Number of Traffic Class PFC supported: 8

Link Aggregation Capability: Capable
Link Aggregation Status: Enabled
Link Aggregation Port Id: 671088650
```

show lldp statistics

Displays the LLDP statistics on all interfaces or a specified interface.

Syntax

show lldp statistics [**interface** [**ethernet***slot/port*]]

Parameters

ethernet

Use this parameter to specify an Ethernet interface, followed by the slot or port number. For devices that do not support line cards, specify 0 for the slot.

slot

Specifies a slot number. 0 is the only valid entry.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

If you do not specify an interface, this command displays the LLDP statistics for all interfaces.

Examples

To display LLDP statistics on the specified interface:

```
device# show lldp statistics interface ethernet 0/18
LLDP Interface statistics for Eth 0/18
Frames transmitted: 659
Frames Aged out:    0
Frames Discarded:   0
Frames with Error:  0
Frames Recieved:    657
TLVs discarded:     0
TLVs unrecognized:  0
```

show loop-detection

Displays loop detection (LD) information at the system, interface (Ethernet or port-channel), or VLAN VXLAN tunnel level.

Syntax

show loop-detection [**disabled-ports** | **globals** | **interface** { **ethernet** *interface* | **port-channel** *interface* } | **vlan** *VLAN_ID*]

show loop-detection [**disabled-ports** | **globals** | **interface** { **ethernet** *interface* | **port-channel** *interface* } | **vlan** *VLAN_ID* | **bridge-domain** *BD-ID*]

Parameters

disabled-ports

Displays the ports that are disabled by LD.

globals

Displays global LD configuration values.

interface

Specifies an Ethernet or port-channel interface.

ethernet*interface*

Specifies an Ethernet interface.

port-channel*interface*

Specifies a port-channel interface.

vlan*VLAN_ID*

Specifies a VLAN.

bridge-domain*BD_ID*

Specifies a bridge domain.

Modes

Privileged EXEC mode

Examples

The following example displays LD information at the system level.

```
device# show loop-detection
Strict Mode:
------------------------

Number of loop-detection instances enabled: 1

Interface: eth 0/6
        Enabled on VLANs: 100
        Shutdown Disable:   No
```

```
        Interface status: UP
        Auto enable in: Never

Packet Statistics:
vlan            sent            rcvd        disable-count
100             100             0           0

Loose Mode:
------------------------

Number of LD instances:   2
Disabled Ports:                   0/7

Packet Statistics:
vlan            sent            rcvd        disable-count
100             100             0           0
```

The following example displays ports disabled by LD.

```
device# show loop-detection disabled-ports
Ports disabled by loop detection
-----------------------------------------
port       age(min)       disable cause
0/6        5              Disabled by Self
```

The following example displays global LD configuration values.

```
device# show loop-detection globals
Loop Detection:                 Disabled
Shutdown-time (minutes):        0
Hello-time (msec):              1000
Raslog-duration (minutes):      10
```

The following example displays LD configuration values for an Ethernet interface.

```
device# show loop-detection interface ethernet 0/6
Number of LD instances:  1
Enabled on VLANs:        100
Shutdown Disable:        No
Interface status:        UP
Auto enable in:          Never

Packet Statistics:
vlan            sent            rcvd        disable-count
100             100             0           0
```

The following example displays LD configuration values, including logical interfaces (LIFs), for a VLAN VXLAN tunnel.

```
device# show loop-detection vlan 20
Number of LD instances: 1
LIF (Logical Interface) Disabled on Ports: eth0/2,VxLAN Tunnel 61441

Packet Statistics:
vlan            sent            rcvd
20              44225           2
```

The following example displays LD configuration values for a VLAN VXLAN tunnel if LD shutdown is disabled.

```
device# show loop-detection vlan 20
Number of LD instances: 1
LIF (Logical Interface) ShutDown is disabled for VLAN 20

Packet Statistics:
vlan            sent            rcvd
20              10              10
```

The following example displays LD configuration values for a BD VXLAN tunnel.

```
device# show loop-detection bridge-domain 8
Number of LD instances:   1
LIF (Logical Interface) Disabled on Ports: eth0/2…

Packet Statistics:
BD            sent            rcvd
8             100             1
```

show mac-address-table

Multiple tunnel entries can be present per MAC entry if the MAC is reachable via multiple tunnels.

Examples

The following example shows the multiple tunnel entries can be present per MAC entry if the MAC is reachable via multiple tunnels.

```
sw# show mac-address-table
Type Code - CCL:Cluster Client Local MAC
CCR:Cluster Client Remote MAC
CR:Cluster Remote MAC
VlanId/BDId Mac-address Type State Ports/LIF/PW/T 30 (V) 0010.9400.0102 EVPN Active Tu
32771 (1.1.1.1) Tu 32772 (2.2.2.2)
30 (V) 0010.9400.0202 EVPN Active Tu 32771 (1.1.1.1)
30 (V) 0010.9400.0302 EVPN Active Tu 32771 (1.1.1.1)
```

Following table captures the difference between Simplified MCT and EVPN MH naming convention:

MAC naming in Simplified MCT	Equivalent MAC naming in EVPN-MH
CCL	ES-Local
CCR	ES-Remote
Static-CCL	Static-ESL
Dynamic-CCL	ES-Local
Static-CCR	Static-ESR

show management-heartbeat manager

Displays the current configuration state of the Management Heartbeat mode.

Syntax

show management-heartbeat manager

Modes

Management Heartbeat mode

Examples

To display the current state of the Management Heartbeat mode, use the following command:

```
SLX(config-management-heartbeat-manage) # show management-heartbeat manager

Admin state: up
Operational state: up
Threshold time: 30 minutes
Action: Maintenance mode enable
Time to last heartbeat: 4 minutes
```

show media

Displays the SFP information for all the interfaces present on a device.

Syntax

show media

Modes

Privileged EXEC mode

Usage Guidelines

The command output will be several pages long.

Examples

To display all SFP information, use the following command:

```
device# show media
  Ethernet 0/1
  Identifier     3    SFP
  Connector      7    LC
  Transceiver    0000000000000010 10_GB/s
  Name           id
  Encoding       6
  Baud Rate      103 (units 100 megabaud)
  Length 9u      0   (units km)
  Length 9u      0   (units 100 meters)
  Length 50u     8   (units 10 meters)
  Length 62.5u   3   (units 10 meters)
  Length Cu      0   (units 1 meter)
  Vendor Name    EXTREME
  Vendor OUI     42:52:4f
  Vendor PN      57-0000075-01
  Vendor Rev     A
  Wavelength     850 (units nm)
  Options        001a Loss_of_Sig,Tx_Fault,Tx_Disable
  BR Max         0
  BR Min         0
  Serial No      AAA108454100431
  Date Code      081108
  Optical Monitor yes
  Temperature    44 Centigrade
  Voltage        3246.8  (Volts)
  Current        0.002  (mAmps)
  TX Power       0.1  (uWatts)
  RX Power       0.1  (uWatts)
(Output truncated)
```

show media interface

Displays the SFP information for a specific interface.

Syntax

show media interface [**ethernet** *slot* / *port*]

Parameters

ethernet

Specifies a physical Ethernet interface.

slot

Specifies a valid slot number. For devices that do not support line cards, specify **0**.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

The command shows if values for *Temperature*, *Voltage*, *Current*, *TX Power*, and *RX Power* have reached threshold limits. The displayed thresholds are *High-Alrm*, *High-Warn*, *Low-Alrm*, or *Low-Warn*.

The *show media interface* command also shows the *TX Power* for all physical interfaces. This information is not displayed for Optics.

Examples

To display SFP information on individual interfaces, use the following command.

```
SLX# show media interface ethernet 0/21
  Interface              Ethernet 0/21
  Identifier             3    SFP
  Connector              7    LC
  Transceiver            0000000000000010 10_GB/s
  Extended Transceiver   0
  Name                   sw
  Encoding               6
  Baud Rate              103 (units 100 megabaud)
  Length 9u              0   (units km)
  Length 9u              0   (units 100 meters)
  Length 50u             8   (units 10 meters)
  Length 62.5u           3   (units 10 meters)
  Length Cu              0   (units 1 meter)
  Vendor Name            EXTREME NETWORKS
  Vendor OUI             00:05:1e
  Vendor PN              57-0000075-01    (10GE SR SFP+)
  Vendor Rev             A
```

```
  Wavelength             850 (units nm)
  Options                001a
  BR Max                 0
  BR Min                 0
  Serial No              AAF315370000GD2
  Date Code              150908
  Optical Monitor        Yes
  Temperature            16 Centigrade                    Normal
  Voltage                3396.6  (mVolts)                 Normal
  Current                0.110  (mAmps)                   Low-Alrm
  TX Power               11.8  (uWatts) / -19.281 (dBm)   Low-Alrm
  RX Power               610.5  (uWatts) / -2.143 (dBm)   Normal


SLX# show media interface ethernet 0/55
  Interface      Ethernet 0/55
  Identifier     13   QSFPP
  Connector      7    LC
  Transceiver            0000000000000002 40_GB/s  Long_dist
  Extended Transceiver   0
  Name           lw
  Encoding       5    IEEE 802.3ba
  Baud Rate      103 (units 100 megabaud)
  Length 9u      10  (units km)
  Length E-50u   0   (units 2 meters)
  Length 50u     0   (units 1 meters)
  Length 62.5u   0   (units 1 meters)
  Length Cu      0   (units 1 meter)
  Vendor Name    EXTREME NETWORKS
  Vendor OUI     d8:84:66
  Vendor PN      EQPT404LR4LCL100 ()
  Vendor Rev     AA
  Wavelength     26020(units 0.05 nm)
  Options        0000
  BR Max         12
  BR Min         210
  Serial No      2035P-00071
  Date Code      200826
  Optical Monitor Yes
  Temperature    23 Centigrade                     Normal
  Voltage        3334.5  (mVolts)                 Normal
  Current (Agg)  179.686  (mAmps)         High-Alarm
  TX Power (Agg) 4220.8  (uWatts) / 6.254 (dBm)  High-Alarm
  RX Power (Agg) 3944.5  (uWatts) / 5.960 (dBm)  High-Alarm
  Channel [0]:
  Current        22.804  (mAmps)
  TX Power       999.4  (uWatts) / -0.003 (dBm)
  RX Power       969.1  (uWatts) / -0.136 (dBm)
  Channel [1]:
  Current        58.480  (mAmps)
  TX Power       972.4  (uWatts) / -0.122 (dBm)
  RX Power       995.5  (uWatts) / -0.020 (dBm)
  Channel [2]:
  Current        54.228  (mAmps)
  TX Power       984.0  (uWatts) / -0.070 (dBm)
  RX Power       651.5  (uWatts) / -1.861 (dBm)
  Channel [3]:
  Current        44.174  (mAmps)
  TX Power       1265.0  (uWatts) / 1.021 (dBm)
  RX Power       1328.4  (uWatts) / 1.233 (dBm)

SLX# show media interface ethernet 0/31
  Interface      Ethernet 0/31
  Identifier     13   QSFPP
```

```
Connector      12   MPO Parallel Optic
Transceiver            0000000000000004 40_GB/s  Short_dist
Extended Transceiver   0
Name           sw
Encoding       5    IEEE 802.3ba
Baud Rate      103 (units 100 megabaud)
Length 9u      0   (units km)
Length E-50u   50  (units 2 meters)
Length 50u     0   (units 1 meters)
Length 62.5u   0   (units 1 meters)
Length Cu      0   (units 1 meter)
Vendor Name    BROCADE
Vendor OUI     00:05:1e
Vendor PN      57-1000129-01    (40GE QSFP+ SR4 INT)
Vendor Rev     A
Wavelength     17000(units 0.05 nm)
Options        0000
BR Max         15
BR Min         222
Serial No      ATA315341000993
Date Code      150820
Optical Monitor Yes
Temperature    31 Centigrade                    Normal
Voltage        3271.0  (mVolts)                Normal
Current (Agg)  19.616  (mAmps)        High-Alarm
TX Power (Agg) N/A (null)                     N/A
RX Power (Agg) 1973.3  (uWatts) / 2.952 (dBm)  High-Warn
Channel [0]:
Current        5.232  (mAmps)
TX Power       Not Supported
RX Power       461.6  (uWatts) / -3.357 (dBm)
Channel [1]:
Current        5.090  (mAmps)
TX Power       Not Supported
RX Power       507.3  (uWatts) / -2.947 (dBm)
Channel [2]:
Current        4.694  (mAmps)
TX Power       Not Supported
RX Power       507.8  (uWatts) / -2.943 (dBm)
Channel [3]:
Current        4.600  (mAmps)
TX Power       Not Supported
RX Power       496.6  (uWatts) / -3.040 (dBm)
```

show media optical-monitoring interface

Displays the optical monitored information for a specific interface.

Syntax

show media optical-monitoring interface [**ethernet** *slot / port*]

Parameters

ethernet

Specifies a physical Ethernet interface.

slot

Specifies a valid slot number. For devices that do not support line cards, specify **0**.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

The command shows if values for *Temperature*, *Voltage*, *Current*, *TX Power*, and *RX Power* have reached threshold limits. The displayed thresholds are *High-Alrm*, *High-Warn*, *Low-Alrm*, or *Low-Warn*.

Examples

To display the global optical monitoring configuration:

```
 SLX# show media optical-monitoring
N/A - Not Available.
Port        Optical    Frequency Wavelength Module      Supply
Channel                     Bias      Channel
            Monitoring Error     Error      Temperature Voltage    TX
Power                     Current   RX Power
            Support    ( GHz )   ( nm )     ( C )       ( mVolts ) ( uWatts /
dBm )            ( mAmps ) ( uWatts / dBm )
=========== ========== ========= ========== =========== ==========
=========================== ========= =================
Et 0/20     YES        0.0       0.000      18          3370.8     23.4 /
-16.308              0.148     596.8 / -2.242
                                           Normal      Normal     Low-
Alrm                   Low-Alrm   Normal

Et 0/21     YES        0.0       0.000      16          3395.1     12.2 /
-19.136              0.104     612.1 / -2.132
                                           Normal      Normal     Low-
Alrm                   Low-Alrm   Normal

Et 0/31     YES        0.0       0.000      17          3366.7     50.6 /
-12.958              0.258     0.0 / -inf
```

```
                                          Normal      Normal     Low-
Alrm                  Low-Alrm   Low-Alrm

Et 0/34     YES        0.0       0.000      19          3369.5     57.9 /
-12.373             0.270     508.5 / -2.937
                                          Normal      Normal     Low-
Alrm                  Low-Alrm   Normal

Et 0/35     YES        0.0       0.000      20          3352.7     0.1 /
-40.000              0.002     519.2 / -2.847
                                          Normal      Normal     Low-
Alrm                  Low-Alrm   Normal

Et 0/37     YES        0.0       0.000      19          3347.9     0.1 /
-40.000              0.002     0.4 / -33.979
                                          Normal      Normal     Low-
Alrm                  Low-Alrm   Low-Alrm

Et 0/38     YES        0.0       0.000      20          3349.3     31.2 /
-15.058             0.210     0.0 / -inf
                                          Normal      Normal     Low-
Alrm                  Low-Alrm   Low-Alrm

Et 0/45     YES        0.0       0.000      19          3432.4     23.8 /
-16.234             0.214     655.1 / -1.837
                                          Normal      Normal     Low-
Alrm                  Low-Alrm   Normal

Et 0/47     YES        0.0       0.000      15          3350.9     0.1 /
-40.000              0.002     0.1 / -40.000
                                          Normal      Normal     Low-
Alrm                  Low-Alrm   Low-Alrm

Et 0/48     YES        0.0       0.000      19          3350.7     38.4 /
-14.157             0.270     557.4 / -2.538
                                          Normal      Normal     Low-
Alrm                  Low-Alrm   Normal

Et 0/51     YES        0.0       0.000      22          3342.6     Aggregate  0.0 /
-inf       145.548   3455.7 /  5.385
                                          Normal      Normal     High-
Alrm                  High-Alrm  High-Alrm
                                                                  Channel[1] 0.0 /
-inf        23.854    710.4 / -1.485
                                                                  Channel[2] 0.0 /
-inf        54.148    784.5 / -1.054
                                                                  Channel[3] 0.0 /
-inf        37.638    989.9 / -0.044
                                                                  Channel[4] 0.0 /
-inf        29.908    970.9 / -0.128

Et 0/55     YES        0.0       0.000      23          3334.5     Aggregate  0.0 /
-inf       179.714   3830.7 /  5.833
                                          Normal      Normal     High-
Alrm                  High-Alrm  High-Alrm
                                                                  Channel[1] 0.0 /
-inf        22.484    949.8 / -0.224
                                                                  Channel[2] 0.0 /
-inf        58.480    948.8 / -0.228
                                                                  Channel[3] 0.0 /
-inf        54.228    689.9 / -1.612
                                                                  Channel[4] 0.0 /
-inf        44.522   1242.2 /  0.942
```

```
SLX#
```

To display the optical monitoring configuration for an interface, use the following command:

```
 SLX# show media optical-monitoring interface ethernet 0/20
N/A - Not Available.
Port      Optical     Frequency   Wavelength  Module       Supply      Channel
Bias       Channel
          Monitoring  Error       Error       Temperature  Voltage     TX Power
Current    RX Power
          Support     ( GHz )     ( nm )       ( C )       (mVolts)    (uWatts)
(mAmps)    (uWatts/dBm)
         ===========  ==========  ========    ==========   =========== ==========
========   ============
Et 0/20    YES            0.0      0.000        18           3371.4    24.7/-16.073
0.142     595.3/-2.253

                                                Normal        Normal    Low-Alrm     Low-
Alrm   Normal

SLX#
SLX# show media optical-monitoring interface ethernet 0/51
N/A - Not Available.
Port        Optical    Frequency Wavelength Module      Supply
Channel                    Bias      Channel
            Monitoring Error     Error      Temperature Voltage    TX
Power                    Current   RX Power
            Support    ( GHz )   ( nm )     ( C )       ( mVolts ) ( uWatts /
dBm )            ( mAmps ) ( uWatts / dBm )
=========== ========== ========= ========== =========== ==========
=========================== ========= =================
Et 0/51     YES        0.0       0.000      22          3341.3     Aggregate  0.0 /
-inf       145.548   3460.3 /  5.391
                                           Normal      Normal     High-
Alrm                   High-Alrm   High-Alrm
                                                                  Channel[1] 0.0 /
-inf        23.854    711.6 / -1.478
                                                                  Channel[2] 0.0 /
-inf        54.148    794.5 / -0.999
                                                                  Channel[3] 0.0 /
-inf        37.638    995.6 / -0.019
                                                                  Channel[4] 0.0 /
-inf        29.908    958.6 / -0.184

SLX#
```

show media tunable-optic-sfpp

Displays the channels on which the tunable optic interfaces are currently operating.

Syntax

show media tunable-optic-sfpp [**channel** *channel_number*]

Parameters

channel *channel_number*

The channel number to display. The range of valid values is from 0 through 102.

Modes

Privileged EXEC mode

Output

The **show media tunable-optic-sfpp** command displays the following information:

Output field	Description
Channel	The number assigned to the channel.
Wavelength	The wavelength on which the optic interface is operating.

Examples

Sample output for a single channel.

```
device# show media tunable-optic-sfpp channel 2
command is show-media-tunable-optic-sfpp-channel-2.
  Channel   Wavelength
  ========= ==============
  2         1568.36
```

Sample output for all channels.

```
device# show media tunable-optic-sfpp
command is show-media-tunable-optic-sfpp.
  Channel   Wavelength
  ========= ==============
  1         1568.77
  2         1568.36
  3         1567.95
  4         1567.54
  5         1567.13
  6         1566.72
  7         1566.31
  8         1565.90
  9         1565.50
  10        1565.09
  11        1564.68
  12        1564.27
```

```
  13        1563.86
  14        1563.45
  15        1563.05
  16        1562.64
  17        1562.23
  18        1561.83
  19        1561.42
  20        1561.01
(Output truncated for brevity.)
```

show monitor

Displays the monitoring information for all port mirroring sessions or for one session.

Syntax

show monitor [**session** *session_number*]

Parameters

session *session_number*

Specifies a session identification number. Valid values range from 1 through 512.

Modes

Privileged EXEC mode

Output

The **show monitor** command displays the following information:

Output field	Description
Session	The identifying value applied to the session
Description	The session description.
State	The current state of the session.
Source Interface	The interface that the session is using to access the device.
Destination Interface	The destination for the session.
Direction	Displays whether the interface is receiving, transmitting, or both.

Examples

The following example displays monitoring information for all port mirroring sessions.

```
device# show monitor
Session                     : 1
Description                 : my_first_session
State                       : Enabled
Source Interface            : Eth 0/1  (Up)
Destination Interface       : Eth 0/11 (Up)
Direction                   : Rx

Session                     : 50
Description                 : [None]
State                       : Enabled
Source Interface            : Eth 0/2  (Down)
Destination Interface       : Eth 0/12 (Up)
Direction                   : Tx
```

The following example displays monitoring information for a specific port mirroring session.

```
device# show monitor session 1

Session                : 1
Description            : my_first_session
State                  : Enabled
Source Interface       : Eth 0/1  (Up)
Destination Interface  : Eth 0/11 (Up)
Direction              : Rx
```

show mpls autobw-template

Displays the output of the MPLS auto-bandwidth template.

Syntax

show mpls autobw-template [**detail**]

Parameters

detail

Displays the auto-bandwith template information in detail.

Modes

Privileged EXEC mode

Usage Guidelines

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example displays a sample output of the command.

```
device# show mpls autobw-template
Total number of auto-bandwidth templates: 2
                  Adjust    Adjust  Over/und   Minimum    Maximum  Monitor Ref.
Name             Interval Threshold    Limit  Bandwidth  Bandwidth    Only Count
aaa                  1200        10    5/ 15       1000       8000      No     3
bbb                   600     Table    3/ 10        200      20000      No     5
```

The following example displays a sample output of the command using the *detail* option.

```
device# show mpls autobw-template detail
Total number of auto-bandwidth templates: 2
Auto-bandwidth template aaa:
 adjustment-interval: 1200 sec, adjustment-threshold: 10, mode: monitor-and-signal
 overflow-limit: 5, underflow-limit: 15
 minimum-bw: 1000 kbps, maximum-bw: 8000 kbps
 sample-record: enabled
 number of paths associated: 3
Auto-bandwidth template bbb:
 adjustment-interval: 600 sec, adjustment-threshold: Table, mode: monitor-and-signal
 overflow-limit: 3, underflow-limit: 10
 minimum-bw: 200 kbps, maximum-bw: 20000 kbps
 sample-record: disabled
 number of paths associated: 5
```

show mpls autobw-threshold-table

Displays the global-threshold table with the range of the current-bandwidth and the corresponding absolute adjustment-threshold.

Syntax

show mpls auto-threshold-table

Modes

Privileged EXEC mode

Usage Guidelines

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example displays the output of the command.

```
device# show mpls autobw-threshold-table
Auto-bandwidth threshold table
Range(kbps)    Threshold(kbps)
0-10    2000
11-1000    3000
1001-10000    5000
10001-max    10000
```

show mpls bypass-lsp

Use the **show mpls bypass-lsp** command for displaying all dynamic bypass LSPs along with static bypass LSPs.

Syntax

```
show mpls bypass-lsp [ debug | detail | down | dynamic | extensive |
   name | static | up [ detail | extensive | wide ] | wide ]

show mpls bypass-lsp dynamic [ debug | detail | extensive | interface
   [ ethernet | ve ] | name | wide ]

show mpls bypass-lsp static [ debug | detail | extensive | interface |
   name | wide ]
```

Parameters

debug

Displays the MPLS Bypass LSP extensive debug information.

detail

Displays the MPLS bypass LSP information in detail.

down

Displays the operationally down bypass LSPs information.

extensive

Displays the MPLS bypass LSP information with extensive detailed information.

interface

Displays the MPLS dynamic bypass LSP interface information.

ethernet

Specifies the ethernet interface.

ve

Specifies the VE interface.

name

Displays an MPLS bypass LSP by the specified name.

static

Displays the MPLS static bypass LSP information.

up

Displays the operationally UP bypass LSPs information.

wide

Displays MPLS bypass LSP brief wide information.

Modes

Privileged EXEC mode

Usage Guidelines

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example displays the output of the show mpls bypass-lsp command.

```
device# show mpls bypass-lsp
Note: Bypass LSPs marked with + are dynamic bypass LSPs
Bypass LSP           To               Admin Oper  Tunnel   Up/Dn Retry Active
Name                 Address          State State Intf     Times Num   Path
my-bypass-lsp        20.20.20.20      UP    UP    tnl3     1     0     path-for-bypass-lsp
```

The following example displays the output of the **show mpls bypass-lsp** command with the static wide options

```
device# show mpls bypass-lsp static wide
Bypass LSP           To               Admin Oper  Tunnel   Up/Dn Retry Active
Name                 Address          State State Intf     Times Num   Path
my-bypass-lsp        20.20.20.20      UP    UP    tnl3     1     0     path-for-bypass-
lsp
```

The following example displays the output of the **show mpls bypass-lsp** command using the extensive option.

```
device# show mpls bypass-lsp extensive
LSP my-bypass-lsp, to 20.20.20.20
 From: 29.29.29.29, admin: UP, status: UP, tunnel interface(primary path): tnl3
 Times primary LSP goes up since enabled: 1
 Adaptive
 Primary path: path-for-bypass-lsp, up: yes, active: yes
  Maximum retries: None, no. of retries: 0
  ReoptimizeTimer configured 360
   ReoptimizeTimer next expiration in 93 seconds
  Setup priority: 7, hold priority: 0, cos: 3
  Max rate: 1000 kbps, mean rate: 1000 kbps, max burst: 5000 bytes
  Tie breaking: random, hop limit: 6
  Exclude any of admin groups: 15 16 17
  Exclude interface(s): Eth 1/3
  CSPF-computation-mode configured: te-metric
  Constraint-based routing enabled: yes
   Path calculated using constraint-based routing: yes
   Path calculated using interface constraint: no
   Path calculated using te-metric
   Path cost: 2
  Explicit path hop count: 1
   18.18.18.18(S)
  Recorded routes:
   Protection codes/Rtr Id flags: P: Local  N: Node  B: Bandwidth  I: InUse R: RtrId
   18.29.1.18 -> 18.20.1.20
 Bypass Tunnel bandwidth
  Maximum bandwidth: 1000 kbps
  Reservable bandwidth [priority] kbps:
   [0] 1000 [1] 1000 [2] 1000 [3] 1000
   [4] 1000 [5] 1000 [6] 1000 [7] 1000
  Current signaled rate: 1000 kbps
 Active Path:
  Tunnel interface: tnl3, outbound interface: Eth 1/1
  Tunnel index: 3, Tunnel instance: 1, Out label: 2061
 History:
```

```
    0  10-13 22:41:58 : LSP tunnel is Enabled
    1  10-13 22:41:58 : CSPF-Computation successful for Primary path path-for-bypass-lsp.
Computed route:
                        ->18.29.1.18->18.20.1.20
    2  10-13 22:41:58 : Primary path path-for-bypass-lsp.  RRO received:
                        ->18.29.1.18->18.20.1.20
    3  10-13 22:41:58 : Primary path path-for-bypass-lsp setup successful . Instance id 1
    4  10-13 22:41:58 : LSP tunnel is UP with Primary path path-for-bypass-lsp as Active
    5  10-13 22:41:58 : Tunnel added or updated, out-interface: Eth 1/1, out-label 2061
 Riding Backup Lsps: 1
  Ingress backups: 1, up: 1, active: 0
  Transit backups: 0, up: 0, active: 0
  Ingress backups
   State  From            To              LSPname
   UP     18.29.1.29      20.20.20.20     my-fac-bkup-frr-lsp
```

show mpls dynamic-bypass interface

Displays the dynamic bypass information.

Syntax

```
show mpls dynamic-bypass interface [ brief | detail | ethernet | port-
   channel | ve ]
```

Parameters

interface

Displays dynamic bypass interface information.

brief

Displays dynamic bypass interface brief information.

detail

Displays dynamic bypass interface detail information.

ethernet

Displays dynamic bypass ethernet interface.

port-channel

Displays dynamic bypass port-channel interface.

ve

Displays dynamic bypass VE interface.

Modes

Privileged EXEC mode

Usage Guidelines

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

show mpls interface

Displays the MPLS-enabled interfaces.

Syntax

show mpls-interface [**detail** | **ethernet** *slot/port* | **port-channel** *number* | **ve** *number*]

Parameters

detail

Displays MPLS-enabled interfaces information in detail.

ethernet *slot/port*

Specifies an Ethernet slot and port.

port-channel *number*

Specifies a port-channel interface.

ve *number*

Specifies the VE interface number.

Modes

Privileged EXEC mode

Usage Guidelines

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

show mpls ldp

Displays the MPLS ldp information.

Syntax

show mpls ldp database [**A.B.C.D** | **filtered**]

show mpls ldp fec [**prefix** [**A.B.C.D or A.B.C.D/L** | [**filtered** [**in** | **out**] | **prefix-filter**]] | **summary** | **vc**]

show mpls ldp interface [**ethernet** *slot/port* | **port-channel** *number* | **ve** *number*]

show mpls ldp neighbor [**A.B.C.D or A.B.C.D/L**]

show mpls ldp path [**A.B.C.D or A.B.C.D/L**]

show mpls ldp peer [**A.B.C.D** | **brief** | **detail**]

show mpls ldp session [**A.B.C.D** | **detail**]

show mpls ldp statistics

show mpls ldp targeted-peer [**A.B.C.D**]

show mpls ldp tunnel [**A.B.C.D or A.B.C.D/L** | **brief** | **detail** | **out-interface** [**ethernet interface** | **ve**]]

Parameters

database

Displays the LDP database information.

A.B.C.D

Displays the peer IP address.

filtered

Displays the sessions with inbound filtered mappings.

fec

Displays the FEC information.

prefix

Displays the prefix FEC information.

A.B.C.D or A.B.C.D/L

Displays the IP address/prefix.

filtered

Displays the filtered prefix FEC.

in

Displays inbound filtered prefix FEC.

out

Displays outbound filtered prefix FEC.

prefix-filter

Displays the prefix-based filter FEC.

summary

Displays the summary information.

vc

Displays the VC FEC information.

interface

Displays the MPLS LDP-enabled interfaces.

ethernet *slot/port*

Displays the dynamic bypass ethernet interface.

port-channel *number*

Displays the dynamic bypass port-channel interface.

ve *number*

Displays the dynamic bypass ve interface.

neighbor

Displays the MPLS LDP neighbor information.

A.B.C.D or A.B.C.D/L

Displays the IP address/prefix.

path

Displays the LDP created LSP information.

A.B.C.D or A.B.C.D/L

Displays the IP address/prefix.

peer

Displays the LDP peer information.

A.B.C.D

Displays the IP address.

brief

Displays the brief information.

detail

Displays the detailed information.

session

Displays the MPLS LDP session information.

A.B.C.D

Displays the IP address.

detail

Displays the detailed information.

statistics

Displays the LDP protocol statistics.

targeted-peer

Displays the LDP targeted peer information.

A.B.C.D

Displays the IP address.

tunnel

Displays the LDP tunnel.

prefix

Displays the prefix FEC information.

A.B.C.D or A.B.C.D/L

Displays the IP address/prefix.

brief

Displays the brief information.

detail

Displays the detailed information.

out-interface

Displays the LDP tunnel for interface.

ethernet *slot/port*

Displays the ethernet interface.

ve

Displays the VE interface.

summary

Displays the summary information.

vc

Displays the VC FEC information

Modes

Privileged EXEC mode

Usage Guidelines

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

show mpls lsp

Displays detailed information about a specific LSP.

Syntax

show mpls lsp [**debug** | **detail** | **down** | **extensive** | **name** | **up** | **wide**]

show mpls lsp down [**debug** | **detail** | **extensive** |**wide**]

show mpls lsp up [**detail** | **extensive** | **wide**]

Parameters

debug

Displays the MPLS LSP extensive debug information.

detail

Displays the MPLS LSP information in detail.

down

Displays the operationally down LSPs information.

extensive

Displays the MPLS LSP extensive information.

name

Displays an MPLS LSP by the specified name.

up

Displays the operationally UP LSPs information.

wide

Displays MPLS LSP brief wide information.

Modes

This command operates under all modes.

Usage Guidelines

The sample history displays for the current adjustment interval.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

This command can display the underflow-limit parameter and the number of consecutive underflows. The adjustment-threshold is used from the global table is indicated with the value for current rate. The **show mpls lsp extensive** command shows the adjustment event with the previous rate and the maximum sampled rate.

Output

The **show mpls lsp** command displays the following information:

Output field	Description
Name	The name of the LSP. LSPs are displayed in alphabetical order.
To	The egress LER for the LSP.
From	The LSPs source address, configured with the **from** command. When a source IP address has not been specified for the LSP with the from command, and the LSP has not been enabled, then '(n/a)' displays in the 'From' field.
admin	The administrative state of the LSP. Once the user activates the LSP with the **enable** command, the administrative state changes from DOWN to UP.
status	The operational state of the LSP. This field indicates whether the LSP has been established through signaling and is capable of having packets forwarded through it. When the status of the LSP is DOWN, the reason why the LSP is down is shown in parentheses. There maybe a short period of time after the user enables the LSP that the administrative state of the LSP is UP, but the status is DOWN. Once the LSP has been established through signaling, both the administrative state and the status is UP.
Tunnel interface (primary path)	The path currently selected for this LSP.
Times primary LSP goes up since enabled	The number of times the status of the LSPs primary path transitions from DOWN to UP.
Metric	The metric for the LSP, configured with the **metric** command.
OSPF shortcuts Enabled	Displays *yes* when OSPF Shortcuts is enabled. Displays *no* when not enabled.
ignore-lsp-metric	Displays *yes* when the configured metrics for the LSP is to be ignored. Displays *no* otherwise.
Pri. path	The name of the primary path for this LSP and whether the path is currently active.
up	Displays if the primary path is UP.
active	Specifies if the primary path is active.
Setup priority	The configured setup priority for the LSP.
hold priority	The configured hold priority for the LSP.
Max rate	The maximum rate of packets that can go through the LSP (in kbps), set with the **traffic-eng max-rate** command.
mean rate	The average rate of packets that can go through the LSP (in kbps), set with the **traffic-eng mean-rate** command.

Output field	Description
mode	Mode displays if the LSP is in monitor-only or monitor-and-signal mode.
adjustment threshold	Displays the configured adjustment-threshold value.
minimum bw	The configured minimum bandwidth.
maximum bw	The configured maximum bandwidth.
overflow limit	Displays the configured overflow-limit value.
underflow limit	The number of samples that have to be below the threshold, to trigger a premature adjustment.
sample-record	Whether the template is set to record the sample history.
Constraint-based routing enabled	Whether CSPF is in effect for the LSP.
Path calculated using constraint-based routing	Whether the explicit path used by the active path was calculated using the constraint-based routing.
Path calculated using interface constraint	Whether the explicit path used by the active path was calculated using the interface-based routing.
Path cost	The total cost of this path.
Tie breaking	The tie-breaking method CSPF uses to select a path from a group of equal-cost paths to the egress LER, set with the **tie-breaking** command.
LDP tunnel enabled	If LDP tunneling is enabled, the line reads "yes". If it is not enabled, the line reads "no".
Soft preemption enabled	Soft preemption minimizes traffic disruptions and gracefully reroutes the preempted LSPs.
Sec. path	The name of the secondary path for this LSP and whether the path is currently active.
active	Displays if the secondary path is active.
Hot-standby	Whether the secondary path is a hot-standby path.
status	The operational state of the secondary path
Setup priority	The configured setup priority for the LSP.
hold priority	The configured hold priority for the LSP
Max rate	The maximum rate of packets that can go through the LSP (in kbps), set with the **traffic-eng max-rate** command.
mean rate	The average rate of packets that can go through the LSP (in kbps), set with the **traffic-eng mean-rate** command.
max burs	The maximum size (in bytes) of the largest burst the LSP can send at the maximum rate, set with the **traffic-eng max-burst** command.
mode	Mode shows if the LSP is in monitor-only or monitor-and-signal mode.
adjustment threshold	Displays the configured adjustment-threshold value.

Output field	Description
minimum bw	The configured minimum bandwidth.
maximum bw	The configured maximum bandwidth.
overflow limit	Displays the configured overflow-limit value.
underflow limit	The number of samples which must be below the threshold to trigger a premature adjustment.
sample-record	Whether the template is set to record the sample history.
Constraint-based routing enabled	Whether CSPF is in effect for the LSP.
hop limit	The maximum number of hops a path calculated by CSPF can have, set with the **hop-limit** command.
Soft preemption enabled	Soft preemption minimizes traffic disruptions and gracefully reroutes the preempted LSPs
Active path attributes	
Tunnel interface	The MPLS tunnel interface port ID.
outbound interface	The outbound label used by the active path of the LSP.
Tunnel index	The tunnel index for the active path of the LSP.
Tunnel instance	
outbound label	The outbound label used by the active path of the LSP.
Auto-bandwidth running info mode	
adjustment interval	Displays the configured adjustment-timer value.
adjustment threshold	Displays the configured adjustment-threshold value.
overflow limit	Displays the configured overflow-limit value.
underflow limit	The number of samples that must be below the threshold to trigger a premature adjustment.
minimum bw	The configured minimum bandwidth.
maximum bw	The configured maximum bandwidth.
Samples collected	Number of samples collected so far in the current adjustment-interval.
max sampled bw	The maximum number of the samples collected so far in the current adjustment-interval.
last sample	The last sampled-bandwidth.
Sample-record	Whether the template is set to record the sample history.
adjustment due in	Displays the time remaining for the current adjust-interval to expire.
Adjustment ignored	This consecutive number of times the adjustment was ignored due to any reason.
Current bandwidth	Current running bandwidth.
Recorded routes	The addresses recorded by the RECORD_ROUTE object during RSVP signaling.

Examples

The following example shows the output of the command, specifying the LSP *name* with the extensive option.

```
device# show mpls bypass-lsp extensive
LSP my-bypass-lsp, to 20.20.20.20
 From: 29.29.29.29, admin: UP, status: UP, tunnel interface(primary path): tnl3
 Times primary LSP goes up since enabled: 1
 Adaptive
 Primary path: path-for-bypass-lsp, up: yes, active: yes
  Maximum retries: None, no. of retries: 0
  ReoptimizeTimer configured 360
   ReoptimizeTimer next expiration in 93 seconds
  Setup priority: 7, hold priority: 0, cos: 3
  Max rate: 1000 kbps, mean rate: 1000 kbps, max burst: 5000 bytes
  Tie breaking: random, hop limit: 6
  Exclude any of admin groups: 15 16 17
  Exclude interface(s): Eth 1/3
  CSPF-computation-mode configured: te-metric
  Constraint-based routing enabled: yes
   Path calculated using constraint-based routing: yes
   Path calculated using interface constraint: no
   Path calculated using te-metric
   Path cost: 2
  Explicit path hop count: 1
   18.18.18.18(S)
  Recorded routes:
   Protection codes/Rtr Id flags: P: Local  N: Node  B: Bandwidth  I: InUse R: RtrId
   18.29.1.18 -> 18.20.1.20
 Bypass Tunnel bandwidth
  Maximum bandwidth: 1000 kbps
  Reservable bandwidth [priority] kbps:
   [0] 1000 [1] 1000 [2] 1000 [3] 1000
   [4] 1000 [5] 1000 [6] 1000 [7] 1000
  Current signaled rate: 1000 kbps
 Active Path:
  Tunnel interface: tnl3, outbound interface: Eth 1/1
  Tunnel index: 3, Tunnel instance: 1, Out label: 2061
 History:
    0  10-13 22:41:58 : LSP tunnel is Enabled
    1  10-13 22:41:58 : CSPF-Computation successful for Primary path path-for-bypass-lsp.
Computed route:
                       ->18.29.1.18->18.20.1.20
    2  10-13 22:41:58 : Primary path path-for-bypass-lsp.  RRO received:
                       ->18.29.1.18->18.20.1.20
    3  10-13 22:41:58 : Primary path path-for-bypass-lsp setup successful . Instance id 1
    4  10-13 22:41:58 : LSP tunnel is UP with Primary path path-for-bypass-lsp as Active
    5  10-13 22:41:58 : Tunnel added or updated, out-interface: Eth 1/1, out-label 2061
 Riding Backup Lsps: 1
  Ingress backups: 1, up: 1, active: 0
  Transit backups: 0, up: 0, active: 0
  Ingress backups
   State  From            To              LSPname
   UP     18.29.1.29      20.20.20.20     my-fac-bkup-frr-lsp
```

The following example displays the output of the command when using the detail option.

```
Router# show mpls lsp extensive
LSP lsp1, to 23.23.23.23
  From: 34.34.34.34, admin: UP, status: UP, tunnel interface(primary path): tnl1
```

```
  Times primary LSP goes up since enabled: 1
  Metric: 0, Adaptive
  OSPF shortcuts Enabled:yes ignore-lsp-metric:yes
  Maximum retries: NONE, no. of retries: 0
  Pri. path: NONE, up: yes, active: yes
  Setup priority: 7, hold priority: 0
  Max rate: 0 kbps, mean rate: 0 kbps, max burst: 0 bytes
  Auto-bandwidth. template: template1, mode: monitor-only
    adjustment interval: 86400 sec, adjustment threshold: 0
    minimum bw: 0 kbps, maximum bw: 2147483647 kbps
    overflow limit: 0, underflow limit: 20, sample-record: disabled
  Constraint-based routing enabled: yes
   Path calculated using constraint-based routing: yes
   Path calculated using interface constraint: no
   Path cost: 20
  Tie breaking: random, hop limit: 0
  LDP tunneling enabled: no
  Soft preemption enabled: no
  Sec. path: via16, active: no
   Hot-standby: no, status: down, adaptive
   Setup priority: 7, hold priority: 0
   Max rate: 0 kbps, mean rate: 0 kbps, max burst: 0 bytes
   Auto-bandwidth. template: NONE, mode: monitor-and-signal
    adjustment interval: 300 sec, adjustment threshold: Table
    minimum bw: 0 kbps, maximum bw: 2147483647 kbps
    overflow limit: 5, underflow-limit: 10, sample-record: enabled
   Constraint-based routing enabled: yes
   hop limit: 0
   Soft preemption enabled: no
  Active Path attributes:
   Tunnel interface: tnl1, outbound interface: e4/3
   Tunnel index: 2, Tunnel instance: 1 outbound label: 2049
   Auto-bandwidth running info. Mode: monitor-only
    adjustment interval: 1200 sec(T), adjustment threshold: Table(T)
    overflow limit: 0, underflow limit: 3
    minimum bw: 0 kbps(T), maximum bw: 9647 kbps(T)
    Samples collected: 14, max sampled bw: 0 kbps, last sample: 0 kbps
    Overflow-count: 0, Underflow-count: 2,max-underflow-sample: 34kbps
    Sample-record: enabled(T)
    adjustment due in 1174 seconds
    Adjustment ignored: 0 time(s)
    No adjustment since activation. Current bandwidth: 0 kbps
   Recorded routes:
    Protection codes/Rtr Id flag: P: Local  N: Node  B: Bandwidth  I: InUse R: RtrId
    31.31.31.16 -> 161.161.161.1
```

The following output displays the command with the autobw-samples option.

```
device# show mpls lsp name lsp1 autobw-samples
LSP lsp1, to 23.23.23.23
  From: 34.34.34.34, admin: UP, status: UP, tunnel interface(primary path): tnl1
  Times primary LSP goes up since enabled: 1
  Metric: 0, Adaptive
  OSPF shortcuts Enabled:yes ignore-lsp-metric:yes
  Maximum retries: NONE, no. of retries: 0
  Pri. path: NONE, up: yes, active: yes
  Setup priority: 7, hold priority: 0
  Max rate: 0 kbps, mean rate: 0 kbps, max burst: 0 bytes
  Auto-bandwidth. template: template1, mode: monitor-only
    adjustment interval: 86400 sec, adjustment threshold: 0
    minimum bw: 0 kbps, maximum bw: 2147483647 kbps
    overflow limit: 0, underflow limit: 20, sample-record: disabled
  Constraint-based routing enabled: yes
   Path calculated using constraint-based routing: yes
```

```
   Path calculated using interface constraint: no
   Path cost: 20
  Tie breaking: random, hop limit: 0
  LDP tunneling enabled: no
  Soft preemption enabled: no
  Sec. path: via16, active: no
   Hot-standby: no, status: down, adaptive
   Setup priority: 7, hold priority: 0
   Max rate: 0 kbps, mean rate: 0 kbps, max burst: 0 bytes
   Auto-bandwidth. template: NONE, mode: monitor-and-signal
    adjustment interval: 300 sec, adjustment threshold: Table
    minimum bw: 0 kbps, maximum bw: 2147483647 kbps
    overflow limit: 5, underflow-limit: 10, sample-record: enabled
   Constraint-based routing enabled: yes
   hop limit: 0
   Soft preemption enabled: no
  Active Path attributes:
   Tunnel interface: tnl1, outbound interface: e4/3
   Tunnel index: 2, Tunnel instance: 1 outbound label: 2049
   Auto-bandwidth running info. Mode: monitor-only
    adjustment interval: 1200 sec(T), adjustment threshold: 3000(A)
    overflow limit: 0, underflow limit: 4
    minimum bw: 0 kbps(T), maximum bw: 9647 kbps(T)
    Samples collected: 5, max sampled bw:6598 kbps,last sample: 0 kbps
    Overflow-count: 0, Underflow-count: 2,max-underflow-sample: 34kbps
    Sample-record: enabled(T)
    adjustment due in 1174 seconds
    Adjustment ignored: 0 time(s)
    No adjustment since activation. Current bandwidth: 0 kbps
   Recorded routes:
    Protection codes/Rtr Id flag: P: Local  N: Node  B: Bandwidth  I: InUse R: RtrId
    31.31.31.16 -> 161.161.161.1
Auto Bandwidth Sample History:
1    Feb  4 19:56:06 : Path p1 active with rate 3000 kbps
     2  Feb  4 19:57:06 : 4445 kbps
     3  Feb  4 19:58:06 : 4855 kbps
     4  Feb  4 19:59:06 : 4501 kbps
     5  Feb  4 20:00:06 : 4200 kbps
     6  Feb  4 20:01:06 : 4455 kbps
     7  Feb  4 20:02:06 : 4319 kbps
     8  Feb  4 20:03:06 : 4299 kbps
     9  Feb  4 20:04:06 : 4582 kbps
    10  Sample recording disabled
    11  Feb  4 20:16:31 : 3630 kbps
    12  Feb  4 20:17:31 : 2924 kbps
    13  Feb  4 20:17:38 : Rate adjusted from 2500 to 4500 kbps
                  Reason: Adjustment-interval expiry
    14  Feb  4 20:18:06 : 4500 kbps
    15  Feb  4 20:19:06 : 4500 kbps
    16  Feb  4 20:20:06 : 4500 kbps
    17  Feb  4 20:21:06 : 4500 kbps
    18  Feb  4 20:16:31 : 4500 kbps
    19  Feb  4 20:17:31 : 4500 kbps
    20  Feb  4 20:17:38 : Adjustment ignored. Threshold not crossed
    21  Feb  4 20:16:31 : 9000 kbps
    22  Feb  4 20:17:31 : 9000 kbps
    23  Feb  4 20:17:38 : Rate adjusted from 4500 to 9000 kbps
                  Reason: Overflow limit exceeded
    24  Feb  4 20:18:06 : 4500 kbps
    25  Feb  4 20:19:06 : 4500 kbps
```

The following example displays the output of the command when using the detail option.

```
Router# show mpls lsp extensive
LSP 11, to 0.0.0.0
From: (n/a), admin: DOWN, status: DOWN Times primary LSP goes up since enabled: 0
Metric: 0
OSPF shortcuts Enabled:yes ignore-lsp-metric:yes
Primary path: None, up: no, active: no
  Maximum retries: None, no. of retries: 0
  Setup priority: 7, hold priority: 0
  Max rate: 0 kbps, mean rate: 0 kbps, max burst: 0 bytes
  Tie breaking: random, hop limit: 0
  Soft preemption enabled: no
```

show mpls policy

Shows the current MPLS policy.

Syntax

show mpls policy

Modes

Privileged EXEC mode

Usage Guidelines

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example shows a sample output of the command.

```
Router#show mpls policy
Current MPLS policy settings:
  CSPF interface constraint: disabled
  CSPF-Group computation-mode: disabled
  CSPF computation-mode use bypass metric: disabled
  CSPF computation-mode use bypass liberal: disabled
  TTL propagation for MPLS label: disabled, IPVPN: disabled, IP over MPLS: enabled
  Inter-AS route filtering: enabled, Intra-AS iBGP route filtering: disabled
  Ingress tunnel accounting: disabled
  Polling interval for MPLS LSP traffic statistics: 300 seconds
  Advertise TE parameters via: OSPF
  Handle IGP neighbor down event - ISIS: No OSPF: No
  LSP rapid retry: enabled, maximum number of retries: no limit
  LSP periodic retry time: 30 seconds
  FRR backup/detour retry time: 30 seconds
  Auto-bandwidth: enabled, sample-interval: 60 seconds
   Maximum samples recorded per LSP: 1500
  Soft preemption cleanup-timer: 30 seconds
  MPLS TE Periodic Flooding Timer : 180 seconds
  MPLS TE flooding thresholds
    Global  UP   thresholds : None
    Global  DOWN thresholds : None
    Default UP   thresholds : 15 30 45 60 75 80 85 90 95 96 97 98 99 100
    Default DOWN thresholds : 99 98 97 96 95 90 85 80 75 60 45 30 15
```

show mpls rsvp

Displays the MPLS RSVP information.

Syntax

show mpls rsvp igp-sync [**link** [**detail** | **ip** *ipv4 addr*] | **lsp** [**detail** | **name** *name*]]

show mpls rsvp interface [**detail** | **ethernet** *slot/port* | **port-channel** *number* | **ve** *vlan_id*]

show mpls rsvp neighbor [**detail** | *ipv4 address*]

show mpls rsvp session [**backup** | **brief** | **destination** | **detail** | **detour** | **down** | **egress** | **extensive** | **in-interface** | **ingress** | **name** | **out-interface** | **transit** | **up** | **wide**]

show mpls rsvp statistics

Parameters

igp-sync

Displays the RSVP IGP synchonization information.

link

Displays the RSVP IGP synchonization link brief information.

detail

Displays the RSVP IGP synchonization link detailed information.

ip *ipv4 addr*

Displays the RSVP IGP synchonization specified link information.

lsp

Displays the RSVP IGP synchonization LSP brief information.

detail

Displays the RSVP IGP synchonization LSP detailed information.

name *name*

Displays the RSVP IGP synchonization specified LSP information.

interface

Displays RSVP interface information.

detail

Displays RSVP interface information in detail.

ethernet *slot/port*

Displays the specifed RSVP Ethernet information.

port-channel *number*

Specifies a port-channel.

ve *vlan_id*

Displays the specified VE information.

neighbor

Displays the RSVP neighbor information.

detail

Displays the RSVP neighbor information in detail.

session

Displays the RSVP session information. For addition information, see the **show mpls rsvp session** command page.

statistics

Displays the RSVP control packet statistics information.

Modes

Privileged EXEC mode

Usage Guidelines

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example shows the command using the interface option in the interface mode.

```
device(config-if-e1000-0/8)# show mpls interface e0/7
Admin: Up    Oper: Up
  MTU: 1500 bytes
  Maximum BW: 10000000 kbps, maximum reservable BW: 10000000 kbps
  Admin group: 0x00000000
  Reservable BW [priority] kbps:
    [0] 10000000    [1] 10000000    [2] 10000000    [3] 10000000
    [4] 10000000    [5] 10000000    [6] 10000000    [7] 10000000
  Last sent reservable BW [priority] kbps:
    [0] 10000000    [1] 10000000    [2] 10000000    [3] 10000000
    [4] 10000000    [5] 10000000    [6] 10000000    [7] 10000000
  Soft Preemption under provisioned BW [priority] kbps: [0] 0    [1] 0    [2] 0    [3] 0
    [4] 0    [5] 0    [6] 0    [7] 0
  LDP tunnel count: 0
```

The following example shows the command using the **interface detail** option in the router mpls mode.

```
device(config-router-mpls)# show mpls rsvp interface detail

                                          Num of OutSegs    Num of
Interface State MD5  RelMsg Bundle SRefresh Act/Inact/Resv    Preempts/softPrmpt
e0/1         Up       OFF  OFF       OFF       OFF         1/0/1             2/2
e0/2         Up       OFF  OFF       OFF       OFF         0/0/0             0/0
e0/10        Dn       OFF  OFF       OFF       OFF         0/0/0             0/0
```

show mpls rsvp interface

Displays the RSVP refresh reduction settings for an interface.

Syntax

show mpls rsvp interface [**detail** | **ethernet** *slot/port* | **port-channel** *number* | **ve** *vlan_id*]

Parameters

detail

Displays the RSVP interface information in detail.

ethernet *slot/port*

Specifies the selected Ethernet interface.

port-channel *number*

Specifies a port-channel interface.

ve *vlan_id*

Specifies the selected VE interface.

Modes

Privileged EXEC mode

Usage Guidelines

To clear the RSVP statistics counters, use the **clear mpls rsvp statistics** command.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

This command operates in all modes.

Output

The **show mpls rsvp interface detail** command displays the following information:

Output field	Description
Status	Whether the interface is UP or DOWN.
MD5	Whether RSVP message authentication is enabled on the interface.
RelMsg	Whether RSVP reliable messaging is enabled on the interface.

Output field	Description
Bundle	Whether RSVP bundle messages are enabled on the interface.
SRefresh	Whether RSVP summary refresh is enabled on the interface.
MPLS TE flooding thresholds in use	
Hello-interval	The interval between successive hello packets in milliseconds.
Hello-tolerance	The number of hello intervals before the node treats the neighbor as if communication has been lost.
PacketType	
Path	The number of Path messages received with a packet processing error.
Resv	The number of RESV messages received with a packet processing error.
PathErr	The number of PathErr messages received with a packet processing error.
ResvErr	The number of ResvErr messages received with a packet processing error.
PathTear	The number of PathTear messages received with a packet processing error.
ResvTear	The number of reservation confirmation messages received with a packet processing error.
ResvConf	The number of reservation confirmation messages received with a packet processing error.
Bundle	The number of bundled RSVP messages sent and received on the interface with a packet processing error.
Ack	The number of Ack messages sent and received on the interface with a packet processing error.
SumRefresh	The number of summary refresh messages sent and received on the interface with a packet processing error.
Hello	The number of RSVP Hello's with a packet processing error
Errors	
Rev MD5 Auth Errors	The number of MD5 authentication errors on received packets on the interface.
Pkt with MsgId drop	Number of packets with dropped message IDs.
Pkt with SRef drop	Number of packets with dropped.
NACK Object	Number of objects without acknowledgment.
Active Facility Backups	Number of Active facility backup tunnels.

Output field	Description
Inactive Facility Backups	Number of inactive facility backup tunnels.
Duplicate preempts dropped	Number of dropped preempts.

Examples

The following example shows a abbreviated output of the command with the detail option.

```
device# show mpls rsvp interface
G = Interface is using global config for Refresh Reduction, Reliable Messaging
L = Interface is using local config for Refresh Reduction, Reliable Messaging
D = Refresh Reduction, Reliable Messaging is exclusively disabled on Interface

                                                    Num of OutSeg      Num of
Interface      State   MD5  RelMes   Bundle  SRefresh  Act/Inact/Resev    Preempts/
softPrpt
Ve20           Down    OFF  ON<G>    OFF     ON<G>     0/0/0              0/0

 MPLS TE flooding thresholds in use
  Default    UP   thresholds: 15 30 45 60 75 80 85 90 95 96 97 98 99 100
  Default    DOWN thresholds: 99 98 97 96 95 90 85 80 75 60 45 30 15

 Hello-interval: 0 sec, Hello-tolerance: 0 <Hello Inactive, Global configuration>

                     Total                Since Last Clear
 PacketType     Sent      Received       Sent      Received
  Path          29373     32824          29373     32824
  Resv          33047     30209          33047     30209
  PathErr       12        0              12        0
  ResvErr       89        10             89        10
  PathTear      111       45             111       45
  ResvTear      0         0              0         0
  ResvConf      0         0              0         0
  Bundle        0         0              0         0
  Ack           0         0              0         0
  SumRefresh    0         0              0         0
  Hello         0         0              0         0

 Errors                    Total             Since Last Clear
    Rev MD5 Auth Errors    0                 0
    Pkt with MsgId drop    0                 0
    Pkt with SRef drop     0                 0
    NACK Object            0                 0

  Active Facility Backups:   0
  Inactive Facility Backups: 0
  Duplicate preempts dropped: 0
  ....
```

show mpls rsvp session

Use the show mpls rsvp session command to view the policy and detailed history of the specified LSP.

Syntax

show mpls rsvp session backup [**detail** | **extensive** | **protection-available** [**active** | **detail** | **extensive** | **inactive** | **wide**] | **protection-unavailable** [**detail** | **extensive** | **wide**] | **wide**]

show mpls rsvp session brief

show mpls rsvp session destination *ip_addr*

show mpls rsvp session detail

show mpls rsvp session detour

show mpls rsvp session down [**detail** | **egress** | **extensive** | **in-interface** | **ingress** | **out-interface** | **transit** | **wide**]

show mpls rsvp session egress

show mpls rsvp session extensive

show mpls rsvp session in-interface [**ethernet** *slot/port* | **port-channel** *number* | **ve** *vlan_id*]

show mpls rsvp session ingress

show mpls rsvp session name

show mpls rsvp session out-interface [**ethernet** *slot/port* | **port-channel** *number* | **ve** *vlan_id*]

show mpls rsvp session transit

show mpls rsvp session up

show mpls rsvp session wide

Parameters

backup

Displays backup session information.

active

Displays active backup session information.

detail

Displays detailed backup session information.

extensive

Displays extensive backup session information, including History.

inactive

Displays inactive, but up backup or detour session information.

protection-available

Displays backup session information, with protection available.

protection-unavailable

Displays backup session information, with protection unavailable.

wide

Displays backup session information, including any long session names.

brief

Displays brief session information.

destination *ip_addr*

Displays the selected destination IP address.

detail

Displays detailed session information.

detour

Displays detour session information.

down

Displays inactive session information.

in-interface

Displays RSVP sessions coming into an interface.

out-interface

Displays RSVP sessions going out on an interface.

ethernet *slot/pot*

Displays the selected Ethernet information.

port-channel *number*

Displays the port-channel interface information.

ve *vlan_id*

Displays the selected virtual Ethernet information.

transit

Displays the transit session information.

egress

Displays egress session information.

ingress

Displays ingress session information.

extensive

Displays the specified LSP RSVP session information, including History.

name *name*

Displays session by the specified name.

up

Displays up session information.

wide

Displays long session names.

Modes

Privileged EXEC mode

Usage Guidelines

Many options in the **show mpls rsvp session** command can be combined for a more specific result. For example, the **show mpls rsvp session backup name lsp1** command is helpful for limiting the output to useful information by session name.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example displays a sample output of the **show mpls rsvp session** command.

```
device# show mpls rsvp session
Codes: DI:Ingress Detour  DT:Transit Detour  DM:Merged Detour
       DE:Egress Detour  BI:Ingress Backup BM: Merged Backup BE:Egress Backup
       RP:Repaired Session BYI: Bypass Ingress

Total Number of such sessions are: 13

Ingress RSVP:  13 session(s)
To              From                St Style Lbl_In  Lbl_Out Out_If    LSPname
13.14.13.13     30.11.1.30(DI)      Up SE    -       3762    Eth 0/6   to13_f30_1
13.14.13.13     30.11.1.30          Up SE    -       2048    Eth 0/5   to13_f30_1
13.14.13.13     30.11.1.30(DI)      Up SE    -       2903    Eth 0/6   to13_f30_2
13.14.13.13     30.11.1.30          Up SE    -       2639    Eth 0/5   to13_f30_2
13.14.13.13     30.11.1.30(DI)      Up SE    -       2066    Eth 0/5   to13_f30_3
                                                                       100
13.14.13.13     30.11.1.30          Up SE    -       2051    Eth 0/6   to13_f30_3
                                                                       100
13.14.13.14     30.11.1.30(DI)      Up SE    -       2154    Eth 0/5   to13_f30_4
                                                                       1000
13.14.13.14     30.11.1.30          Up SE    -       2052    Eth 0/6   to13_f30_4
                                                                       1000
13.14.13.14     30.11.1.30(DI)      Up SE    -       2083    Eth 0/5   to13_f30_5
                                                                       101
13.14.13.14     30.11.1.30          Up SE    -       2053    Eth 0/6   to13_f30_5
                                                                       101
13.14.13.14     30.11.1.30(DI)      Up SE    -       2153    Eth 0/6   to13_f30_6
                                                                       102
13.14.13.14     30.11.1.30          Up SE    -       2054    Eth 0/5   to13_f30_6
                                                                       102
13.14.13.14     30.11.1.30(DI)      Up SE    -       3496    Eth 0/5   to13_f30_7
                                                                       103
13.14.13.14     30.11.1.30          Up SE    -       3000    Eth 0/6   to13_f30_7
                                                                       103
13.14.13.14     30.11.1.30(DI)      Up SE    -       2156    Eth 0/5   to13_f30_8
                                                                       104
```

```
13.14.13.14     30.11.1.30          Up SE    -       2056    Eth 0/6   to13_f30_8
                                                                       104
13.14.13.14     30.11.1.30(DI)      Up SE    -       2157    Eth 0/6   to13_f30_9
                                                                       105
13.14.13.14     30.11.1.30          Up SE    -       2057    Eth 0/5   to13_f30_9
                                                                       105
13.14.13.14     30.11.1.30(DI)      Up SE    -       2158    Eth 0/6   to13_f30_9
                                                                       06
13.14.13.14     30.11.1.30          Up SE    -       2059    Eth 0/5   to13_f30_9
                                                                       06
13.14.13.14     30.11.1.30(DI)      Up SE    -       3319    Eth 0/5   to13_f30_9
                                                                       07
13.14.13.14     30.11.1.30          Up SE    -       2849    Eth 0/6   to13_f30_9
                                                                       07
13.14.13.14     30.11.1.30(DI)      Up SE    -       2160    Eth 0/6   to13_f30_9
                                                                       08
13.14.13.14     30.11.1.30          Up SE    -       2061    Eth 0/5   to13_f30_9
                                                                       08
13.14.13.14     30.11.1.30(DI)      Up SE    -       2161    Eth 0/5   to13_f30_9
                                                                       09
13.14.13.14     30.11.1.30          Up SE    -       2063    Eth 0/6   to13_f30_9
                                                                       09
```

The following example displays a sample output of the **show mpls rsvp session backup** command.

```
device# show mpls rsvp session backup
Codes: DI:Ingress Detour  DT:Transit Detour  DM:Merged Detour
       DE:Egress Detour  BI:Ingress Backup BM: Merged Backup BE:Egress Backup
       RP:Repaired Session BYI: Bypass Ingress

Total Number of such sessions are: 4000

Ingress RSVP:  2000 session(s)
To              From                St Style Lbl_In  Lbl_Out Out_If    LSPname
172.16.50.1     172.16.20.1         Up SE    -       2360    Ve 41     R20_to_R50
                                                                       _p3_p3_1
172.16.50.1     172.16.20.1(BI)     Up -     -       3581    Ve 52     R20_to_R50
                                                                       _p3_p3_1
172.16.50.1     172.16.20.1         Up SE    -       2131    Ve 41     R20_to_R50
                                                                       _p3_p3_10
172.16.50.1     172.16.20.1(BI)     Up -     -       3076    Ve 52     R20_to_R50
                                                                       _p3_p3_10
172.16.50.1     172.16.20.1         Up SE    -       2130    Ve 41     R20_to_R50
                                                                       _p3_p3_100
172.16.50.1     172.16.20.1(BI)     Up -     -       3075    Ve 52     R20_to_R50
                                                                       _p3_p3_100
172.16.50.1     172.16.20.1         Up SE    -       2129    Ve 41     R20_to_R50
                                                                       _p3_p3_100
                                                                       0
172.16.50.1     172.16.20.1(BI)     Up -     -       3074    Ve 52     R20_to_R50
                                                                       _p3_p3_100
                                                                       0
172.16.50.1     172.16.20.1         Up SE    -       2128    Ve 41     R20_to_R50
                                                                       _p3_p3_101
172.16.50.1     172.16.20.1(BI)     Up -     -       3073    Ve 52     R20_to_R50
                                                                       _p3_p3_101
172.16.50.1     172.16.20.1         Up SE    -       2127    Ve 41     R20_to_R50
                                                                       _p3_p3_102
172.16.50.1     172.16.20.1(BI)     Up -     -       3072    Ve 52     R20_to_R50
                                                                       _p3_p3_102
172.16.50.1     172.16.20.1         Up SE    -       2126    Ve 41     R20_to_R50
                                                                       _p3_p3_103
```

```
172.16.50.1     172.16.20.1(BI)      Up -     -       4095    Ve 52     R20_to_R50
                                                                        _p3_p3_103
172.16.50.1     172.16.20.1          Up SE    -       2125    Ve 41     R20_to_R50
                                                                        _p3_p3_104
172.16.50.1     172.16.20.1(BI)      Up -     -       4089    Ve 52     R20_to_R50
                                                                        _p3_p3_104
172.16.50.1     172.16.20.1          Up SE    -       2124    Ve 41     R20_to_R50
                                                                        _p3_p3_105
172.16.50.1     172.16.20.1(BI)      Up -     -       4085    Ve 52     R20_to_R50
                                                                        _p3_p3_105
172.16.50.1     172.16.20.1          Up SE    -       2123    Ve 41     R20_to_R50
                                                                        _p3_p3_106
172.16.50.1     172.16.20.1(BI)      Up -     -       4084    Ve 52     R20_to_R50
                                                                        _p3_p3_106
172.16.50.1     172.16.20.1          Up SE    -       2122    Ve 41     R20_to_R50
                                                                        _p3_p3_107
172.16.50.1     172.16.20.1(BI)      Up -     -       4083    Ve 52     R20_to_R50
                                                                        _p3_p3_107
172.16.50.1     172.16.20.1          Up SE    -       2121    Ve 41     R20_to_R50
                                                                        _p3_p3_108
172.16.50.1     172.16.20.1(BI)      Up -     -       4079    Ve 52     R20_to_R50
                                                                        _p3_p3_108
172.16.50.1     172.16.20.1          Up SE    -       2120    Ve 41     R20_to_R50
                                                                        _p3_p3_109
172.16.50.1     172.16.20.1(BI)      Up -     -       4077    Ve 52     R20_to_R50
                                                                        _p3_p3_109
172.16.50.1     172.16.20.1          Up SE    -       2119    Ve 41     R20_to_R50
                                                                        _p3_p3_11
172.16.50.1     172.16.20.1(BI)      Up -     -       4069    Ve 52     R20_to_R50
                                                                        _p3_p3_11
172.16.50.1     172.16.20.1          Up SE    -       2118    Ve 41     R20_to_R50
                                                                        _p3_p3_110
172.16.50.1     172.16.20.1(BI)      Up -     -       4068    Ve 52     R20_to_R50
                                                                        _p3_p3_110
172.16.50.1     172.16.20.1          Up SE    -       2117    Ve 41     R20_to_R50
                                                                        _p3_p3_111
172.16.50.1     172.16.20.1(BI)      Up -     -       4066    Ve 52     R20_to_R50
Aborted: by user
device#
```

The following example displays a sample output of the **show mpls rsvp session** command using the wide option.

```
device# show mpls rsvp session wide
Codes: DI:Ingress Detour  DT:Transit Detour  DM:Merged Detour
       DE:Egress Detour  BI:Ingress Backup BM: Merged Backup BE:Egress Backup
       RP:Repaired Session BYI: Bypass Ingress

Total Number of such sessions are: 6

Ingress RSVP:     3 session(s)
To              From                 St Style Lbl_In  Lbl_Out Out_If    LSPname
19.19.19.19     29.29.29.29(BYI)     Up SE    -       3       Eth 0/4   my-bypass-transit
20.20.20.20     29.29.29.29(BYI)     Up SE    -       2049    Eth 0/1   my-bypass-ingress
20.20.20.20     29.29.29.29(BI)      Up -     -       3       Eth 0/1   my-fbkup-lsp-
ingress
20.20.20.20     29.29.29.29          Up SE    -       2056    Eth 0/3   my-fbkup-lsp-
ingress

Transit RSVP:     1 session(s)
To              From                 St Style Lbl_In  Lbl_Out Out_If    LSPname
19.19.19.19     18.18.18.18          Up SE    2048    3       Eth 0/3   my-fbkup-lsp-
transit
19.19.19.19     18.18.18.18(BI)      Up -     2048    3       Eth 0/4   my-fbkup-lsp-
```

```
transit

Egress RSVP:     2 session(s)
To              From                 St Style Lbl_In  Lbl_Out Out_If    LSPname
29.29.29.29     20.20.20.20          Up SE    3       -       -         my-fbkup-lsp-
egress
29.29.29.29     20.20.20.20          Up SE    3       -       -         my-bypass-
egress      Up SE    -       2051    Eth 1/6   to13_f30_3
                                                                        100
```

The following example displays a sample output of the **show mpls rsvp session** command with the detail option.

```
device# show mpls rsvp session detail
Codes: DI:Ingress Detour  DT:Transit Detour  DM:Merged Detour
       DE:Egress Detour  BI:Ingress Backup BM: Merged Backup BE:Egress Backup
       RP:Repaired Session BYI: Bypass Ingress

Total Number of such sessions are: 7

Ingress RSVP:     3 session(s)
To              From                 St Style Lbl_In  Lbl_Out Out_If    LSPname
19.19.19.19     29.29.29.29(BYI)     Up SE    -       3       Eth 0/4   my-bypass-
                                                                        transit
  Tunnel ID: 7, LSP ID: 1
  Time left in seconds (PATH refresh: 11, ttd: 4294156
                        RESV refresh: 21, ttd: 152)
  Tspec: peak 0 kbps rate 0 kbps size 0 bytes m 20 M 65535
   Setup priority: 7, hold priority: 0
   Session attribute flags:0x04
   (SE Style)
  Explicit path hop count: 1
   29.19.2.19 (S)
  Received RRO count: 1
   Protection codes/Rtr Id flag: P: Local  N: Node  B: Bandwidth  I: InUse R: RtrId
   29.19.2.19
  PATH sentto:   29.19.2.19      (Eth 1/4        ) (MD5 OFF), Message ID: --
  RESV rcvfrom:  29.19.2.19      (Eth 1/4        ) (MD5 OFF), Message ID: --

To              From                 St Style Lbl_In  Lbl_Out Out_If    LSPname
20.20.20.20     29.29.29.29(BYI)     Up SE    -       2049    Eth 0/1   my-bypass-
                                                                        ingress
  Tunnel ID: 6, LSP ID: 1
  Time left in seconds (PATH refresh: 9, ttd: 4294154
                        RESV refresh: 10, ttd: 154)
  Tspec: peak 0 kbps rate 0 kbps size 0 bytes m 20 M 65535
   Setup priority: 7, hold priority: 0
   Session attribute flags:0x04
   (SE Style)
  Explicit path hop count: 2
   18.29.1.18 (S) -> 18.20.1.20 (S)
  Received RRO count: 2
   Protection codes/Rtr Id flag: P: Local  N: Node  B: Bandwidth  I: InUse R: RtrId
   18.29.1.18  -> 18.20.1.20
  PATH sentto:   18.29.1.18      (Eth 0/1        ) (MD5 OFF), Message ID: --
  RESV rcvfrom:  18.29.1.18      (Eth 0/1        ) (MD5 OFF), Message ID: --

To              From                 St Style Lbl_In  Lbl_Out Out_If    LSPname
20.20.20.20     29.29.29.29(BI)      Up -     -       3       Eth 0/1   my-fbkup-l
                                                                        sp-ingress
  Tunnel ID: 8, LSP ID: 1
  Time left in seconds (PATH refresh: 0, ttd: 4294015)
  Tspec: peak 0 kbps rate 0 kbps size 0 bytes m 20 M 65535
   Setup priority: 7, hold priority: 0
```

```
   Session attribute flags:0x06
   (Label recording,SE Style)
  Explicit path hop count: 1
   20.20.20.20 (S)
  PATH rcvfrom: None (downstream only)
  PATH sentto:   20.20.20.20     (Eth 0/1        ) (MD5 OFF), Message ID: --
  Riding bypass lsp: my-bypass-ingress

To              From                St Style Lbl_In  Lbl_Out Out_If    LSPname
20.20.20.20     29.29.29.29         Up SE    -       2056    Eth 0/3   my-fbkup-l
                                                                       sp-ingress
  Tunnel ID: 8, LSP ID: 1
  Time left in seconds (PATH refresh: 14, ttd: 4294172
                        RESV refresh: 24, ttd: 122)
  Tspec: peak 0 kbps rate 0 kbps size 0 bytes m 20 M 65535
   Setup priority: 7, hold priority: 0
   Session attribute flags:0x17
   (Label recording,SE Style,Protection: Local,Node)
   Setup priority: 7, hold priority: 0
   Bandwidth: 0 kbps, hop limit: 255
   Backup LSP: UP.  Nexthop (node) protection available
    Bandwidth protection not available.
    Up/Down times: 1, num retries: 0
  Explicit path hop count: 2
   29.19.1.19 (S) -> 20.19.1.20 (S)
  Received RRO count: 2
   Protection codes/Rtr Id flag: P: Local  N: Node  B: Bandwidth  I: InUse R: RtrId
   29.19.1.19 (P) -> 20.19.1.20
  PATH sentto:   29.19.1.19      (Eth 0/3        ) (MD5 OFF), Message ID: --
  RESV rcvfrom:  29.19.1.19      (Eth 0/3        ) (MD5 OFF), Message ID: --


Transit RSVP:     1 session(s)
To              From                St Style Lbl_In  Lbl_Out Out_If    LSPname
19.19.19.19     18.18.18.18         Up SE    2048    3       Eth 0/3   my-fbkup-l
                                                                       sp-transit
  Tunnel ID: 4, LSP ID: 1
  Time left in seconds (PATH refresh: 29, ttd: 126
                        RESV refresh: 10, ttd: 146)
  Tspec: peak 0 kbps rate 0 kbps size 0 bytes m 20 M 65535
   Setup priority: 7, hold priority: 0
   Session attribute flags:0x17
   (Label recording,SE Style,Protection: Local,Node)
   Setup priority: 7, hold priority: 0
   Bandwidth: 0 kbps, hop limit: 255
   Backup LSP: UP.  Nexthop (link) protection available
    Bandwidth protection not available.
    Up/Down times: 1, num retries: 0
  Explicit path hop count: 1
   29.19.1.19 (S)
  Received RRO count: 1
   Protection codes/Rtr Id flag: P: Local  N: Node  B: Bandwidth  I: InUse R: RtrId
   29.19.1.19
  PATH rcvfrom:  18.29.1.18      (Eth 0/1        ) (MD5 OFF) , Message ID: --
  PATH sentto:   29.19.1.19      (Eth 0/3        ) (MD5 OFF), Message ID: --
  RESV rcvfrom:  29.19.1.19      (Eth 0/3        ) (MD5 OFF), Message ID: --

To              From                St Style Lbl_In  Lbl_Out Out_If    LSPname
19.19.19.19     18.18.18.18(BI)     Up -     2048    3       Eth 0/4   my-fbkup-l
                                                                       sp-transit
  Tunnel ID: 4, LSP ID: 1
  Time left in seconds (PATH refresh: 0, ttd: 4294317)
  Tspec: peak 0 kbps rate 0 kbps size 0 bytes m 20 M 65535
   Setup priority: 7, hold priority: 0
```

```
   Session attribute flags:0x06
   (Label recording,SE Style)
  Explicit path hop count: 1
   19.19.19.19 (S)
  PATH rcvfrom: None (downstream only)
  PATH sentto:   19.19.19.19     (Eth 1/4        ) (MD5 OFF), Message ID: --
  Riding bypass lsp: my-bypass-transit


Egress RSVP:     3 session(s)
To              From                 St Style Lbl_In  Lbl_Out Out_If    LSPname
29.29.29.29     20.20.20.20          Up SE    3       -       -         my-fbkup-l
                                                                        sp-egress
  Tunnel ID: 1, LSP ID: 1
  Time left in seconds (PATH refresh: 20, ttd: 133
                        RESV refresh: 38, ttd: 4293457)
  Tspec: peak 0 kbps rate 0 kbps size 0 bytes m 20 M 65535
   Setup priority: 7, hold priority: 0
   Session attribute flags:0x17
   (Label recording,SE Style,Protection: Local,Node)
   Setup priority: 7, hold priority: 0
   Bandwidth: 0 kbps, hop limit: 255
  PATH rcvfrom:  29.19.1.19      (Eth 0/3        ) (MD5 OFF) , Message ID: --

To              From                 St Style Lbl_In  Lbl_Out Out_If    LSPname
29.29.29.29     20.20.20.20          Up SE    3       -       -         my-bypass-
                                                                        egress
  Tunnel ID: 3, LSP ID: 1
  Time left in seconds (PATH refresh: 0, ttd: 142
                        RESV refresh: 1, ttd: 4293660)
  Tspec: peak 0 kbps rate 0 kbps size 0 bytes m 20 M 65535
   Setup priority: 7, hold priority: 0
   Session attribute flags:0x04
   (SE Style)
  PATH rcvfrom:  18.29.1.18      (Eth 0/1        ) (MD5 OFF) , Message ID: --

To              From                 St Style Lbl_In  Lbl_Out Out_If    LSPname
29.29.29.29     19.19.19.19          Up SE    3       -       -         dbyp-29.19
                                                                        .1.19-14
  Tunnel ID: 19, LSP ID: 1
  Time left in seconds (PATH refresh: 28, ttd: 156
                        RESV refresh: 15, ttd: 4293589)
  Tspec: peak 0 kbps rate 0 kbps size 0 bytes m 20 M 65535
   Setup priority: 7, hold priority: 0
   Session attribute flags:0x04
   (SE Style)
  PATH rcvfrom:  29.14.1.14      (Eth 0/7        ) (MD5 OFF) , Message ID: --
```

show mpls statistics

Displays MPLS statistics.

Syntax

show mpls statistics { **oam** }

show mpls statistics { **transit** [**label** *label* | **ldp** [*ip_addr* | *submask* | *label*] | **rsvp** *label*] }

show mpls statistics { **tunnel** [**destination** *ip_addr* | **index** *vif_index* | **ldp** [**destination** *ip_addr* | **index** *vif_index*] | **rsvp** [**destination** *ip_addr* | **index** *vif_index* | **name** *name*]] }

Parameters

oam

Displays the MPLS OAM statistics.

transit

Displays the MPLS transit statistics.
label *label*

Displays the MPLS transit statistics for the selected label.

ldp *ip_addr*

Displays the MPLS transit LDP statisticsfor the selected IP address.

rsvp

Displays the MPLS transit RSVP statistics .

tunnel

Displays the MPLS tunnel statistics.
destination *destination*

Displays the MPLS tunnel statistics for the selected tunnel destination.

index *vif_index*

Displays the MPLS tunnel statistics for the selected tunnel index.

The tunnel index is the index derived from tunnel interface, as displayed by the show mpls lsp detail command.

ldp

Displays the MPLS tunnel LDP statistics.

destination *destination*

Displays the MPLS tunnel statistics for the selected tunnel destination.

index *vif_index*

Displays the MPLS tunnel statistics for the selected tunnel index.

The tunnel index is the index derived from tunnel interface, as displayed by the show mpls lsp detail command.

rsvp

Displays the MPLS tunnel RSVP statistics.

destination *destination*

Displays the MPLS tunnel statistics for the selected tunnel destination.

index *vif_index*

Displays the MPLS tunnel statistics for the selected tunnel index.

The tunnel index is the index derived from tunnel interface, as displayed by the show mpls lsp detail command.

name *name*

Displays the MPLS tunnel statistics for the selected named tunnel.

Modes

Privileged EXEC mode

Usage Guidelines

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Output

The **show mpls statistics** command displays the following information:

The tunnel index displayed by this command is the LSP tunnel index maintained by MPLS. This index cannot be used to display the MPLS statistics. Use the **show mpls statistics tunnel** command to get the tunnel index for this purpose.

Output field	Description
Name	Tunnel name.
Intf	Interface tunnel name.
Prot	Protection code: L-Local, R- RtrId
Total Packets	Displays the total number of packets.
Total Bytes	Displays the total number of bytes.
Since Last Clear Packets	Displays the number of packets since last clear.
Since Last Clear Bytes	Displays the number of bytes since the last clear.
Rate Pkts/sec	Displays the packets per second rate.
Rate Bytes/sec	Displays the bytes per second rate.

Examples

The following example shows the command using the tunnel option.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp t2
device(config-router-mpls-lsp-t2)# show mpls statistics tunnel
                    Total                Since Last clear               Rate
Name  Intf   Prot   Packets   Bytes       Packets   Bytes     Pkts/sec   Bytes/sec
t1    tnl0   R      2004      28175882    2004      28175882  6             93919
t2    tnl1   L      3101      40373763    3101      40373763  10            134579
```

The following example shows the command using the tunnel rsvp option.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp t2
device(config-router-mpls-lsp-t2)# show mpls statistics tunnel rsvp
                    Total                 Since Last clear              Rate
Name  Intf          Packets   Bytes       Packets   Bytes     Pkts/sec   Bytes/sec
t1    tnl0          2004      28175882    2004      28175882  6             93919
```

The following example shows the command using the transit option.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp t2
device(config-router-mpls-lsp-t2)# show mpls statistics transit
                   Total                 Since Last clear               Rate
IN Label   Prot    Packets   Bytes       Packets   Bytes     Pkts/sec   Bytes/sec
2048       R       2004      28175882    2004      28175882  6             93919
2050       L       3101      40373763    3101      40373763  10            134579
```

The following example shows the command using the transit ldp option.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp t2
device(config-router-mpls-lsp-t2)# show mpls statistics transit ldp
                   Total                 Since Last clear               Rate
IN Label           Packets   Bytes       Packets   Bytes     Pkts/sec   Bytes/sec
2050               3101      40373763    3101      40373763  10            134579
```

show mpls te database

Displays MPLS TE information.

Syntax

show mpls te [**area** *ipv4_addr* | **detail** | **link** *ipv4_addr* | **node** *ipv4_addr*]

Parameters

area *ipv4_addr*

Displays the specified OSPF area or IS-IS level information.

detail

Displays detailed information.

link*ipv4_addr*

Displays the specified link information.

node*ipv4_addr*

Displays the specified node information by the node router ID.

Modes

Privileged EXEC mode

Usage Guidelines

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Fate-sharing group membership for any given TE link or node consists of its own membership to the group, and the TE node to which it belongs. The output from the **show mpls te database detail** command displays the fate-sharing groups to which the TE links or nodes belong.

Examples

In the following example output, node *10.20.20.20* displays fate-sharing group information for *group1/100* and *group2/10* .

```
device# show mpls te database detail
This Router is 10.100.100.100
Global Link Gen 21
Area 0
  NodeID: 10.20.20.20, Type: Router
info from applied local policies:
  cspf-group member information (name/penalty):
    group1/100
    Type: P2P, To: 10.1.1.1, Local: 10.1.1.2, Remote: 10.1.1.1, Gen 16
```

```
    Admin Group: 0x00000000
    Metric: 1
    Link BW: 10000000 kbits/sec
    Reservable BW: 10000000 kbits/sec
    Unreserved BW:
      [0] 10000000 kbits/sec [1] 10000000 kbits/sec
      [2] 10000000 kbits/sec [3] 10000000 kbits/sec
      [4] 10000000 kbits/sec [5] 10000000 kbits/sec
      [6] 10000000 kbits/sec [7] 10000000 kbits/sec
  info from applied local policies:
   cspf-group member information (name/penalty):
     group2/10
   Type: P2P, To: 10.1.2.1, Local: 10.1.2.2, Remote: 10.1.2.1, Gen 13
    Admin Group: 0x00000000
    Metric: 1
    Link BW: 10000000 kbits/sec
    Reservable BW: 10000000 kbits/sec
    Unreserved BW:
      [0] 10000000 kbits/sec [1] 10000000 kbits/sec
      [2] 10000000 kbits/sec [3] 10000000 kbits/sec
      [4] 10000000 kbits/sec [5] 10000000 kbits/sec
      [6] 10000000 kbits/sec [7] 10000000 kbits/sec
```

show mvrp

Displays the global MVRP information on the device including configured ports, global enable status, and global timer settings.

Syntax

show mvrp

Modes

Privileged EXEC mode

Usage Guidelines

This feature is supported on the SLX 9250, SLX 9540, SLX 9640, SLX 9740, Extreme 8720, and Extreme 8820 devices.

Output

The **show mvrp** command displays the following information:

Output field	Description
Total configured mvrp ports	Total number of configured MVRP ports on the device
Global Status	Whether MVRP is globally enabled or disabled
Join-timer (in centiseconds)	Global join timer setting
Leave-timer (in centiseconds)	Global leave timer setting
Leaveall-timer (in centiseconds)	Global leave-all timer setting
MVRP Port(s)	List of MVRP-enabled Ethernet or port-channel interfaces

Examples

The following example displays the global MRVP information on the device.

```
device# show mvrp
-----------------------------------------------------------------
Total configured mvrp ports            : 5
Global Status                          : Enabled
Join-timer(in centiseconds)            : 20
Leave-timer(in centiseconds)           : 100
Leaveall-timer(in centiseconds)        : 1000
-----------------------------------------------------------------
MVRP Port(s): eth1/1, eth1/5, eth1/7, eth1/9, po11
```

show mvrp attributes

Displays the VLAN information and MVRP FSM states for each VLAN including the port state for all or specific MVRP-enabled Ethernet or port-channel interfaces.

Syntax

show mvrp attributes [**interface** {**ethernet** *slot/port* | **port-channel** *number* }] [**vlan** *ID*]

Parameters

interface

Displays the MVRP information for a specific MVRP-enabled interface.

ethernet *slot/port*

Specifies an Ethernet interface.

port-channel *number*

Specifies the port-channel interface.

vlan *ID*

Specifies the VLAN ID.

Modes

Privileged EXEC mode

Usage Guidelines

This feature is supported on the SLX 9250, SLX 9540, SLX 9640, SLX 9740, Extreme 8720, and Extreme 8820 devices.

The **show mvrp attributes** command without any options displays the VLAN information and MVRP FSM states for each VLAN for all MVRP-enabled Ethernet and port-channel interfaces.

Output

The **show mvrp attributes** command displays the following information:

Output field	Description
Port/Port-Channel	MVRP Ethernet or port-channel interface
State	State of the port: Forwarding, Disabled, or Blocking
VLAN	VLAN ID

Output field	Description
Registrar State	• IN—Registered • LV—Leave-all • MT—Empty
Registrar Mgmt	• Normal—Dynamically added • Fixed—Statically added • Forbidden—Forbidden VLAN
Applicant State	Applicant record for each attribute; whether it has been actively making a declaration, or has been passive.

Examples

The following example displays MVRP attributes for all interfaces.

```
device# show mvrp attributes
Port : eth0/17   State : Disabled
-------------------------------------------------------------------------------
VLAN       Registrar            Registrar            Applicant
           State                Mgmt                 State
-------------------------------------------------------------------------------
Port : eth0/5    State : Forwarding
-------------------------------------------------------------------------------
VLAN       Registrar            Registrar            Applicant
           State                Mgmt                 State
-------------------------------------------------------------------------------
1          In                   Fixed                Quiet Active
5          Empty                Normal               Quiet Active
10         In                   Fixed                Quiet Active
Port : po10      State : Forwarding
-------------------------------------------------------------------------------
VLAN       Registrar            Registrar            Applicant
           State                Mgmt                 State
-------------------------------------------------------------------------------
1          In                   Fixed                Quiet Active
5          In                   Normal               Very Anxious Observer
10         Empty                Normal               Quiet Active
```

The following example displays MVRP attributes for a specified VLAN.

```
device# show mvrp attributes vlan 10
-------------------------------------------------------------------------------------------
PORT            VLAN       Registrar            Registrar            Applicant
                           State                Mgmt                 State
-------------------------------------------------------------------------------------------
eth0/5          10         In                   Fixed                Quiet
Active
po10            10         Empty                Normal               Quiet Active
```

show mvrp interface

Displays the MVRP information for an interface including status, timer and applicant-mode settings and information about registered, declared, and forbidden VLANs.

Syntax

show mvrp inteface { **ethernet** *slot/port* | **port-channel** *number* }

Parameters

ethernet *slot/port*

Specifies the Ethernet interface.

port-channel *number*

Specifies the port channel of the interface.

Modes

Privileged EXEC mode

Usage Guidelines

This feature is supported on the SLX 9250, SLX 9540, SLX 9640, SLX 9740, Extreme 8720, and Extreme 8820 devices.

Output

The **show mvrp interface** command displays the following information:

Output field	Description
MVRP Status	Whether MVRP is enabled or disabled on the interface
Join-timer (in centiseconds)	Join timer setting configured on the interface
Leave-timer (in centiseconds)	Leave timer setting configured on the interface
Leaveall-timer (in centiseconds)	Leave-all timer setting configured on the interface
P2p	Whether the interface is a point-to-point
Applicant Mode	Whether the interface applicant mode is a normal-participant or non-participant
Registered Vlan(s)	List of registered VLANs on the interface
Declared Vlan(s)	List of declared VLANs on the interface
Forbidden Vlan(s)	List of forbidden VLANs on the interface

Examples

The following example displays the MVRP information for an Ethernet interface.

```
device# show mvrp interface ethernet 0/1
-------------------------------------------------------------------------------------------
MVRP Status                             : Enabled
Join-timer(in centiseconds)             : 20
Leave-timer(in centiseconds)            : 100
Leaveall-timer(in centiseconds)         : 1000
P2p                                     : Yes
Applicant Mode                          : normal-participant
-------------------------------------------------------------------------------------------
Registered Vlan(s)                      : 1 to 60 77 100 to 500 999
Declared Vlan(s)                        : 1 to 60 77 100 to 500 999
Forbidden Vlan(s)                       : 10
-------------------------------------------------------------------------------------------
```

show mvrp statistics

Displays statistics for received and transmitted MVRP messages on the MVRP-enabled interfaces.

Syntax

show mvrp statistics [**interface** { **ethernet** *slot/port* | **port-channel** *number* }]

Parameters

interface

Displays the MVRP statistics for a specific MVRP-enabled interface.

ethernet *slot/port*

Specifies an Ethernet interface.

port-channel *number*

Specifies the port-channel interface.

Modes

Privileged EXEC mode

Usage Guidelines

This feature is supported on the SLX 9250, SLX 9540, SLX 9640, SLX 9740, Extreme 8720, and Extreme 8820 devices.

The **show mvrp statistics** command when executed without any options, displays the statistics for all MVRP-enabled interfaces. Execute the **show mvrp statistics** command with the *interface* option to display statistics of *ethernet* or *port-channel* interfaces.

Output

The **show mvrp statistics** command displays the following information:

Output field	Description
Port/Port-Channel	Ethernet or port-channel interface.
Message type	Received or transmitted MVRP message type.
New	Count of new messages.
In	Count of IN messages. This message type is for attributes that are not declared but registered on the interface.

Output field	Description
Join In	Count of Join In messages. This message type is for attributes that are declared as well as registered on the interface.
Join Empty	Count of Join Empty messages. This message type is for attributes that are declared but not registered on the interface
Leave	Count of Leave event messages indicating the withdrawal of a VLAN.
Leave-all	Count of Leave-all event messages for the garbage collection of VLANs from the entire topology.
Total PDUs	Total number of MVRPDU messages on the interface.

Examples

The following example displays the statistics for all MVRP-enabled interfaces.

```
device# show mvrp statistics
Port : eth0/1
-------------------------------------------------------------------------------
Message type                    Transmitted  Received
-------------------------------------------------------------------------------
New                             0            0
In                              0            1809
Join In                         1816         0
Join Empty                      1788         0
Empty                           0            771
Leave                           99           0
Leave-all                       264          512
-------------------------------------------------------------------------------
Total PDUs                      1827         1293
-------------------------------------------------------------------------------
Port-channel : Po100
-------------------------------------------------------------
Message type                    Transmitted  Received
-------------------------------------------------------------------------------
New                             0            2
In                              693          0
Join In                         1800         1777
Join Empty                      0            1956
Empty                           396          0
Leave                           0            96
Leave-all                       369          346
-------------------------------------------------------------------------------
Total PDUs                      1807         1799
-------------------------------------------------------------------------------
```

show netconf

Displays NETCONF session.

Syntax

show netconf

Modes

Privileged EXEC mode

Usage Guidelines

The text output is extensive. Extreme Networks recommends redirecting the output to a text file.

Examples

Typical NETCONF session output.

```
device# show netconf
netconf-state capabilities capability urn:ietf:params:netconf:base:1.0
netconf-state capabilities capability urn:ietf:params:netconf:base:1.1
netconf-state capabilities capability urn:ietf:params:netconf:capability:writable-
running:1.0
netconf-state capabilities capability urn:ietf:params:netconf:capability:startup:1.0
netconf-state capabilities capability urn:ietf:params:netconf:capability:xpath:1.0
netconf-state capabilities capability urn:ietf:params:netconf:capability:validate:1.0
netconf-state capabilities capability urn:ietf:params:netconf:capability:validate:1.1
netconf-state capabilities capability http://tail-f.com/ns/netconf/actions/1.0
<output truncated>
```

show netconf capabilities

Displays the capabilities associated with each NETCONF session.

Syntax

show netconf capabilities

Modes

Privileged EXEC mode

Usage Guidelines

Because the text output is extensive, we recommend redirecting the output to a text file.

Examples

Typical command example of output.

```
device# show netconf capabilities
netconf-state capabilities capability urn:ietf:params:netconf:base:1.0
netconf-state capabilities capability urn:ietf:params:netconf:base:1.1
netconf-state capabilities capability urn:ietf:params:netconf:capability:writable-
running:1.0
netconf-state capabilities capability urn:ietf:params:netconf:capability:startup:1.0
netconf-state capabilities capability urn:ietf:params:netconf:capability:xpath:1.0
netconf-state capabilities capability urn:ietf:params:netconf:capability:validate:1.0
netconf-state capabilities capability urn:ietf:params:netconf:capability:validate:1.1
netconf-state capabilities capability http://tail-f.com/ns/netconf/actions/1.0
<output truncated>
```

show notification stream

Displays notifications about the event stream.

Syntax

show notification stream

Modes

Privileged EXEC mode

Examples

Typical output example for this command.

```
device# show notification stream ?
Possible completions:
  no event streams present
```

show ntp status

Displays the Network Time Protocol (NTP) status.

Syntax

show ntp status

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the active NTP server. If an NTP server is not configured, the command output displays the server as "LOCL". Otherwise, the command displays the NTP server IP address.

Examples

To show the local device NTP status when NTP server is configured:

```
device# show ntp status
 Clock is synchronized, stratum 3, reference clock is 10.20.232.222
 precision is 2**-22
 reference time is e0bdcea2.94df0a0d (10:59:46.2497645069 GMT Wed Jun 26 2019)
 clock offset is 0.0854 msec, root delay is 69.0540 msec
 root dispersion is 34.5350 msec, peer dispersion is 31.9061 msec
 system poll interval is 64, last clock update was 300 sec ago

 NTP server mode is enabled, NTP client mode is enabled
 NTP master mode is disabled
```

show ntp status association detail

This command lists detailed NTP server and peer association information. You can view detailed information of one NTP server and peer.

Syntax

show ntp status association detail { **ipv4 address** | **ipv6 address** }

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to view detailed information of one NTP server and peer.

Examples

To show the NTP status association details.

```
device# show ntp status association detail

131.216.1.101 configured server, sys peer, stratum 2
 ref ID 204.123.2.5, time d21da706.1ed27000 (16:14:22.517107712 GMT+05:30 Fri Jan 20 2017)
 our mode client, peer mode server, our poll intvl 6, peer poll intvl 6,
 root delay 0.02256774 msec, root disp 0.01150512, reach 377, root dist 0.36969603
 delay 290.94232711 msec, offset -1.08355772 msec, dispersion 4.58729275,
 precision 2**-16, version 4
 org time d21da713.f8f25000 (16:14:35.4176629760 GMT+05:30 Fri Jan 6 2017)
 rcv time d21da714.2602742a (16:14:36.637695018 GMT+05:30 Fri Jan 6 2017)
 xmt time d21da713.d31f723f (16:14:35.3542053439 GMT+05:30 Fri Jan 6 2017)
 filter delay    296.5594  322.7792  323.5571  297.6697  290.9942  303.5554  305.9971
295.0019
 filter offset     0.4430  -13.4441  -14.2241   -4.0003   -1.0083   -1.4414   -3.0034
1.9941
 filter disp       1.9984    1.0025    0.0035    6.8889    5.8899    4.8895    3.9920
2.9944
 filter epoch        5779      5843      5909      5452      5518      5585
5650      5715
```

The output fields are:	
server	Indicates server is statically configured.
symmetric active peer	Indicates peer is statically configured.
symmetric passive peer	Indicates peer is dynamically configured.
sys_peer	This peer is the system peer.
candidate	survivor in the selection algorithm. This peer is chosen as candidate in the combine algorithm.
reject	This peer is rejected by the selection algorithm.

The output fields are:	
falsetick	This peer is dropped as falseticker by the selection algorithm.
outlyer	This peer is dropped as outlyer by the clustering algorithm.
Stratum	Stratum number
ref ID	IPv4 address or hash of IPv6 address of the upstream time server to which the peer is synchronized.
Time	Last time stamp that the peer received from its master.
our mode	This system's mode relative to peer (active /passive /client /server / bdcast /bdcast client).
peer mode	Mode of peer relative to this system.
our poll intvl	This system's poll interval to this peer.
peer poll intvl	Poll interval of peer to this system.
root delay	The delay along path to root (the final stratum 1 time source).
root disp	Dispersion of path to root.
reach peer	The peer reachability (bit string in octal).
Delay	Round-trip delay to peer.
offset	Offset of peer clock relative to this clock.
Dispersion	Dispersion of peer clock.
precision	Precision of peer clock.
version	Peer NTP version number.
org time	Originate time stamp of the last packet.
rcv time	Receive time stamp of the last packet.
xmt time	Transmit time stamp of the last packet.
filter delay	Round-trip delay in milliseconds of last 8 samples.
filter offset	Clock offset in milliseconds of last 8 samples.
filter error	Approximate error of last 8 samples.

show ntp status associations

Displays NTP servers and peers association.

Syntax

show ntp associations

Modes

Privileged EXEC mode

Examples

To show the NTP server status associations.

```
device# show ntp status associations
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
2620:100:0:f404  .PPS.            1 u   20   64   17    0.460   -4.844   0.897
+216.45.57.38    20.162.227.208   2 u  502 1024  377  241.941   12.103  10.920
-172.19.69.1     172.82.134.51    3 u  741 1024  377  223.985   -7.426   2.571
*216.45.57.38    128.252.19.1     2 u  884 1024  377  230.046    1.422   5.871
+10.0.017        208.75.89.4      3 u  858 1024  377  211.094   -1.801   6.431

* synced, # selected, + candidate, - outlayer, x falseticker
```

The character in the left margin indicates the fate of this server/peer in the clock selection process.

The output fields are:	
<space>	Discarded as not valid (TEST10-TEST13).
x	Discarded as falseticker in the selection algorithm.
-	Discarded as outlier in the clustering algorithm.
+	Candidate in the combine algorithm.
#	Survivor in the selection algorithm.
remote	IPv4 or IPv6 address of the peer.
refid	Reference clock type or address for the peer or kisscode.
st	Stratum setting for the peer.
when	Sec/min/hr since last received packet
poll	Poll interval (log2 s)
reach	Reach shift register (octal)
delay	Round-trip delay to peer, in milliseconds.

The output fields are:	
offset	Relative time difference between a peer clock and a local clock, in milliseconds.
jitter	Jitter

show overlay-gateway

Displays status and statistics for the VXLAN overlay-gateway instance.

Syntax

show overlay-gateway [**name** *name* | **vlan statistics** | **statistics**]

Parameters

name

Name of the configured VXLAN gateway.

vlan statistics

Displays statistics for each VLAN for the VXLAN gateway. Statistics include transmitted and received packet counts and byte counts exchanged for each exported VLAN. Because each exported VLAN maps to a VXLAN, these statistics apply on a per-VXLAN-counters basis. Per-VLAN counters are not enabled by default. You need to first run the **enable statistics direction** command for the gateway to enable statistics for specified VLAN IDs.

statistics

Displays statistics for the VXLAN gateway. Statistics include transmitted and received packet counts and byte counts. These counters are derived by aggregating tunnel counters for all the tunnels of the gateway.

Modes

Privileged EXEC mode

Usage Guidelines

Output includes the gateway name, the system-assigned gateway ID, source IP address, VRF, administration state, and number of tunnels associated. Additionally, the output displays the QoS TTL and DSCP modes for VxLAN tunnels in all supported platforms.

If you specify the gateway name, the gateway must already be configured.

Examples

To show the status for a gateway instance that is configured for Layer 2 extension with a loopback interface:

```
device# show overlay-gateway
    Overlay Gateway "GW1", ID 1
    Type Layer2-Extension, Tunnel mode VXLAN
    IP address 10.10.10.1 (Loopback 10), Vrf default-vrf
    Admin state up
        QOS mode TTL: PIPE, DSCP: PIPE
        Number of tunnels 2
```

```
        Packet count: RX 0               TX 0
        Byte count  : RX (NA)            TX 0
```

To show statistics for the gateway instance:

```
device# show overlay-gateway statistics

Gateway Name          RX packets      TX packets      RX bytes        TX bytes
==================== =============== =============== ========= ==============
GW1                   200000          10000           22227772        1110111
```

To display statistics for VLANs attached to the VXLAN gateway:

```
device# show overlay-gateway name GW1 vlan statistics

                              Packets          Bytes
VLAN    VNI     Tx      Rx        Tx         Rx
-----------------------------------------------------
10      1010   10000   200000    1110111    22227772
11      1011   2200    -         221334     -
21      1021   -       1         -          100


device# show overlay-gateway name test vlan statistics
VLAN ID   RX packets           TX packets
========= ==================== ====================
30        0                    0
40        3696                 3696
```

show onieversion

Displays the installed version of ONIE.

Syntax

show onieversion

Modes

Privileged EXEC Mode

Usage Guidelines

This command is only supported on the SLX 9150, SLX 9250, Extreme 8720, and Extreme 8520 devices.

Examples

This example shows the usage of the command.

```
SLX # show onieversion
ONIE Version=2020.05.00.07
SLX #
```

show policy-map

Displays information for the configured policy maps including class-map policer parameters.

Syntax

show policy-map [**control-plane** [**map-name** *policyname*]] | [**details** *policyname* | [{ **interface** [**ethernet** *slot/port* | **ve** *ve-id*] } | **system**] [**input** | **output**]]

Parameters

control-plane [**map-name** *policyname*]

Displays the policy map in the control plane.

details *policyname*

Displays the detail configuration of the policy map along with binding information.

interface [**ethernet** *slot/port* | **ve** *ve-id*]

Displays the information of the policy map for the specified interface. Enter a valid slot and port number for an Ethernet or a Virtual Ethernet (VE) interface.

system map-name *policyname*

Displays the information for the globally-applied policy map.

input

Inbound - direction where the policy map is applied.

output

Outbound - direction where the policy map is applied.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command without any keywords to display all policy map binding information including the control plane and all interfaces.

Output

The **show policy-map** command displays the following information:

Output field	Description
Interface	The interface for which rate limiting information is being displayed.
Direction	The traffic direction for which rate limiting is applied.
police-priority-map	Remarked priority map used for Policer application (802.1 p priority remarked map).
Conform	The traffic in bytes that has been forwarded from this interface that is within the CIR bandwidth limits.
Exceeded	The traffic that has been exceeded the bandwidth available in the CIR limits and has not exceed the EIR limits for this rate-limit policy.
Violated	The traffic that has exceeded the bandwidth available in the CIR and EIR limits.

Examples

The following example displays all policy map binding information including the control plane and all interfaces.

```
device# show policy-map
Number of policy maps : 46
Policy-Map cp-pmap1
  Bound To: ControlPlane(in)
Policy-Map P1-DEFAULT-RL
  Bound To:None
Policy-Map P2-DEFAULT-RL-10000000000
  Bound To: Eth 1/27(in)
Policy-Map P3-DEFAULT-RL-1500000000
  Bound To:None
….
```

The following example displays the policy map in the control plane.

```
device# show policy-map control-plane

Ingress Direction :
Policy-Map cp-pmap1
  Class cm1
    matches 480661 packets 61524608 bytes
    Police cir 22222
     Stats:
       Operational cir:22000 cbs:3332 eir:0 ebs:0
       Conform Byte:0 Exceed Byte:0 Violate Byte:0
```

The following example displays the interface-specific policy-map information.

```
device# show policy-map interface ethernet 1/1 in

Ingress Direction :
Policy-Map p2
```

```
Class c2
matches 7867567 packets 1007048576 bytes
Police cir 1000000
       Stats:
         Operational cir:1010000 cbs:149999 eir:0 ebs:0
         Conform Byte:1180928 Exceed Byte:0 Violate Byte:1005867648
```

The following example displays the system-specific policy-map information.

```
device# # show policy-map system map-name pm1

Ingress Direction :
Policy-Map pm1
Class cm1
matches 480661 packets 61524608 bytes
Police cir 100000
Stats:
 Operational cir:109000 cbs:14999 eir:0 ebs:0
  Conform Byte:265088 Exceed Byte:0 Violate Byte:0
```

This example shows the configuration of the policy map that is attached to a control plane interface.

```
device# show policy-map control-plane

Ingress Direction :
 Policy-Map map-ssh
    Class class-ssh-2
      matches 91785 packets 11748480 bytes
      Police cir 100000
        Stats:
          Operational cir:102000 cbs:15000 eir:0 ebs:0
          Conform Byte:11748480 Exceed Byte:0 Violate Byte:0

    Class class-ssh-3
      matches 91764 packets 11745792 bytes
      Police cir 1000000
        Stats:
          Operational cir:997000 cbs:150000 eir:0 ebs:0
          Conform Byte:11745792 Exceed Byte:0 Violate Byte:0
```

To display the configured policy-map details at **ingress** direction.

```
SLX# show policy-map interface Ve 100 in

Ingress Direction :
 Policy-Map policy-map_1
    Class class-map_1
      matches 0 packets 0 bytes
      Police cir 1111111 eir 1111111
        Stats:
          Operational cir:1112000 cbs:166665 eir:1112000 ebs:166665
          Conform Byte:0 Exceed Byte:0 Violate Byte:0
SLX#
```

To display the configured policy-map details at **egress** direction.

```
SLX# show policy-map interface Ve 100 out

Egress Direction :
 Policy-Map policy-map_2
    Class class-map_2
      matches 0 packets 0 bytes
      Police cir 1111111 eir 1111111
        Stats:
```

```
          Operational cir:1112000 cbs:166665 eir:1112000 ebs:166665
          Conform Byte:0 Exceed Byte:0 Violate Byte:0
SLX#
```

To display the configured policy-map details for both direction.

```
SLX# show policy-map interface Ve 100

Ingress Direction
 Policy-Map policy-map_1
    Class class-map_1
      matches 0 packets 0 bytes
      Police cir 1111111 eir 1111111
        Stats:
          Operational cir:1112000 cbs:166665 eir:1112000 ebs:166665
          Conform Byte:0 Exceed Byte:0 Violate Byte:0

Egress Direction
 Policy-Map policy-map_1
    Class class-map_1
      matches 0 packets 0 bytes
      Police cir 1111111 eir 1111111
        Stats:
          Operational cir:1112000 cbs:166665 eir:1112000 ebs:166665
          Conform Byte:0 Exceed Byte:0 Violate Byte:0
SLX#
```

```
To clear the policy-map counters at ingress direction:
SLX# clear policy-map-counters interface Ve 100 in

To clear the policy-map counters at egress direction:
SLX# clear policy-map-counters interface Ve 100 out

To clear the policy-map counters for both direction:
SLX# clear policy-map-counters interface Ve 100
```

show port-channel

Displays the link aggregation group (LAG) information for a port-channel.

Syntax

show port-channel [*number* | **detail** | **summary**]

Parameters

number

Specifies a LAG port-channel group number.

detail

Displays detailed LAG information for a port-channel.

summary

Displays the summary information per channel-group.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the LAGs present on the system with details about the LACP counters on their member links. LAG interfaces are called port-channels.

If you do not specify a port-channel, all port-channels are displayed.

When using the **show port-channel** *number* command, an asterisk in the command output designates that the designated port channel is the primary link through which the BUM (broadcast, unknown unicast and multicast) traffic flows.

Examples

The following example displays detailed port-channel information.

```
device# show port-channel detail
 LACP Aggregator: Po 10
 Aggregator type: Standard
  Actor System ID - 0x8000,f4-6e-95-9f-13-e2
  Admin Key: 0010 - Oper Key 0010
  Receive link count: 2 - Transmit link count: 2
  Individual: 0 - Ready: 1
  Partner System ID - 0x8000,f4-6e-95-9f-15-a4
  Partner Oper Key 0010
 Flag * indicates: Primary link in port-channel
 Number of Ports: 2
 Minimum links: 1
 Member ports:
   Link: Eth 0/9 (0xC012140) sync: 1
   Link: Eth 0/10 (0xC014140) sync: 1   *
```

The following example displays the summary output of a port-channel.

```
device# show port-channel summary
Flags:  D - Down               P - Up in port-channel

(members)
        U - Up (port-channel)   * - Primary link in port-

channel
        S - Switched
        M - Not in use. Min-links not met
===== =============== ========== ===============
Group Port-channel    Protocol   Member ports
===== =============== ========== ===============
1     Po 1    (D)     None
```

show port-channel load-balance

Displays the load balance configuration information for the system.

Syntax

show port-channel load-balance

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the load balance configuration on the system.

Examples

The following example displays the output for the load balancing configuration on an Extreme 8820.

```
SLX # show port-channel load-balance
Header parameters
        Ethernet Mask: smac-dmac etype vlan
        ip: sip-dip protocol
        ipv6: sipv6-dipv6 ipv6-next-hdr
        l4: src-dst-port
        mpls: all-labels

Hash Settings
        normalize:0, rotate:3
SLX #
```

The following example displays the output for the load balancing configuration on a SLX 9150.

```
SLX # show port-channel load-balance
Header parameters
    Ethernet Mask: sa-mac da-mac etype vlan
    ip: src-ip dst-ip protocol src-l4-port dst-l4-port
    ipv6: ipv6-src-ip ipv6-dst-ip ipv6-next-hdr ipv6-src-l4-port ipv6-dst-l4-port

Hash Settings
    hdr-start:Forwarding, hdr-count:3, include_src_port:0
load-balance-type hash-based

SLX #
```

The following example displays the output for the load balancing configuration on a Extreme 8820 device.

```


SLX # show port-channel load-balance
      Header parameters
              Ethernet Mask: smac-dmac etype vlan
              ip: sip-dip protocol
```

```
              ipv6: sipv6-dipv6 ipv6-next-hdr
              l4: src-dst-port
              mpls: all-labels

      Hash Settings
              hdr-start:LastTerminated, normalize:0, rotate:3
```

show port port-channel ethernet

Displays the detailed LACP attributes that are configured and negotiated with its partner.

Syntax

show port port-channel ethernet *port_id*

Parameters

port_id

Specifies the port to display.

Modes

Privileged EXEC mode

Examples

The following example displays the LACP attributes for an Ethernet interface.

```
device# show port port-channel ethernet 0/6
 LACP link info: eth 0/6 - 0x118430006
 Actor System ID: 0x8000,01-e0-52-00-00-01
 Partner System ID: 0x0000,00-00-00-00-00-00
 Actor port priority: 0x8000 (32768)
 Admin key: 0x0003 (3) Oper key: 0x0003 (3)
 Receive machine state : Defaulted
 Periodic Transmission machine state : Fast periodic
 Mux machine state : Waiting
 Admin state: ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
 Oper state: ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
 Partner oper state: ACT:0 TIM:1 AGG:1 SYN:1 COL:0 DIS:0 DEF:1 EXP:0
 Partner oper port: 0
 Selected: :2
 Defaulted State Action: No Default-Up
```

show port-security

Displays the configuration information related to port security.

Syntax

show port-security [**addresses** | **interface ethernet** *slot/port*]

Modes

Privileged EXEC mode

Interface configuration mode

Output

The **show port-security** command displays the following information:

Output field	Description
Secure Port	The port on which port MAC security is enabled.
MaxSecureAddress (count)	The maximum limit for the number of secure MAC addresses allowed on the interface.
StaticSec (count)	The number of MAC addresses that are manually configured.
Violated	The status that shows whether the port security violation has occurred.
Action	The configured response action that will be taken when a port security violation occurs.
Sticky	The status that shows whether sticky MAC learning is enabled.
Port Security	The status that shows whether port MAC security is enabled.
Port Status	The status of the port.
Violation Mode	The configured response action that will be taken when a port security violation occurs.
Violated	The status that shows whether the port security violation has occurred.
Sticky Enabled	The status that shows whether sticky MAC learning is enabled.
Maximum MAC addresses	The maximum limit for the number of secure MAC addresses allowed on the interface.
Total MAC addresses	The total number of secure MAC addresses learned on the interface.
Configured MAC addresses	The total number of secure MAC addresses configured on the interface manually.
Last violation time	The time when the last port security violation occurred.
Shutdown time (in Minutes)	The configured auto recovery time for port security violation.
Vlan	The VLAN to which the port is mapped.
Mac-address	The secured MAC address.
Type	The types of secure MAC addresses that are used in port MAC security.
Ports	The port on which port MAC security is enabled.

Examples

To display the port MAC security configuration details across ports on the device, enter the following command:

```
device(conf-if-eth-3/2)# do show port-security
Secure    MaxSecureAddr  CurrentAddr  StaticSec  Violated  Action   Sticky
Port         (count)       (count)     (count)
Eth 3/2       10           0            1           No     Shutdown  No
```

To display the statistics of the port MAC security configured for an interface, enter the following command:

```
device(conf-if-eth-3/2)# do show port-security interface ethernet 3/2
Port Security               : Enabled
Port Status                 : Up
Violation Mode              : Shutdown
Violated                    : No
Sticky Enabled              : No
Maximum MAC addresses       : 10
Total MAC addresses         : 0
Configured MAC addresses    : 1
Last violation time         :
Shutdown time (in Minutes)  : 0
```

To list the secure MAC addresses configured on the device, enter the following command.

```
device(conf-if-eth-3/2)# do show port-security addresses
                    Secure Mac Address Table
------------------------------------------------------------------
Vlan       Mac-address            Type                      Ports
250        3200.1110.0002         Secure-Static             Eth 3/2
```

show process cpu

Displays information about the active processes in the switch and their corresponding CPU utilization statistics.

Syntax

show process cpu [**summary**] [**history**] [**top**] [**all-partitions**]

Parameters

summary

Displays a summary view of cpu usage.

history

Displays the history of CPU usage.

top

Displays current CPU utilization.

all-partitions

Displays a summary view of all partitions.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local device.

For an explanation of process states, refer to the UNIX manual page for the **ps** command.

Examples

The following example displays a summary of all processes.

```
device# show process cpu summary
 Realtime Statistics:
Total CPU Utilization: 0% (user procs:0%, system-kernel:0%, iowait:0%)
Load Average: One minute: 0.00; Five minutes: 0.03; Fifteen minutes: 0.01
```

The following example displays CPU usage information by processes.

```
device# show process cpu
 Realtime Statistics:
Total CPU Utilization: 0% (user procs:0%, system-kernel:0%, iowait:0%)
Load Average: One minute: 0.00; Five minutes: 0.02; Fifteen minutes: 0.00
Active Processes Lifetime Statistic:
  PID   Process          CPU%  State      Started
17169   sh                1.00    S       13:44:27 Jul  1, 2012
 2060   emd               0.80    S       21:52:27 Jun 29, 2012
```

```
 2462   SWITCH_TMR_0      0.60    S       21:53:08 Jun 29, 2012
17170   imishow_proc_cp   0.50    S       13:44:27 Jul  1, 2012
 2207   ospfd             0.20    S       21:52:41 Jun 29, 2012
 2211   mstpd             0.20    S       21:52:41 Jun 29, 2012
 2208   rtmd              0.10    S       21:52:41 Jun 29, 2012
(Output truncated)
```

show process info

Displays system processes hierarchically.

Syntax

show process info

Modes

Privileged EXEC mode

Usage Guidelines

Pagination is not supported with this command. Use **more** in the terminal window to display the output one page at a time.

This command is supported only on the local switch.

Examples

```
device# show process info

PID     CMD
2       kthreadd
3       \_ migration/0
4       \_ ksoftirqd/0
5       \_ watchdog/0
6       \_ migration/1
7       \_ ksoftirqd/1
8       \_ watchdog/1
9       \_ migration/2
10      \_ ksoftirqd/2
11      \_ watchdog/2
12      \_ migration/3
13      \_ ksoftirqd/3
14      \_ watchdog/3
15      \_ migration/4
16      \_ ksoftirqd/4
17      \_ watchdog/4
18      \_ migration/5
19      \_ ksoftirqd/5
20      \_ watchdog/5
21      \_ migration/6
22      \_ ksoftirqd/6
[Output truncated]
```

show process memory

Displays the memory usage information based on processes running in the system.

Syntax

show process memory [**summary**]

Parameters

summary

Displays a summary view of memory usage.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local device.

Examples

To show memory usage information by individual processes:

```
device# show process memory
%Memory Used: 24.8368%; TotalMemory: 8080312 KB; Total Used: 2006888 KB
Total Free: 6073424 KB; Low Free: 271728 KB; High Free: 4906964 KB; Cached: 747948 KB
  PID   Process          MEM%        VSIZE(KB)       RSS(KB)       PSS(KB)
 6954   hslagtd          3.30         707412         268644         264050
 4405   Dcmd             2.20         385352         182672         152818
 4652   postgres         2.10         216252         173192         143609
 4752   Mcdsd            0.90         235628          75204          47126
 5725   ribmgr           0.80         299724          71828          44743
 6958   fibagt           0.80         246888          69828          42998
 5726   srm              0.80         209512          67516          40639
 5718   nsm              0.60         323520          56376          28656
 5723   ospfd            0.60         326592          54836          27710
 5747   ospf6d           0.60         326364          54488          27389
 5738   arpd             0.60         239348          54328          27438
 5734   mstpd            0.60         214624          51368          24154
 5722   bgpd             0.60         340812          50976          23826
 4647   postgres         0.60         157476          48840          24130
 3623   raslogd          0.50         160440          47968          22327
 5739   iphelpd          0.50         259464          47112          20244
 5729   pimd             0.50         315092          46972          19983
 3640   snmpd            0.50         237116          46656          15292
 5730   mc_hms           0.50         299128          46496          19167
 5727   rpsd             0.50         296804          45580          18620
 5735   vrrpd            0.50         254660          44384          17446
 5750   bfdd             0.50         319116          44348          17457
 2594   confd            0.50          54236          43568          42450
 5724   mctd             0.50         232356          43224          16240
 5732   qosd             0.50         201584          41272          14225
 5744   sflowd           0.50         218208          41192          14140
```

```
 5749   tnlmgrd          0.50         220264          40988          14230
 6956   mcagtd           0.50         275560          40444          13511
 5731   ssmd             0.40         203412          40392          13322
 3626   pemd             0.40         229504          39972           9939
 5736   dauthd           0.40         192548          39544          12202
 5742   ptpd             0.40         191572          38372          11763
 5751   ctpd             0.40         205632          38076          11403
 5728   radv             0.40         181964          38060          11246
 5740   onmd             0.40         200644          37940          10597
 5720   l2sysd           0.40         190976          37792          10911
 5737   igmpd            0.40         193056          37576          10373
 5733   lacpd            0.40         183620          37364          10106
 5743   rmond            0.40         183568          37308          10059
 5721   mcast_ssd        0.40         216288          36624           9737
 6955   l2agtd           0.40         210108          36384           9697
 5741   eldd             0.40         188508          36292           9441
 5746   udldd            0.40         188404          36040           9272
 5745   pcapd            0.40         188492          36032           9347
 6959   tnlagtd          0.40         191432          35036           8593
 3630   pdmd             0.40         172824          34352           8118
 6957   qosagtd          0.30          99716          29360           7477
 3642   tsd              0.30         106700          27628           5874
 4877   postgres         0.30         166956          27572          21316
[output omitted, as will vary by device]
```

show qos cpu cfg

Displays information about the current CPU protection configuration.

Syntax

show qos cpu cfg slot *slot_id* [**burst** | **shaper** | **rate**]

Parameters

slot *slot_id*

Specifies a valid slot number. For devices that do not support line cards, specify **0**.

burst

Specifies port and group traffic burst rates for IPv6 subnet rate limiting.

shaper

Specifies port and group traffic shaper rates for IPv6 subnet rate limiting.

rate

Specifies shaping rate for IPv6 subnet rate limiting.

Modes

Privileged EXEC mode

Usage Guidelines

IPv6 subnet rate limiting is configured by means of the **ipv6 subnet-rate-limit** command.

Examples

To display information about the CPU configuration.

```
device# show qos cpu cfg slot 0
Slot 1 CPU QoS Config

CPU Port shaper rate: 5000 Kbps
CPU Group shaper rates (Kbps)
Group  Aggr   P0     P1     P2     P3     P4     P5     P6     P7
-------------------------------------------------------------------
  0    5000   5000   5000   5000   5000   5000   5000   5000   5000
  1    5000   5000   5000   5000   5000   5000   5000   5000   5000
  2    5000   5000   5000   5000   5000   5000   5000   5000   5000
  3    5000   5000   5000   5000   5000   5000   5000   5000   5000
  4    5000   5000   5000   5000   5000   5000   5000   5000   5000
  5    5000   5000   5000   5000   5000   5000   5000   5000   5000
  6    5000   5000   5000   5000   5000   5000   5000   5000   5000
  7    5000   5000   5000   5000   5000   5000   5000   5000   5000
  8    5000   5000   5000   5000   5000   5000   5000   5000   5000
  9    5000   5000   5000   5000   5000   5000   5000   5000   5000
 10    5000   5000   5000   5000   5000   5000   5000   5000   5000
```

```
 11    5000   5000   5000   5000   5000   5000   5000   5000   5000

CPU Port burst size: 1 Kbytes
CPU Group burst size (Kbytes)
Group  Aggr  P0    P1    P2    P3    P4    P5    P6    P7
-------------------------------------------------------------
  0    1     1     1     1     1     1     1     1     1
  1    1     1     1     1     1     1     1     1     1
  2    1     1     1     1     1     1     1     1     1
  3    1     1     1     1     1     1     1     1     1
  4    1     1     1     1     1     1     1     1     1
  5    1     1     1     1     1     1     1     1     1
  6    1     1     1     1     1     1     1     1     1
  7    1     1     1     1     1     1     1     1     1
  8    1     1     1     1     1     1     1     1     1
  9    1     1     1     1     1     1     1     1     1
 10    1     1     1     1     1     1     1     1     1
 11    1     1     1     1     1     1     1     1     1

CPU Group WFQ values
Group  Aggr  P0    P1    P2    P3    P4    P5    P6    P7
-------------------------------------------------------------
  0    1     20    50    50    50    50    50    50    100
  1    1     20    50    50    50    50    50    50    100
  2    1     20    50    50    50    50    50    50    100
  3    1     20    50    50    50    50    50    50    100
  4    1     20    50    50    50    50    50    50    100
  5    1     20    50    50    50    50    50    50    100
  6    1     20    50    50    50    50    50    50    100
  7    1     20    50    50    50    50    50    50    100
  8    1     20    50    50    50    50    50    50    100
  9    1     20    50    50    50    50    50    50    100
 10    1     20    50    50    50    50    50    50    100
 11    1     20    50    50    50    50    50    50    100
```

To display information only about the IPv6 subnet rate-limiting traffic shaper configuration.

```
device# show qos cpu cfg slot 0 shaper
Slot 0 CPU QoS Config

CPU Port shaper rate: 5000 Kbps
CPU Group shaper rates (Kbps)
Group  Aggr   P0     P1     P2     P3     P4     P5     P6     P7
-------------------------------------------------------------------
  0    5000   5000   5000   5000   5000   5000   5000   5000   5000
  1    5000   5000   5000   5000   5000   5000   5000   5000   5000
  2    5000   5000   5000   5000   5000   5000   5000   5000   5000
  3    5000   5000   5000   5000   5000   5000   5000   5000   5000
  4    5000   5000   5000   5000   5000   5000   5000   5000   5000
  5    5000   5000   5000   5000   5000   5000   5000   5000   5000
  6    5000   5000   5000   5000   5000   5000   5000   5000   5000
  7    5000   5000   5000   5000   5000   5000   5000   5000   5000
  8    5000   5000   5000   5000   5000   5000   5000   5000   5000
  9    5000   5000   5000   5000   5000   5000   5000   5000   5000
 10    5000   5000   5000   5000   5000   5000   5000   5000   5000
 11    5000   5000   5000   5000   5000   5000   5000   5000   5000
```

To display information only about the IPv6 subnet shaping rate configuration.

```
device# show qos cpu cfg slot 0 rate
```

```
Slot 0 CPU QoS Config

Name                  Egid   Group        Pkts       Bytes          PPS          bps
-------------------------------------------------------------------------------------
Protocol              7f80   0            0          0              0            0
Management            7f81   1
IP Host               7f82   2            11907      173855778      724          845632
MC RPF Fail           7f83   3            0          0              0            0
MC LHR                7f84   4            0          0              0            0
```

show qos cpu info

Displays information on CPU groups and effective group IDs (EGID).

Syntax

show qos cpu info

Modes

Privileged EXEC mode

Examples

```
device# show qos cpu info

Name                  Egid  Group  Description
-----------------------------------------------
Protocol              7f80    0    Protocol Packets (ARP, L2, etc)
Management            7f81    1    Management (ping, local route)
IP Host               7f82    2    IP Host (subnet route)
MC RPF Fail           7f83    3    Multicast RPF failure
MC LHR                7f84    4    Multicast RP and LHR
MC FHR                7f85    5    Multicast FHR
SFlow Port            7f86    6    SFlow Packets (Port sflow)
SFlow ACL In          7f87    6    ACL sflow ingress permit
SFlow ACL In Deny     7f88    6    ACL sFlow ingress deny
SFlow ACL Eg          7f89    6    ACL sflow egress permit
SFlow ACL Eg Deny     7f8a    6    ACL sflow egress deny
VXLAN Snoop           7f8b    6    VXLAN Visibility Snoop
ACL Log               7f8c    7    ACL Logging
ACL Log In            7f8d    7    ACL Logging ingress permit
ACL Log In Deny       7f8e    7    ACL Logging ingress deny
ACL Log Eg            7f8f    7    ACL Logging egress permit
ACL Log Eg Deny       7f90    7    ACL Logging egress deny
Snoop                 7f91    8    Snoop (VxLAN)
Diagnostics           7f92    9    Diagnostics and debug
OAM                   7f93   10    OAM and CFM
Exceptions            7f96   12    Errors, Exceptions (TTL, MTU)
ICMP Redirect         7f95   12    ICMP Redirect
```

show qos flowcontrol interface

Displays the configured flow control information for a specific interface, port channel, or all interfaces on the device.

Syntax

show qos flowcontrol interface { **all** | **ethernet** *slot/port* | **port-channel** *number* }

Parameters

all

Displays the flow control information on all interfaces.

ethernet *slot/port*

Displays the flow control information on the specified interface.

port-channel *number*

Displays the flow control information on the interface for the specified port channel.

Modes

Privileged EXEC mode

Usage Guidelines

This command displays the flow control mode, generation (Tx) and reception (Rx) status, and Tx and Rx PAUSE frame counts.

Examples

The following example displays the flow control information for all interfaces.

```
device# show qos flowcontrol interface all
Interface Ethernet 1/1
  Mode Off
Interface Ethernet 1/2
  Mode Off
Interface Ethernet 1/3
  Mode Off
Interface Ethernet 1/4
  Mode Off
...
Interface Ethernet 3/18
  Mode 802.3x
     TX    RX          TX Output Paused    RX
  Admin Admin     Frames  512 BitTimes     Frames
  ------------------------------------------------
     Off   On          0                        0
```

The following example displays the flow control information on a specific interface.

```
device# show qos flowcontrol interface ethernet 3/18
Interface Ethernet 3/18
  Mode 802.3x
     TX    RX         TX Output Paused    RX
  Admin Admin     Frames  512 BitTimes     Frames
  ------------------------------------------------
     Off   On          0                       0
```

show qos interface all

Displays QoS configuration information about Ethernet, Virtual Ethernet, and port-channel interfaces.

Syntax

show qos interface all

Modes

Privileged EXEC mode.

Usage Guidelines

This command can produce pages of output.

Examples

To show QoS information for all interfaces use the following command.

```
device# show qos interface all
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ve 20
  Provisioning Mode: none

  DSCP Mutation Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      ---------------------------------------
       0 :    00 01 02 03 04 05 06 07 08 09
       1 :    10 11 12 13 14 15 16 17 18 19
       2 :    20 21 22 23 24 25 26 27 28 29
       3 :    30 31 32 33 34 35 36 37 38 39
       4 :    40 41 42 43 44 45 46 47 48 49
       5 :    50 51 52 53 54 55 56 57 58 59
       6 :    60 61 62 63

  DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
      d1 :  d2  0   1   2   3   4   5   6   7   8   9
      -------------------------------------------------
       0 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
       1 :     1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
       2 :     2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
       3 :     3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
       4 :     5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
       5 :     6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
       6 :     7/0 7/0 7/0 7/0

  DSCP-to-CoS Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      ---------------------------------------
       0 :    00 00 00 00 00 00 00 00 01 01
       1 :    01 01 01 01 01 01 02 02 02 02
       2 :    02 02 02 02 03 03 03 03 03 03
       3 :    03 03 04 04 04 04 04 04 04 04
       4 :    05 05 05 05 05 05 05 05 06 06
       5 :    06 06 06 06 06 06 07 07 07 07
```

```
      6 :    07 07 07 07

  Per Traffic-Class Tail Drop Threshold (bytes)
            TC:      0      1      2      3      4      5      6      7
     ------------------------------------------------------------------
     Threshold:      0      0      0      0      0      0      0      0

  Flow control mode Off

...

  Traffic Class Scheduler configured for 8 Strict Priority queues
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ethernet 2/125
  Provisioning Mode: none
  Default TC: 0

  CoS-to-TC Map: default
             In-CoS: 0  1  2  3  4  5  6  7
     ------------------------------------
             Out-TC: 0  1  2  3  4  5  6  7
             Out-DP: 0  0  0  0  0  0  0  0

  TC-to-CoS Map: default
              In-TC: 0  1  2  3  4  5  6  7
     ------------------------------------
     Out-CoS(DP=0): 0  1  2  3  4  5  6  7
     Out-CoS(DP=1): 0  1  2  3  4  5  6  7
     Out-CoS(DP=2): 0  1  2  3  4  5  6  7
     Out-CoS(DP=3): 0  1  2  3  4  5  6  7

  DSCP Mutation Map: default (DSCP = d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    30 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63

  DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
     d1 :  d2  0   1   2   3   4   5   6   7   8   9
     -----------------------------------------------
      0 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
      1 :     1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
      2 :     2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
      3 :     3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
      4 :     5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
      5 :     6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
      6 :     7/0 7/0 7/0 7/0

  DSCP-to-CoS Map: default (DSCP = d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ------------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
      1 :    01 01 01 01 01 01 02 02 02 02
      2 :    02 02 02 02 03 03 03 03 03 03
      3 :    03 03 04 04 04 04 04 04 04 04
      4 :    05 05 05 05 05 05 05 05 06 06
      5 :    06 06 06 06 06 06 07 07 07 07
      6 :    07 07 07 07
```

```
  Per Traffic-Class Tail Drop Threshold (bytes)
            TC:      0      1      2      3      4      5      6      7
    ------------------------------------------------------------------
    Threshold:      0      0      0      0      0      0      0      0

  Flow control mode Off

  Traffic Class Scheduler configured for 8 Strict Priority queues
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ethernet 1/125
  Provisioning Mode: none
  Default TC: 0

  CoS-to-TC Map: default
            In-CoS: 0  1  2  3  4  5  6  7
    -----------------------------------
            Out-TC: 0  1  2  3  4  5  6  7
            Out-DP: 0  0  0  0  0  0  0  0

  TC-to-CoS Map: default
             In-TC: 0  1  2  3  4  5  6  7
    -----------------------------------
    Out-CoS(DP=0): 0  1  2  3  4  5  6  7
    Out-CoS(DP=1): 0  1  2  3  4  5  6  7
    Out-CoS(DP=2): 0  1  2  3  4  5  6  7
    Out-CoS(DP=3): 0  1  2  3  4  5  6  7

  DSCP Mutation Map: default (DSCP = d1d2)
    d1 :  d2 0  1  2  3  4  5  6  7  8  9
    -----------------------------------
     0 :    00 01 02 03 04 05 06 07 08 09
     1 :    10 11 12 13 14 15 16 17 18 19
     2 :    20 21 22 23 24 25 26 27 28 29
     3 :    30 31 32 33 34 35 36 37 38 39
     4 :    40 41 42 43 44 45 46 47 48 49
     5 :    50 51 52 53 54 55 56 57 58 59
     6 :    60 61 62 63

  DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
    d1 :  d2  0   1   2   3   4   5   6   7   8   9
    -------------------------------------------------
     0 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
     1 :     1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
     2 :     2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
     3 :     3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
     4 :     5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
     5 :     6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
     6 :     7/0 7/0 7/0 7/0

  DSCP-to-CoS Map: default (DSCP = d1d2)
    d1 :  d2 0  1  2  3  4  5  6  7  8  9
    -----------------------------------
     0 :    00 00 00 00 00 00 00 00 01 01
     1 :    01 01 01 01 01 01 02 02 02 02
     2 :    02 02 02 02 03 03 03 03 03 03
     3 :    03 03 04 04 04 04 04 04 04 04
     4 :    05 05 05 05 05 05 05 05 06 06
     5 :    06 06 06 06 06 06 07 07 07 07
     6 :    07 07 07 07

  Per Traffic-Class Tail Drop Threshold (bytes)
            TC:      0      1      2      3      4      5      6      7
    ------------------------------------------------------------------
    Threshold:      0      0      0      0      0      0      0      0
```

```
  Flow control mode Off

... <output truncated>
```

show qos interface

Displays QoS configuration information for a specific port-channel or ethernet interface.

Syntax

show qos interface [**ethernet** *slot/port* | **port-channel** *port-channel-number*]

Parameters

etherenet *slot/port*

A specific Ethernet interface slot and port number.

port-channel *port-channel-number*

A specific port-channel interface number.

Modes

Privileged EXEC mode.

Usage Guidelines

This command lists the details of all QoS maps supported in a device and those applied on the interface.

Examples

To display the QoS configuration for a specific interface use the following command. This output is displayed when executed on a SLX 9250 device.

```
SLX# show qos interface ethernet 0/13
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence,
       DSCP = Differentiated Services Code Point]
Interface Ethernet 0/13
  Trust CoS : True    Remark CoS : False
  Trust DSCP: True    Remark DSCP: False
  Provisioning Mode: mls
  Default TC: 0

  CoS-to-TC Map: default
             In-CoS: 0  1  2  3  4  5  6  7
         -----------------------------------
             Out-TC: 0  1  2  3  4  5  6  7
             Out-DP: 0  0  0  0  0  0  0  0

 TC-to-CoS Map: default
              In-TC: 0  1  2  3  4  5  6  7
         -----------------------------------
         Out-CoS(DP=0): 0  1  2  3  4  5  6  7
         Out-CoS(DP=1): 0  1  2  3  4  5  6  7
         Out-CoS(DP=2): 0  1  2  3  4  5  6  7
         Out-CoS(DP=3): 0  1  2  3  4  5  6  7

  TC-to-DSCP Map: default
```

```
               In-TC:  0   1   2   3   4   5   6   7
      ------------------------------------------------
      Out-DSCP(DP=0): 00  08  16  24  32  40  48  56
      Out-DSCP(DP=1): 00  08  16  24  32  40  48  56
      Out-DSCP(DP=2): 00  08  16  24  32  40  48  56
      Out-DSCP(DP=3): 00  08  16  24  32  40  48  56

  DSCP Mutation Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      ------------------------------------
       0 :    00 01 02 03 04 05 06 07 08 09
       1 :    10 11 12 13 14 15 16 17 18 19
       2 :    20 21 22 23 24 25 26 27 28 29
       3 :    30 31 32 33 34 35 36 37 38 39
       4 :    40 41 42 43 44 45 46 47 48 49
       5 :    50 51 52 53 54 55 56 57 58 59
       6 :    60 61 62 63

  DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
      d1 :  d2  0   1   2   3   4   5   6   7   8   9
      ------------------------------------------------
       0 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
       1 :     1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
       2 :     2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
       3 :     3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
       4 :     5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
       5 :     6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
       6 :     7/0 7/0 7/0 7/0

  DSCP-to-CoS Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      ------------------------------------
       0 :    00 00 00 00 00 00 00 00 01 01
       1 :    01 01 01 01 01 01 02 02 02 02
       2 :    02 02 02 02 03 03 03 03 03 03
       3 :    03 03 04 04 04 04 04 04 04 04
       4 :    05 05 05 05 05 05 05 05 06 06
       5 :    06 06 06 06 06 06 07 07 07 07
       6 :    07 07 07 07

  Per Traffic-Class Tail Drop Threshold (bytes)
             TC:      0      1      2      3      4      5      6      7
      ------------------------------------------------------------------
      Threshold:      0      0      0      0      0      0      0      0

  Flow control mode Off

  Traffic Class Scheduler configured for 8 Strict Priority queues
SLX#
```

To display the QoS configuration for a specific interface use the following command. This output is displayed when executed on a SLX 9740 device.

```
SLX# show qos interface ethernet 0/10
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence,
       DSCP = Differentiated Services Code Point]
Interface Ethernet 0/10
  Trust CoS : True    Remark CoS : True
  Trust DSCP: False   Remark DSCP: False
  Provisioning Mode: mls
  Default TC: 0

  CoS-to-TC Map: default
             In-CoS: 0  1  2  3  4  5  6  7
```

```
    ------------------------------------
           Out-TC: 0  1  2  3  4  5  6  7
           Out-DP: 0  0  0  0  0  0  0  0

CoS Mutation Map: cos_cos_map_1
            In-CoS: 0  1  2  3  4  5  6  7
    ------------------------------------
           Out-CoS: 0  1  2  5  4  5  6  7

TC-to-DSCP Map: default
             In-TC:  0   1   2   3   4   5   6   7
    ------------------------------------------------
    Out-DSCP(DP=0): 00  08  16  24  32  40  48  56
    Out-DSCP(DP=1): 00  08  16  24  32  40  48  56
    Out-DSCP(DP=2): 00  08  16  24  32  40  48  56
    Out-DSCP(DP=3): 00  08  16  24  32  40  48  56

DSCP Mutation Map: default (DSCP = d1d2)
    d1 :  d2 0  1  2  3  4  5  6  7  8  9
    ------------------------------------
     0 :    00 01 02 03 04 05 06 07 08 09
     1 :    10 11 12 13 14 15 16 17 18 19
     2 :    20 21 22 23 24 25 26 27 28 29
     3 :    30 31 32 33 34 35 36 37 38 39
     4 :    40 41 42 43 44 45 46 47 48 49
     5 :    50 51 52 53 54 55 56 57 58 59
     6 :    60 61 62 63

DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
    d1 :  d2  0   1   2   3   4   5   6   7   8   9
    -------------------------------------------------
     0 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
     1 :     1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
     2 :     2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
     3 :     3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
     4 :     5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
     5 :     6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
     6 :     7/0 7/0 7/0 7/0

DSCP-to-CoS Map: default (DSCP = d1d2)
    d1 :  d2 0  1  2  3  4  5  6  7  8  9
    ------------------------------------
     0 :    00 00 00 00 00 00 00 00 01 01
     1 :    01 01 01 01 01 01 02 02 02 02
     2 :    02 02 02 02 03 03 03 03 03 03
     3 :    03 03 04 04 04 04 04 04 04 04
     4 :    05 05 05 05 05 05 05 05 06 06
     5 :    06 06 06 06 06 06 07 07 07 07
     6 :    07 07 07 07

Per Traffic-Class Tail Drop Threshold (bytes)
           TC:      0      1      2      3      4      5      6      7
    ------------------------------------------------------------------
    Threshold:      0      0      0      0      0      0      0      0

Flow control mode Off

Traffic Class Scheduler configured for 8 Strict Priority queues
```

show qos interface port-channel

Displays QoS configuration information about a specific port channel interface.

Syntax

show qos interface port-channel *port_channel_number*

Parameters

port_channel_number

A specific port channel number.

Modes

Privileged EXEC mode.

Usage Guidelines

The insight interface port management module is on port-channel 1.

Examples

Follow this example to view information about the insight interface port channel.

```
device#  show qos interface port-channel 1
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ethernet 3/125
  Provisioning Mode: none
  Default TC: 0

  CoS-to-TC Map: default
             In-CoS: 0  1  2  3  4  5  6  7
      ------------------------------------
             Out-TC: 0  1  2  3  4  5  6  7
             Out-DP: 0  0  0  0  0  0  0  0

  TC-to-CoS Map: default
              In-TC: 0  1  2  3  4  5  6  7
      ------------------------------------
      Out-CoS(DP=0): 0  1  2  3  4  5  6  7
      Out-CoS(DP=1): 0  1  2  3  4  5  6  7
      Out-CoS(DP=2): 0  1  2  3  4  5  6  7
      Out-CoS(DP=3): 0  1  2  3  4  5  6  7

  DSCP Mutation Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      ------------------------------------
       0 :    00 01 02 03 04 05 06 07 08 09
       1 :    10 11 12 13 14 15 16 17 18 19
       2 :    20 21 22 23 24 25 26 27 28 29
       3 :    30 31 32 33 34 35 36 37 38 39
       4 :    40 41 42 43 44 45 46 47 48 49
       5 :    50 51 52 53 54 55 56 57 58 59
       6 :    60 61 62 63
```

```
  DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
      d1 :  d2  0   1   2   3   4   5   6   7   8   9
      ------------------------------------------------
       0 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
       1 :     1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
       2 :     2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
       3 :     3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
       4 :     5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
       5 :     6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
       6 :     7/0 7/0 7/0 7/0

  DSCP-to-CoS Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      -------------------------------------
       0 :    00 00 00 00 00 00 00 00 01 01
       1 :    01 01 01 01 01 01 02 02 02 02
       2 :    02 02 02 02 03 03 03 03 03 03
       3 :    03 03 04 04 04 04 04 04 04 04
       4 :    05 05 05 05 05 05 05 05 06 06
       5 :    06 06 06 06 06 06 07 07 07 07
       6 :    07 07 07 07

  Per Traffic-Class Tail Drop Threshold (bytes)
             TC:      0       1       2       3       4       5       6       7
      ------------------------------------------------------------------------
      Threshold:      0       0       0       0       0       0       0       0

  Flow control mode Off

  Traffic Class Scheduler configured for 8 Strict Priority queues
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ethernet 2/125
  Provisioning Mode: none
  Default TC: 0

  CoS-to-TC Map: default
              In-CoS: 0  1  2  3  4  5  6  7
      ------------------------------------
              Out-TC: 0  1  2  3  4  5  6  7
              Out-DP: 0  0  0  0  0  0  0  0

  TC-to-CoS Map: default
               In-TC: 0  1  2  3  4  5  6  7
      ------------------------------------
      Out-CoS(DP=0): 0  1  2  3  4  5  6  7
      Out-CoS(DP=1): 0  1  2  3  4  5  6  7
      Out-CoS(DP=2): 0  1  2  3  4  5  6  7
      Out-CoS(DP=3): 0  1  2  3  4  5  6  7

  DSCP Mutation Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      -------------------------------------
       0 :    00 01 02 03 04 05 06 07 08 09
       1 :    10 11 12 13 14 15 16 17 18 19
       2 :    20 21 22 23 24 25 26 27 28 29
       3 :    30 31 32 33 34 35 36 37 38 39
       4 :    40 41 42 43 44 45 46 47 48 49
       5 :    50 51 52 53 54 55 56 57 58 59
       6 :    60 61 62 63

  DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
      d1 :  d2  0   1   2   3   4   5   6   7   8   9
      ------------------------------------------------
```

```
      0 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
      1 :     1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
      2 :     2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
      3 :     3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
      4 :     5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
      5 :     6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
      6 :     7/0 7/0 7/0 7/0

  DSCP-to-CoS Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      ------------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
      1 :    01 01 01 01 01 01 02 02 02 02
      2 :    02 02 02 02 03 03 03 03 03 03
      3 :    03 03 04 04 04 04 04 04 04 04
      4 :    05 05 05 05 05 05 05 05 06 06
      5 :    06 06 06 06 06 06 07 07 07 07
      6 :    07 07 07 07

  Per Traffic-Class Tail Drop Threshold (bytes)
             TC:      0      1      2      3      4      5      6      7
      ------------------------------------------------------------------
      Threshold:      0      0      0      0      0      0      0      0

  Flow control mode Off

  Traffic Class Scheduler configured for 8 Strict Priority queues
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ethernet 1/125
  Provisioning Mode: none
  Default TC: 0

  CoS-to-TC Map: default
              In-CoS: 0  1  2  3  4  5  6  7
      ------------------------------------
              Out-TC: 0  1  2  3  4  5  6  7
              Out-DP: 0  0  0  0  0  0  0  0

  TC-to-CoS Map: default
               In-TC: 0  1  2  3  4  5  6  7
      ------------------------------------
      Out-CoS(DP=0): 0  1  2  3  4  5  6  7
      Out-CoS(DP=1): 0  1  2  3  4  5  6  7
      Out-CoS(DP=2): 0  1  2  3  4  5  6  7
      Out-CoS(DP=3): 0  1  2  3  4  5  6  7

  DSCP Mutation Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      ------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    30 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63

  DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
      d1 :  d2  0   1   2   3   4   5   6   7   8   9
      ------------------------------------------------
      0 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
      1 :     1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
      2 :     2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
      3 :     3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
```

```
      4 :     5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
      5 :     6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
      6 :     7/0 7/0 7/0 7/0

  DSCP-to-CoS Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      ------------------------------------
       0 :    00 00 00 00 00 00 00 00 01 01
       1 :    01 01 01 01 01 01 02 02 02 02
       2 :    02 02 02 02 03 03 03 03 03 03
       3 :    03 03 04 04 04 04 04 04 04 04
       4 :    05 05 05 05 05 05 05 05 06 06
       5 :    06 06 06 06 06 06 07 07 07 07
       6 :    07 07 07 07

  Per Traffic-Class Tail Drop Threshold (bytes)
              TC:      0      1      2      3      4      5      6      7
      ------------------------------------------------------------------
      Threshold:      0      0      0      0      0      0      0      0

  Flow control mode Off

  Traffic Class Scheduler configured for 8 Strict Priority queues
```

Follow this example to view information about a specific port channel interface.

```
device# show qos interface port-channel 20
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ethernet 3/48
  Provisioning Mode: none
  Default TC: 0

  CoS-to-TC Map: default
              In-CoS: 0  1  2  3  4  5  6  7
      ------------------------------------
              Out-TC: 0  1  2  3  4  5  6  7
              Out-DP: 0  0  0  0  0  0  0  0

  TC-to-CoS Map: default
               In-TC: 0  1  2  3  4  5  6  7
      ------------------------------------
      Out-CoS(DP=0): 0  1  2  3  4  5  6  7
      Out-CoS(DP=1): 0  1  2  3  4  5  6  7
      Out-CoS(DP=2): 0  1  2  3  4  5  6  7
      Out-CoS(DP=3): 0  1  2  3  4  5  6  7

  DSCP Mutation Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      ------------------------------------
       0 :    00 01 02 03 04 05 06 07 08 09
       1 :    10 11 12 13 14 15 16 17 18 19
       2 :    20 21 22 23 24 25 26 27 28 29
       3 :    30 31 32 33 34 35 36 37 38 39
       4 :    40 41 42 43 44 45 46 47 48 49
       5 :    50 51 52 53 54 55 56 57 58 59
       6 :    60 61 62 63

  DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
      d1 :  d2  0   1   2   3   4   5   6   7   8   9
      ------------------------------------------------
       0 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
       1 :     1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
       2 :     2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
```

```
      3 :     3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
      4 :     5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
      5 :     6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
      6 :     7/0 7/0 7/0 7/0

  DSCP-to-CoS Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      ---------------------------------------
       0 :    00 00 00 00 00 00 00 00 01 01
       1 :    01 01 01 01 01 01 02 02 02 02
       2 :    02 02 02 02 03 03 03 03 03 03
       3 :    03 03 04 04 04 04 04 04 04 04
       4 :    05 05 05 05 05 05 05 05 06 06
       5 :    06 06 06 06 06 06 07 07 07 07
       6 :    07 07 07 07

  Per Traffic-Class Tail Drop Threshold (bytes)
              TC:      0      1      2      3      4      5      6      7
      ------------------------------------------------------------------
      Threshold:      0      0      0      0      0      0      0      0

  Flow control mode Off


  Per Traffic-Class Tail Drop Threshold (bytes)
              TC:      0      1      2      3      4      5      6      7
      ------------------------------------------------------------------
      Threshold:      0      0      0      0      0      0      0      0

  Flow control mode Off

  Traffic Class Scheduler configured for 8 Strict Priority queues
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ethernet 3/2
  Provisioning Mode: none
  Default TC: 0

  CoS-to-TC Map: default
              In-CoS: 0  1  2  3  4  5  6  7
      ------------------------------------
              Out-TC: 0  1  2  3  4  5  6  7
              Out-DP: 0  0  0  0  0  0  0  0

  TC-to-CoS Map: default
               In-TC: 0  1  2  3  4  5  6  7
      ------------------------------------
      Out-CoS(DP=0): 0  1  2  3  4  5  6  7
      Out-CoS(DP=1): 0  1  2  3  4  5  6  7
      Out-CoS(DP=2): 0  1  2  3  4  5  6  7
      Out-CoS(DP=3): 0  1  2  3  4  5  6  7

  DSCP Mutation Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      ---------------------------------------
       0 :    00 01 02 03 04 05 06 07 08 09
       1 :    10 11 12 13 14 15 16 17 18 19
       2 :    20 21 22 23 24 25 26 27 28 29
       3 :    30 31 32 33 34 35 36 37 38 39
       4 :    40 41 42 43 44 45 46 47 48 49
       5 :    50 51 52 53 54 55 56 57 58 59
       6 :    60 61 62 63

  DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
      d1 :  d2  0   1   2   3   4   5   6   7   8   9
```

```
      ------------------------------------------------
       0 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
       1 :     1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
       2 :     2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
       3 :     3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
       4 :     5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
       5 :     6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
       6 :     7/0 7/0 7/0 7/0

  DSCP-to-CoS Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      -----------------------------------
       0 :    00 00 00 00 00 00 00 00 01 01
       1 :    01 01 01 01 01 01 02 02 02 02
       2 :    02 02 02 02 03 03 03 03 03 03
       3 :    03 03 04 04 04 04 04 04 04 04
       4 :    05 05 05 05 05 05 05 05 06 06
       5 :    06 06 06 06 06 06 07 07 07 07
       6 :    07 07 07 07

  Per Traffic-Class Tail Drop Threshold (bytes)
             TC:      0      1      2      3      4      5      6      7
      ------------------------------------------------------------------
      Threshold:      0      0      0      0      0      0      0      0

  Flow control mode Off

...<output truncated>

  Traffic Class Scheduler configured for 8 Strict Priority queues
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ethernet 1/41
  Provisioning Mode: none
  Default TC: 0

  CoS-to-TC Map: default
             In-CoS: 0  1  2  3  4  5  6  7
      -------------------------------------
             Out-TC: 0  1  2  3  4  5  6  7
             Out-DP: 0  0  0  0  0  0  0  0

  TC-to-CoS Map: default
              In-TC: 0  1  2  3  4  5  6  7
      -------------------------------------
      Out-CoS(DP=0): 0  1  2  3  4  5  6  7
      Out-CoS(DP=1): 0  1  2  3  4  5  6  7
      Out-CoS(DP=2): 0  1  2  3  4  5  6  7
      Out-CoS(DP=3): 0  1  2  3  4  5  6  7

  DSCP Mutation Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      -----------------------------------
       0 :    00 01 02 03 04 05 06 07 08 09
       1 :    10 11 12 13 14 15 16 17 18 19
       2 :    20 21 22 23 24 25 26 27 28 29
       3 :    30 31 32 33 34 35 36 37 38 39
       4 :    40 41 42 43 44 45 46 47 48 49
       5 :    50 51 52 53 54 55 56 57 58 59
       6 :    60 61 62 63

  DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
      d1 :  d2  0   1   2   3   4   5   6   7   8   9
      ------------------------------------------------
       0 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
```

```
     1 :     1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
     2 :     2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
     3 :     3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
     4 :     5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
     5 :     6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
     6 :     7/0 7/0 7/0 7/0

DSCP-to-CoS Map: default (DSCP = d1d2)
    d1 :  d2 0  1  2  3  4  5  6  7  8  9
    ---------------------------------------
     0 :    00 00 00 00 00 00 00 00 01 01
     1 :    01 01 01 01 01 01 02 02 02 02
     2 :    02 02 02 02 03 03 03 03 03 03
     3 :    03 03 04 04 04 04 04 04 04 04
     4 :    05 05 05 05 05 05 05 05 06 06
     5 :    06 06 06 06 06 06 07 07 07 07
     6 :    07 07 07 07

Per Traffic-Class Tail Drop Threshold (bytes)
           TC:      0      1      2      3      4      5      6      7
    ------------------------------------------------------------------
    Threshold:      0      0      0      0      0      0      0      0

Flow control mode Off

Traffic Class Scheduler configured for 8 Strict Priority queues
```

show qos interface ve

Displays QoS configuration information about a specific Virtual Ethernet interface.

Syntax

show qos interface ve *ve_number*

Parameters

ve_number

A specific Virtual Ethernet number.

Modes

Privileged EXEC mode.

Examples

Follow this example to view information about a specific VE interface.

```
device# show qos interface ve 20
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]
Interface Ve 20
  Provisioning Mode: none

  DSCP Mutation Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      ---------------------------------------
       0 :    00 01 02 03 04 05 06 07 08 09
       1 :    10 11 12 13 14 15 16 17 18 19
       2 :    20 21 22 23 24 25 26 27 28 29
       3 :    30 31 32 33 34 35 36 37 38 39
       4 :    40 41 42 43 44 45 46 47 48 49
       5 :    50 51 52 53 54 55 56 57 58 59
       6 :    60 61 62 63

  DSCP-to-TC Map: default (x/y: TC = x, DP = y, DSCP = d1d2)
      d1 :  d2  0   1   2   3   4   5   6   7   8   9
      ------------------------------------------------
       0 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 1/0 1/0
       1 :     1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
       2 :     2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
       3 :     3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
       4 :     5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
       5 :     6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
       6 :     7/0 7/0 7/0 7/0

  DSCP-to-CoS Map: default (DSCP = d1d2)
      d1 :  d2 0  1  2  3  4  5  6  7  8  9
      ---------------------------------------
       0 :    00 00 00 00 00 00 00 00 01 01
       1 :    01 01 01 01 01 01 02 02 02 02
       2 :    02 02 02 02 03 03 03 03 03 03
       3 :    03 03 04 04 04 04 04 04 04 04
       4 :    05 05 05 05 05 05 05 05 06 06
       5 :    06 06 06 06 06 06 07 07 07 07
```

```
     6 :    07 07 07 07

Per Traffic-Class Tail Drop Threshold (bytes)
           TC:      0      1      2      3      4      5      6      7
    ------------------------------------------------------------------
    Threshold:      0      0      0      0      0      0      0      0

Flow control mode Off

Traffic Class Scheduler configured for 8 Strict Priority queues
```

show qos maps

Displays details about all configured QoS maps.

Syntax

show qos maps [*cos-mutation-map-name*]

Parameters

cos-mutation-map-name

Optional. The name of the CoS Mutation map for which to view detailed information.

Modes

Privilege Execution Mode

Usage Guidelines

This command shows CoS Mutation information for SLX 9740 and Extreme 8820.

This command shows Traffic Class to CoS mappings for all other devices.

Output

The **show qos maps** command displays the following information:

Output Field	Description
CoS-to-TC Map (all-zero-map)	This map is used to map all CoS values to traffic-class 0 (zero).
TC-to-CoS Map (all-zero-map)	This table is only visible on SLX 9150, SLX 9250, Extreme 8520, and Extreme 8720. This displays the traffic-class to class of service mapping where all incoming TC mappings are set to CoS 0 (zero).
TC-to-CoS Maps (user configured maps)	This table is only visible on SLX 9150, SLX 9250, Extreme 8520, and Extreme 8720. This displays all the user created traffic-class to class of service mapping.
CoS Mutation map (all-zero-map)	This table is only visible on SLX 9740 and Extreme 8820. This displays the CoS Mutation mapping where each incoming CoS value is mapped to 0 (zero).
CoS Mutation map (user configured map)	This table is only visible on SLX 9740 and Extreme 8820. This displays the user defined CoS Mutation mapping.
DSCP Mutation Map (all-zero-map)	This table displays the DSCP mutation all-zero-map.
DSCP to TC Map (all-zero-map)	This table displays the DSCP to traffic-class all-zero-map.

Output Field	Description
DSCP to CoS map (all-zero-map)	This table displays the DSCP to class of service all-zero-map.
Enabled on the following interfaces	Available for all the tables and lists the interfaces where these maps are applied.

Examples

This example shows the output of the **show qos map** when executed on a SLX 9250 device.

```
SLX# show qos maps
  [Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence,
         DSCP = Differentiated Services Code Point]

  CoS-to-TC Map: all-zero-map
             In-CoS: 0  1  2  3  4  5  6  7
      -------------------------------------
             Out-TC: 0  0  0  0  0  0  0  0
             Out-DP: 0  0  0  0  0  0  0  0

      Enabled on the following interfaces:

  TC-to-DSCP Map: all-zero-map
               In-TC:  0   1   2   3   4   5   6   7
      ------------------------------------------------
      Out-DSCP(DP=0): 00  00  00  00  00  00  00  00
      Out-DSCP(DP=1): 00  08  16  24  32  40  48  56
      Out-DSCP(DP=2): 00  08  16  24  32  40  48  56
      Enabled on the following interfaces:

  TC-to-CoS Map: all-zero-map
               In-TC: 0  1  2  3  4  5  6  7
      -------------------------------------
      Out-CoS(DP=0): 0  0  0  0  0  0  0  0
      Out-CoS(DP=1): 0  0  0  0  0  0  0  0
      Out-CoS(DP=2): 0  0  0  0  0  0  0  0
      Enabled on the following interfaces:

  DSCP-to-TC Map: all-zero-map (x/y: TC = x, DP = y, DSCP = d1d2)
      d1 :  d2  0   1   2   3   4   5   6   7   8   9
      -------------------------------------------------
       0 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0
       1 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0
       2 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0
       3 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0
       4 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0
       5 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0
       6 :     0/0 0/0 0/0 0/0

      Enabled on the following interfaces:
```

This example shows the output of the **show qos map** when executed on a SLX 9740 device.

```
SLX# show qos maps
```

```
[Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence,
       DSCP = Differentiated Services Code Point]

CoS-to-TC Map: all-zero-map
           In-CoS: 0  1  2  3  4  5  6  7
    -----------------------------------
           Out-TC: 0  0  0  0  0  0  0  0
           Out-DP: 0  0  0  0  0  0  0  0

    Enabled on the following interfaces:

TC-to-DSCP Map: all-zero-map
             In-TC:  0   1   2   3   4   5   6   7
    ------------------------------------------------
    Out-DSCP(DP=0): 00  00  00  00  00  00  00  00
    Out-DSCP(DP=1): 00  08  16  24  32  40  48  56
    Out-DSCP(DP=2): 00  08  16  24  32  40  48  56
    Enabled on the following interfaces:

COS Mutation Map : all-zero-map
           In-CoS: 0  1  2  3  4  5  6  7
    -----------------------------------
          Out-CoS: 0  0  0  0  0  0  0  0
    Enabled on the following interfaces: Eth 0/5

COS Mutation Map : test-cos-mut-map-1
           In-CoS: 0  1  2  3  4  5  6  7
    -----------------------------------
          Out-CoS: 0  3  1  0  0  0  0  0
    Enabled on the following interfaces: Eth 0/3

DSCP-to-TC Map: all-zero-map (x/y: TC = x, DP = y, DSCP = d1d2)
    d1 :  d2  0   1   2   3   4   5   6   7   8   9
    ------------------------------------------------
     0 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0
     1 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0
     2 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0
     3 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0
     4 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0
     5 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0
     6 :     0/0 0/0 0/0 0/0

    Enabled on the following interfaces:
```

show qos maps cos-mutation

This commands displays detailed information of the CoS Mutation map passed as a parameter.

Syntax

show qos map cos-mutation [*cos-mutation-map-name*]

Parameters

cos-mutation-map-name

Optional. The name of the CoS Mutation map for which to display details. When not provided, details of all cos-mutation maps are displayed.

Modes

Privileged EXEC Mode

Usage Guidelines

This command is only supported on SLX 9740 and Extreme 8820. Executing this command on other platforms will return an error.

Supported In

SLX 9740 and Extreme 8820

Output

The **show qos map cos-mutation** command displays the following information:

Output Field	Description
CoS Mutation Map	Name of the CoS Mutation map for which data is displayed.
In-CoS	The incoming CoS value.
Out-CoS	The value to be applied for each outgoing packet.
Enabled on the following interfaces	List of interfaces on which the QoS CoS Mutation map is applied.

Examples

This example displays information for a QoS CoS Mutation map.

```
SLX# show qos maps cos-mutation qm_cm_1
  [Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence,
         DSCP = Differentiated Services Code Point]
```

```
    CoS Mutation Map: qm_cm_1
             In-CoS: 0  1  2  3  4  5  6  7
      ------------------------------------
            Out-CoS: 0  1  2  5  4  5  6  7

      Enabled on the following interfaces: Po 100, Po 101, Po 102, Eth 0/10, Eth 0/11,
Eth 0/12, Eth 0/13, Eth 0/15.
```

Related Commands

- map cos to cos on page 1080
- qos map cos-mutation on page 1437
- qos cos-mutation on page 1424

show qos maps cos-traffic-class

Displays configured CoS-to-traffic class mutation maps.

Syntax

show qos maps cos-traffic-class

Modes

Privileged EXEC mode.

Examples

To display information on defined QoS CoS-to-traffic class mutation maps and where they are applied, use this command.

```
device# show qos maps cos-traffic-class

Cos-to-Traffic Class map 'cosTCMap'
In-Cos        : 0 1 2 3 4 5 6 7
-------------------------------------
TrafficClass  : 0 1 2 3 3 6 6 6
DropPrecedence: 0 0 0 0 0 1 0 1

Enabled on the following interfaces:
    Eth 1/4
```

show qos maps dscp-cos

Displays configured DSCP to CoS mutation maps.

Syntax

show qos maps dscp-cos

Modes

Privileged EXEC mode

Examples

To display information on defined QoS DSCP to CoS mutation maps and where they are applied, use this command.

```
device# show qos maps dscp-cos

Dscp-to-CoS map 'dscpCoS' (dscp= d1d2)
d1 :  d2 0  1  2  3  4  5  6  7  8  9
---------------------------------------
0 :    00 00 00 00 00 00 00 00 01 01
1 :    01 01 01 01 01 01 02 02 02 02
2 :    02 02 02 04 03 03 03 03 03 03
3 :    03 03 04 04 04 04 04 04 04 04
4 :    05 05 05 05 05 05 05 05 06 06
5 :    06 06 06 06 06 06 07 07 07 07
6 :    07 07 07 07

   Enabled on the following interfaces:
    Eth 1/3
```

show qos maps dscp-mutation

Displays configured DSCP mutation maps.

Syntax

show qos maps dscp-mutation [*map-name*]

Parameters

map-name

Displays the specified DSCP mutation map.

Modes

Privileged EXEC mode

Examples

To display information on defined QoS DSCP mutation maps and where they are applied, use this command.

```
device# show qos maps dscp-mutation

Dscp-to-Dscp Mutation map 'dscpMut' (dscp= d1d2)
d1 :  d2 0  1  2  3  4  5  6  7  8  9
---------------------------------------
0 :    00 01 02 03 04 05 06 07 08 09
1 :    10 11 12 13 14 15 16 17 18 19
2 :    20 21 22 23 24 25 26 27 28 29
3 :    30 31 32 33 34 35 36 37 38 39
4 :    40 41 42 43 44 45 46 47 48 49
5 :    50 51 52 53 54 55 56 57 58 59
6 :    40 61 62 63

   Enabled on the following interfaces:
    Eth 1/3
```

show qos maps dscp-traffic-class

Displays configured DSCP to traffic class mutation maps or displays information about a specific map.

Syntax

show qos maps dscp-traffic-class [*map-name*]

Parameters

map-name

Name of the QoS DSCP-to-traffic-class map.

Modes

Privileged EXEC mode

Usage Guidelines

Note

This command is supported on the Extreme 8720, Extreme 8520, SLX 9250, and SLX 9150 devices only.

Examples

This example displays information on defined QoS DSCP to traffic class mutation maps and where they are applied.

```
device# show qos maps dscp-traffic-class

Dscp-to-Traffic-Class map 'dscpTC'
{x/y: traffic-class = x, drop-precedence = y & dscp = d1d2}
d1 :  d2  0   1   2   3   4   5   6   7   8   9
-------------------------------------------------
0 :     0/0 0/0 0/0 0/0 0/0 0/0 0/0 0/0 4/2 1/0
1 :     1/0 1/0 1/0 1/0 1/0 1/0 2/0 2/0 2/0 2/0
2 :     2/0 2/0 2/0 2/0 3/0 3/0 3/0 3/0 3/0 3/0
3 :     3/0 3/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0 4/0
4 :     5/0 5/0 5/0 5/0 5/0 5/0 5/0 5/0 6/0 6/0
5 :     6/0 6/0 6/0 6/0 6/0 6/0 7/0 7/0 7/0 7/0
6 :     7/0 7/0 7/0 7/0

   Enabled on the following interfaces:
    Eth 1/4
```

This example shows information about a specified map.

```
device# show qos maps dscp-traffic-class td-map1
  [Note: CoS = Class of Service, TC = Traffic Class, DP = Drop Precedence]

  TC-to-DSCP Map: td-map1
              In-TC: 00   1   2   3   4   5   6   7
```

```
    ------------------------------------------
    Out-DSCP(DP=0): 00  08  12  24  32  40  48  56
    Out-DSCP(DP=1): 00  08  13  24  32  43  48  56
    Out-DSCP(DP=2): 00  00  00  00  00  00  00  00
    Out-DSCP(DP=3): 00  00  00  00  00  00  00  00
```

show qos maps traffic-class-cos

Displays configured traffic class to CoS mutation maps.

Syntax

show qos maps traffic-class-cos

Modes

Privileged EXEC mode

Supported In

SLX 9150, SLX 9250, Extreme 8520, and Extreme 8720

Examples

To display information on defined QoS DSCP to traffic class to CoS mutation maps and where they are applied, use this command.

```
device# show qos maps traffic-class-cos

Traffic Class-to-Cos map 'tcCoS' (drop-precedence = dp0 to dp3)
   TrafficClass  : 0  1  2  3  4  5  6  7
   ---------------------------------------
   Out-Cos(dp0)  : 0  1  2  3  4  5  6  7
   Out-Cos(dp1)  : 0  1  2  3  4  5  6  7
   Out-Cos(dp2)  : 0  1  2  3  4  4  6  7
   Out-Cos(dp3)  : 0  1  2  3  4  5  6  7

   Enabled on the following interfaces:
    Eth 1/4
```

show qos maps traffic-class-dscp

Displays configured traffic class to CoS mutation maps.

Syntax

show qos maps traffic-class-cos

Modes

Privileged EXEC mode

Examples

This example displays the defined QoS DSCP to traffic class to CoS mutation maps and where they are applied.

```
 device# show qos maps traffic-class-cos

Traffic Class-to-Cos map 'tcCoS' (drop-precedence = dp0 to dp3)
   TrafficClass  : 0  1  2  3  4  5  6  7
   ---------------------------------------
   Out-Cos(dp0)  : 0  1  2  3  4  5  6  7
   Out-Cos(dp1)  : 0  1  2  3  4  5  6  7
   Out-Cos(dp2)  : 0  1  2  3  4  4  6  7
   Out-Cos(dp3)  : 0  1  2  3  4  5  6  7

   Enabled on the following interfaces:
    Eth 1/4
```

show qos-mpls maps dscp-exp

Displays configured QoS Multiprotocol Label Switching (MPLS) DSCP to EXP egress mutation maps.

Syntax

show qos-mpls maps dscp-exp

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the Extreme 8820 and SLX 9740 devices only.

Examples

```
device# show qos-mpls maps dscp-exp

dscp-exp map    'dscpExp' (dscp= d1d2)
 d1     : d2 0  1  2  3  4  5  6  7  8  9
 ------- --------------------------------
 0      :    0  0  2  0  0  0  0  0  1  1
 1      :    1  1  1  1  1  1  2  2  2  2
 2      :    2  2  2  2  3  3  3  3  3  3
 3      :    3  3  4  4  4  4  4  4  4  4
 4      :    5  5  5  5  5  5  5  5  6  6
 5      :    6  6  6  6  6  6  7  7  7  7
 6      :    7  7  7  0

Enabled on the following slots:
  ALL
```

show qos-mpls maps exp-dscp

Displays configured QoS Multiprotocol Label Switching (MPLS) EXP to DSCP mutation maps.

Syntax

show qos-mpls maps exp-dscp

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the Extreme 8820 and SLX 9740 devices only.

Examples

```
device# show qos-mpls maps exp-dscp

exp-dscp map 'expDSCP'
    Exp   : 0  1  2  3  4  5  6  7
   ------- ------------------------
    DSCP  : 0  2  4  3  6  4  5  7

Enabled on the following slots:
   ALL
```

show qos-mpls maps exp-traffic-class

Displays configured QoS Multiprotocol Label Switching (MPLS) EXP to traffic class mutation maps.

Syntax

show qos-mpls maps exp-traffic-class

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported on the Extreme 8820 and SLX 9740 devices only.

Examples

```
device# show qos-mpls maps exp-traffic-class

exp-traffic-class map 'expTc'
    Exp   :    0  1  2  3  4  5  6  7
   ------- ------------------------
traffic-class  : 5  5  4  6  5  5  5  5
drop-precedence: 0  1  1  1  0  2  2  1

   Enabled on the following slots:
     ALL
```

show qos tx-queue interface

Displays a summary of the runtime egress queue state information applied to a Layer 2 interface.

Syntax

show qos tx-queue interface { **ethernet** *slot/port* }

Parameters

ethernet

Represents a valid, physical Ethernet interface.

slot

Specifies a valid slot number. The only valid value is 0.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Examples

This example displays the runtime egress queue state information retrieved from the data plane.

```
device# show qos tx-queue interface ethernet 0/1
Interface Ethernet 0/1
          In-use        Max             TX        Dropped                TX
Dropped
  TC       Bytes      Bytes        Packets        Packets             Bytes
Bytes

-------------------------------------------------------------------------------------------
-
    0          0     748288               0              0
0                 0
    1          0     748288    35739153669              0
1133120185038                 0
    2          0     748288               0              0
0                 0
    3          0     748288               0              0
0                 0
    4          0     748288               0              0
0                 0
    5          0     748288               0              0
0                 0
    6          0     748288               0              0
0                 0
    7          0     748288       30715725              2        2765239372
164
```

show rmon

Displays the current RMON status on the device.

Syntax

```
show rmon [ alarms [ number ] [ brief ] | events [ number ] [ brief ] |
   logs [ event_number ] | statistics [ number ] [ brief ] ]
```

Parameters

alarms

Specifies to display the RMON alarm table.

number

Specifies the alarm index identification number. Valid values range from 1 through 65535.

brief

Specifies to display a brief summary of the output.

events

Specifies to display the RMON events table.

number

Specifies the event index identification number. Valid values range from 1 through 65535.

brief

Specifies to display a brief summary of the output.

logs

Specifies to display the RMON log table.

event_number

Specifies the event log index identification number. Valid values range from 1 through 65535.

statistics

Specifies to display the statistics identification number.

number

Specifies the statistics identification number. Valid values range from 1 through 65535.

brief

Specifies a brief summary of the output.

Modes

Privileged EXEC mode

Examples

To display the RMON statistics:

```
device# show rmon statistics

rmon collection index 4
    Interface index is Id: 67108864 , Name : Ethernet 0/13
    Receive Statistics:
        218903 packets, 14015626 bytes,  0 packs dropped
        Multicasts: 218884, Broadcasts: 18
        Under-size : 0, Jabbers: 0, CRC: 0
        Fragments: 0, Collisions: 0
             64 byte pkts: 218722, 65-127 byte pkts: 174
        128-255 byte pkts: 0, 256-511 byte pkts: 6
        512-1023 byte pkts: 0, 1024-1518 byte pkts: 0
        Over 1518-byte pkts(Oversize - Jumbo): 0
    Owner: RMON_SNMP
    Status: ok(1)
```

To display the RMON events:

```
device# show rmon events

event Index = 4
        Description "My Description"
        Event type Log & SnmpTrap
        Event community name admin
        Last Time Sent = 00:00:00
        Owner  admin
```

show rmon history

Displays information gathered by rmon event and rmon alarm commands.

Syntax

show rmon history [**statistics** | *history_index*]

Parameters

statistics

Displays a more detailed synopsis.

history_index

Specifies the RMON history identification number. Valid values range from 1 through 65535.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display a synopsis of the statistics collected by the **rmon event** and **rmon alarm** commands.

Add the **statistics** parameter to display the detailed history.

Examples

To display the RMON history:

```
device# show rmon history

RMON history control entry 1
interface: ifIndex.1745682445 Ethernet 0/13
buckets requested: 20
buckets granted: 20
sampling interval: 10
Owner: jsmith
```

show remote-attestation

Displays the status of Remote Attestation and the calculated boot-aggregate value.

Syntax

show remote-attestation [**status** | **boot-aggregate**]

Parameters

boot-aggregate

Displays the calculated boot aggregate for this SLX-OS device.

status

Displays details of the remote Keylime server used for remote attestation. This command also displays the details of Keylime agent(local) details such as uuid, and agent-port.

Modes

Privileged EXEC mode

Examples

This example displays the boot aggregate.

```
device# show remote-attestation boot-aggregate
sha1:fcd94d739efd625fb774202de99961d9ed1ccdaf
```

SLX# show remote-attestation status

```
SLX# show remote-attestation status
Keylime-agent status: Enabled
Registrar Host: 1.1.1.1
Registrar Port: 8888
Keylime-agent Port: 9999
Keylime-agent UUID: 15e67a855f19d569e7baa8d3b279839cc0b11b8180fa0eec22a0b673e4cd89cd
IMA Status: Enabled(needs reboot)
```

```
SLX# show remote-attestation status
Keylime-agent status: Disabled
Registrar Host: Not configured
Registrar Port: 8890
Keylime-agent Port: 9002
Keylime-agent UUID: auto
IMA Status: Disabled
```

Platform Availability

This command is only available on the Extreme 8720 and Extreme 8520 devices.

show rollback checkpoint

Displays information about configuration rollback checkpoints.

Syntax

show rollback checkpoint [**all** | *cp-name* | **summary**]

Parameters

all

Specifies all checkpoints created by the user.

cp-name

Specifies the name of a checkpoint.

summary

Specifies brief details.

Modes

Privileged EXEC mode

Usage Guidelines

The default is **all** if this is not specified.

The output for *cp-name* is similar to that for **show running-config**.

Examples

This example displays summary information.

```
device# show rollback checkpoint summary
User checkpoint summary
-------------------------------
1) checkpoint_before_vlans :
Created by   admin
Created at   Thu Apr  5 08:10:55 2018
Size is   8912  bytes
Description:  "Before VLAN configs"

2) default :
Created by   admin
Created at   Thu Apr  5 09:18:53 2018
Size is   8907  bytes
Description:  "Default Configs"
```

This example displays running configuration information for checkpoint "test".

```
device# show rollback checkpoint test
Name: test

root enable
```

```
clock timezone Etc/GMT
ha
process-restart mpls
no process-restart bgp
no process-restart isis
no process-restart ospfv2
no process-restart ospfv3
!
hardware
profile tcam default
profile route default
profile lag default
profile counters default
!
```

show rollback diff checkpoint

Compares two configuration rollback checkpoints and displays the differences between the two.

Syntax

show rollback diff checkpoint *cp-name* [**checkpoint** *cp-name*]

Parameters

cp-name

Specifies the name of the first checkpoint for comparison.

checkpoint*cp-name*

Specifies the name of the second checkpoint for comparison.

Modes

Privileged EXEC mode

Usage Guidelines

Differences are noted by - (removed) and + (added).

The **show rollback diff checkpoint** *cp-name* **checkpoint** *cp-name* command compares the two checkpoints provided and displays the differences between the two.

The **show rollback diff checkpoint** *cp-name* command displays the differences between the running configuration and the checkpoint configuration provided.

Examples

This example displays a comparison between checkpoints "default" and "test".

```
device# show rollback  diff checkpoint default  checkpoint test
interface Ethernet 1/10
- switchport port-security shutdown-time 10
- switchport trunk native-vlan 2
+ switchport port-security max 100
```

show rollback feature-status

Displays whether configuration rollback is enabled or not.

Syntax

show rollback feature-status

Modes

Privileged EXEC mode

Examples

This example displays configuration rollback status.

```
device# show rollback feature-status

    Rollback feature is       :     Disabled
```

show rollback log

Displays the configuration rollback log, including errors resulting from rollback.

Syntax

show rollback log [**errors**]

Parameters

errors

Specifies rollback errors, whether from the plugin or the backend.

Modes

Privileged EXEC mode

Usage Guidelines

The command and option display ongoing logs of a rollback operation that is in progress. Otherwise, the logs of the last completed rollback are displayed.

Examples

This example displays errors.

```
device# show rollback log errors
event-handler ev1
  action python-script show_interface.py
Error: flash://show_interface.py script for event handler ev1 could not be found or read.
```

show rollback patch checkpoint

Displays the configuration rollback patch between the running configuration and a checkpoint configuration.

Syntax

show rollback patch checkpoint *cp-name*

Parameters

cp-name

Specifies the name of a checkpoint.

Modes

Privileged EXEC mode

Examples

This example displays the configuration rollback patch between the running configuration and the checkpoint named "chkpt1".

```
device# show rollback patch checkpoint chkpt1
Collecting Running-Config...
Generating Rollback Patch...
interface Ethernet 0/10
no switchport trunk native-vlan 7
no switchport trunk tag native-vlan
no switchport trunk allowed vlan add 1,3-10
interface Ve 10
ip address 10.10.10.10/24
shutdown
vlan 10
name VLAN100
```

show rollback status

Displays information about the status of configuration rollback execution.

Syntax

show rollback status { **current** | **history** }

Parameters

current

Specifies current rollback status.

history

Specifies the status of the last five rollbacks.

Modes

Privileged EXEC mode

Usage Guidelines

The **current** option displays information about the rollback when it is in process, such as the rollback operation, checkpoint name, rollback status, and timestamp when rollback was issued. Status is displayed as "In Progress" with all other fields updated except End Time.

The **history** option displays information about rollback execution status, such as who issued the rollback, the checkpoint name, rollback status, timestamp when rollback was issued, and time taken for rollback to complete.

Examples

This example displays current status.

```
device# show rollback status current
Operation                 :  Rollback To Checkpoint
Checkpoint Name           :  vlan-config
Rollback done By          :  admin
Rollback Mode             :  best-effort
Start Time                :  Thu Apr  5 09:32:24 2018
Status                    :  In-Progress
```

This example displays rollback history.

```
device# show rollback status history
Operation                 :  Rollback To Checkpoint
Checkpoint Name           :  vlan-config
Rollback done By          :  admin
Rollback Mode             :  best-effort
Start Time                :  Thu Apr  5 09:32:24 2018
End Time                  :  Thu Apr  5 09:32:57 2018
Time Taken For Rollback   :  33 seconds
```

```
Status                    :  Success
Operation                 :  Rollback To Checkpoint
Checkpoint Name           :  bgp-config
Rollback done By          :  admin
Rollback Mode             :  best-effort
Start Time                :  Thu Apr  5 07:32:24 2018
End Time                  :  Thu Apr  5 07:32:57 2018
Time Taken For Rollback   :  38 seconds
Status                    :  Success
```

show route-map

Displays route-map configuration details.

Syntax

show route-map [*name*]

show route-map interface [**ethernet** *slot/port* | **port-channel** *index* | **ve** *ve-number*]

Parameters

name

Specifies the name of the route-map.

interface

Specifies an interface.

ethernet *slot/port*

Specifies a physical interface.

port-channel *index*

Specifies a port-channel.

ve *ve-number*

Specifies a virtual Ethernet interface.

Modes

Privileged EXEC mode

Output

The **show route-map** command displays the following information:

Output field	Description
Active/ Inactive	Indicates the instantiation of the route-map configuration into the underlying hardware. Possible meanings for inactive may be no room in the TCAM for programming the ACL, or the exhaustion of next-hop entries within the hardware next-hop table.
Selected	Indicates which of the configured next hops is currently being used by the policy. If the keyword selected is absent from the display, it indicates that none of the next hops in the list is being used and the packet is being routed by the standard routing mechanism.
Policy routing matches	Provides a summary of the number of times any of the match criteria within the specific ACL have been hit. If the ACL binding was unable to allocate a counter for the ACL (due to resource exhaustion) the count value will show "Counter not available" otherwise an actual counter value will be displayed.

Examples

The following example displays route-map details for all route-maps.

```
device# show route-map
Interface Ethernet 1/6
 ip policy route-map route1
```

The following example displays route-map details for a specific route-map.

```
device# show route-map route1
Interface Ethernet 1/6
ip policy route-map route1 permit 1 (Active)
    match ip address acl test1
    set ip next-hop 6.0.0.1 (selected) (recursive)
       next-hop 10.10.10.1
    Policy routing matches: 1443 packets
```

The following example displays route-map details on a specific interface.

```
device# show route-map interface ethernet 1/6
Interface Ethernet 1/6
ip policy route-map route1 permit 1 (Active)
    match ip address acl test1
    set ip next-hop 6.0.0.1 (selected) (recursive)
       next-hop 10.10.10.1
    Policy routing matches: 1543 packets
```

The following example displays the route map configuration from the running configuration.

```
SLX# show running-config route-map r1
route-map r1 permit 10
   match ip address acl test1
   next-hop-recursion
   set ip next-hop 4.4.4.4
!
SLX#
```

The following example displays the configured route-maps.

```
SLX# show route-map
Interface Ethernet 0/17
   ip policy route-map r1
SLX#
```

The following example shows the information for a particular route map. This example also shows that recursive next hop resolution is enabled on the route map.

```
SLX# show route-map r1
Interface Ethernet 0/17
ip policy route-map r1 permit 10 (Active)
    match ip address acl test1
    set ip next-hop 4.4.4.4 (selected) (recursive)
        next-hop 10.10.10.1
    Policy routing matches: 0 packets    Note: Counter values are partial
```

The following example shows the route map configured on a particular interface. This example also shows that recursive next hop resolution is enabled on the route map.

In the below output, 10.10.10.1 is the actual IPv4 next-hop for the recursive route and 2002:db1:0:0:0:ee00:41:2222 the actual IPv6 next-hop.

```
SLX# show route-map interface eth 0/17
Interface Ethernet 0/17
ip policy route-map r1 permit 10 (Active)
    match ip address acl test1
    set ip next-hop 4.4.4.4 (selected) (recursive)
        next-hop 10.10.10.1
    Policy routing matches: 1543 packets    Note: Counter values are partial
SLX#
SLX# show route-map interface eth 0/18
Interface Ethernet 0/18
ip policy route-map r2 permit 10 (Active)
    match ip address acl test1
    set ip next-hop 2001:db8:0:0:0:ff00:42:1111 (selected) (recursive)
        next-hop 2002:db1:0:0:0:ee00:41:2222
    Policy routing matches: 1543 packets
SLX#
```

show run router mpls cspf-group

Displays the CSPF fate-sharing group configuration for all groups configured on a device.

Syntax

```
show run router mpls cspg-group group_name [ from | link| node
   [ ip_addr ] ] | subnet ip_addr/mask ]
```

Parameters

from *ip_addr*

Configures the CSPF group from the specified IP address.

link *ip_addr*

Configures the CSPF group from and to the specified IP address.

node *ip_addr*

Configures the CSPF group node IP address.

subnet *ip_addr/mask*

Configures the CSPF group subnet address.

Modes

EXEC mode

Usage Guidelines

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example displays the fate-sharing group configuration for all groups currently configured on the device.

```
device# show run router mpls cspf-group gold
cspf-group test8
penalty 65535
node 10.7.7.3
node 10.7.7.8
```

show running-config

Displays the contents of the running configuration.

Syntax

show running-config

Parameters

Refer to the Usage Guidelines.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display the running configuration.

This command is supported only on the local device.

To display the list of available configuration entries, enter **show running-config ?**.

The **show running-config** option displays the global configuration and also the configuration on all interfaces.

The **show running-config interface** options display only the configuration for the interfaces specified.

Examples

The following command example displays the contents of the device running configuration.

```
device# show running-config
```

show running-config aaa

Displays the configuration attributes for the authentication, authorization, and accounting (AAA) server from the configuration database.

Syntax

```
show running-config aaa [ accounting [ commands | exec ] | authentication
   [ login ] ]
```

Parameters

accounting

Configures Login or Command accounting

commands

Enable/Disable Command accounting

exec

Enable/Disable Login accounting

authentication

Configures preferred order of Authentication output modifiers

login

Configures the order of sources for login (default = 'local')

Modes

Privileged EXEC mode

Usage Guidelines

Refer to the **aaa authentication** command for a description of the displayed attributes.

Examples

To display the authentication mode:

```
device# show running-config aaa
aaa authentication radius local
aaa accounting exec default start-stop none
aaa accounting commands default start-stop none

device# show running-config aaa authentication
aaa authentication login radius local

device# show running-config aaa authentication
aaa authentication login ldap local-auth-fallback
```

show running-config aaa accounting

Displays the AAA server accounting configuration.

Syntax

show running-config aaa accounting

Modes

Privileged EXEC mode

Usage Guidelines

Refer to the **aaa authentication** command for a description of the displayed attributes.

Examples

To displaying the authentication mode:

```
device# show running-config aaa accounting
aaa accounting exec default start-stop tacacs+
aaa accounting commands default start-stop tacacs+
```

show running-config aaa authorization

Displays AAA server authorization configuration.

Syntax

show running-config aaa authorization

Modes

Privileged EXEC mode

Examples

The following example shows how to display AAA authorization status.

```
show running-config aaa authorization

aaa authorization commands tacacs+
```

show running-config aaa authorization command

Displays the current status for TACACS+ authorization of command privileges for the user role.

Syntax

show running-config aaa authorization command

Modes

Privileged EXEC mode

Usage Guidelines

This command displays the current status for TACACS+ authorization of command privileges for the user role. You must configure at least one TACACS+ server in order for this feature to function.

Examples

Example of the active status:

```
device# show running-config aaa authorization command
aaa command authorization tacacs+
```

Example of the inactive status:

```
device# show running-config aaa authorization command
aaa command authorization none
```

show running-config access-list overlay type vxlan

Displays the running configuration for all overlay VXLAN standard or extended ACLs or for a specific ACL.

Syntax

```
show running-config access-list overlay type vxlan { standard |
   extended } [ overlay-vxlan-acl-name ]
```

Parameters

standard

Specifies one or all standard overlay VXLAN ACLs.

extended

Specifies one or all extended overlay VXLAN ACLs.

overlay-vxlan-acl-name

Specifies an ACL.

Modes

Privileged EXEC mode

Usage Guidelines

Overlay ACLs are supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example displays the running config for an extended overlay ACL.

```
device# show running-config access-list overlay type vxlan extended overlay_vxlan_ext
overlay access-list type vxlan extended overlay_vxlan_ext
seq 10 permit dst-vtep-ip 10.1.1.1 src-vtep-ip any vni 5 native dst-ip any src-ip
100.1.1.1 dst-port any src-port 5555 count sflow (Active)
```

show running-config arp

Displays static ARP entries created in the running configuration, using the **arp** command, with an option to display ARP ACLs.

Syntax

show running-config arp

show running-config arp *ip-address* [**ethernet** *slot* **/** *port* | **ve** *ve-id*]

show running-config arp access-list

show running-config arp access-list *arp-acl-name* [**permit ip host** [*host-ip-address* [**mac host** [*host-mac-address*]]]]

Parameters

ip-address

Specifies the IPv4 address of a static ARP.

ethernet

Specifies a physical Ethernet interface.

slot

Specifies a valid slot number. For devices that do not support line cards, specify **0**.

port

Specifies a valid port number.

ve *ve-id*

Specifies a virtual ethernet (VE) interface.

access-list *arp-acl-name*

Specifies the name of an ARP ACL defined on the device.

permit ip host *host-ip-address*

Specifies rules that permit ARP messages from hosts specified by both IPv4 and MAC addresses.

host-ip-address

Specifies the IPv4 address.

mac host *host-mac-address*

Specifies the MAC address.

Modes

Privileged EXEC mode

Examples

The following example displays a sample run of the **show running-config arp** command.

```
device# show running-config arp
device# arp 12.1.1.2 0000.0000.0001 interface Ethernet 1/72
```

The following example displays a sample run of the **show running-config arp access-list** option.

```
device# show running-config arp access-list
device# arp access-list acl1
 permit ip host 13.1.1.2 mac host 0000.0000.0002
!
```

show running-config control-plan ip subnet-rate-limit

Displays the configured Committed Information Rate (CIR) and Committed Burst Size (CBS) for IPv4 and IPv6 subnet trap frames.

Syntax

show running-config control-plan ip subnet-rate-limit

Modes

Control plane configuration mode

Examples

The following example shows the configured CIR and CBS.

```
device# configure terminal
device(config)# control-plane
device(config-control-plane)# show running-config control-plane ip subnet-rate-limit

control-plane
   ip subnet-rate-limit cir 220 cbs 20
```

show running-config dpod

Displays Dynamic Ports on Demand (DPOD) license information.

Syntax

show running-config dpod [*slot/port*]

Command Default

Displays all port reservations on the local switch.

Parameters

slot

Specifies a valid slot number. For devices that do not support line cards, specify **0**.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display port reservations for a specified port or for all ports on the local switch.

Examples

To display port reservations for all ports on the local switch:

```
device# show running-config dpod 8/15
dpod 8/15
 reserve
!
switch# show running-config dpod 8/16
dpod 8/16
 reserve
```

To display port reservations on a switch that does not support the DPOD feature:

```
device# show running-config dpod

%No entries found
```

show running-config event-handler

Displays details of one or all event-handler profiles configured on the switch. You can filter the results by description, Python-script action, or trigger ID. You can also display the Python-script action associated with a profile.

Syntax

show running-config event-handler [*event-handler-name*]

show running-config event-handler *event-handler-name* **description**

show running-config event-handler *event-handler-name* **action**

show running-config event-handler *event-handler-name* **trigger** [*trigger-id* [**raslog** *raslog-id* [**pattern** *posix-ext-regex*]]]

Parameters

event-handler-name

Specifies the name of the event-handler profile. Valid values can have from 1 through 32 characters. The first character must be alphabetic.

action

Displays by Python script file-names.

description

Describes the event-handler profile. The string can be 1 through 128 characters in length.

trigger *trigger-id*

Specifies an event-handler trigger. When the trigger-condition occurs, a Python script is run.

raslog *raslog-id*

Specifies a RASlog message ID as the trigger.

pattern *posix-ext-regex*

Specifies a POSIX extended regular expression to search for a match within the specified RASlog message ID. For examples, refer to the "trigger" topic.

Modes

Privileged EXEC mode

Output

The **show running-config event-handler** command displays the following information:

Output field	Description
event-handler	Displays the event-handler name.
action python-script	Displays the name of the Python script called if the event handler is triggered.
trigger	Displays a trigger name and definitions

Examples

The following example displays the details of all triggers defined for a specified event-handler.

```
device# show running-config event-handler evh1 trigger
event-handler evh1
 trigger 1 raslog NSM-1001
```

The following example displays the details of the action defined for a specified event-handler.

```
device# show running-config event-handler evh1 action
event-handler evh1
 action python-script vlan.py
```

The following example displays the details of all defined event-handlers.

```
device# show running-config event-handler

event-handler evh1
 trigger 10 raslog NSM-1001
 action python-script vlan.py

event-handler evh2
 trigger 100 raslog NSM-1003
 action python-script vlan.py
!
```

show running-config ip access-list

Displays a list of IPv4 ACLs defined on the switch, including the rules they contain.

Syntax

```
show running-config ip access-list [ { standard | extended }
   [ ACL_name ] ]
```

Parameters

standard

Specifies the standard ACL type.

extended

Specifies the extended ACL type.

ACL_name

Specifies the ACL name.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

Not specifying **standard** or **extended** displays a list of all IPv4 ACLs defined on the switch.

If you specify **standard** or **extended**, you can also specify an ACL.

To display details of IPv4 ACLs bound to interfaces, use the **show access-list ip** command.

Examples

The following example displays the IPv4 ACLs defined on the switch.

```
device# show running-config ip access-list

ip access-list standard stdACL3
  seq 5 permit host 10.20.33.4
  seq 7 permit any
ip access-list extended extdACL5
  seq 5 deny tcp host 10.24.26.145 any eq 23
  seq 7 deny tcp any any eq 80
  seq 10 deny udp any any range 10 25
  seq 15 permit tcp any
ip access-list extended extdACLwithNoRules
```

show running-config ip receive

Syntax

show running-config ip receive [**access-group** [*acl-name* [**sequence**]]]

Parameters

access-group

Specifies IPv4 ACLs applied at device-level.

acl-name

Specifies an IPv4 standard or extended ACL.

sequence

Displays the sequence number. For devices with only one rACL applied, the default sequence number is 10.

Modes

Privileged EXEC mode

Usage Guidelines

Output

The **show running-config ip receive** command displays the following information:

Output field	Description
sequence	Displays the sequence number. For devices with only one rACL applied, the default sequence number is 10.

Examples

The following example displays the sequence numbers for two rACLs applied to a device.

```
device# show running-config ip receive access-group ext1 sequence
ip receive access-group ext1 sequence 10

device# show running-config ip receive access-group std1 sequence
ip receive access-group std1 sequence 20
```

show running-config ipv6

Displays global ipv6 configurations.

Syntax

show running-config ipv6 [**access-list** [**extended** | **standard**] *ipv6-acl-name* **seq** *sequence-number*]

show running-config ipv6 [**import routes**]

show running-config ipv6 [**nd** [**global-suppress-ra** | **ra-dns-server** | **ra-domain-name**]]

show running-config ipv6 [**prefix-list** [**ge** | **le**] *prefix-length*]

show running-config ipv6 [**protocol** [**vrrp** | **vrrp-extended**]

show running-config ipv6 [**receive access-group**]

show running-config ipv6 [**route**]

show running-config ipv6 [**router ospf** [**vrf**]]

Parameters

access-list

Specifies the access-control list (ACL)

extended

Specifies the extended IP ACL.

standard

Specifies the standard IP ACL.

ipv6-acl-name

The IPv6 ACL name.

seq *sequence-number*

Specifies the sequence number.

import routes

Specifies import IPv6 routes.

nd

Displays neighbor discovery commands.

global-suppress-ra

Sets the suppress-ra option globally .

ra-dns-server

Sets the global DNS server option applied on all ND6.

ra-domain-name

Set the global domain name option that applied on all ND6 interfaces.

prefix-list

Specifies the prefix-list.

ge

Specifies the minimum IPv6 prefix length.

prefix-length

The IPv6 prefix length. The range is from 1 through 128.

le

Specifies the maximum IPv6 prefix length.

protocol

Set the global domain name option that applied on all ND6 interfaces.

vrrp

Specifies the Virtual Router Redundancy Protocol IPv6 (VRRPv3).

vrrp-extended

Specifies the Virtual Router Redundancy Protocol IPv6 Extended (VRRPv3-E).

receive

Specifies the receive ACL.

access-group

Specifies to bind or unbind the existing ACL.

route

Specifies the IPv6 unicast static route.

router

Specifies the IPv6 router.

ospf

Specifies the Open Shortest Path First (OSPF) version 3.

vrf

Specifies the VRF instance.

Modes

Privileged EXEC mode

Examples

The following is an example of the **show running-config ipv6** command output.

```
device# show running-config ipv6
ipv6 route 3063:6363::/64 fe80::52eb:1aff:fe97:cf51 ve 4050
ipv6 nd ra-dns-server 2000:1234:122:ffff::ffee
ipv6 nd ra-dns-server 3500:35:0:35::1
ipv6 nd ra-domain-name extreme.com
ipv6 nd ra-domain-name user.co.in
ipv6 nd ra-domain-name netiron.com
```

show running-config ipv6 access-list

Displays a list of IPv6 ACLs defined on the switch, including the rules they contain.

Syntax

```
show running-config ipv6 access-list [ { standard | extended }
   [ ACL_name ] ]
```

Parameters

standard

Specifies the standard ACL type.

extended

Specifies the extended ACL type.

ACL_name

Specifies the ACL name.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

Not specifying **standard** or **extended** displays a list of all IPv6 ACLs defined on the switch.

If you specify **standard** or **extended**, you can also specify an ACL.

To display details of all IPv6 ACLs bound to interfaces, use the **show access-list ipv6** command.

Examples

The following example displays all standard IPv6 ACLs defined on the switch:

```
device# show running-config ipv6 access-list standard
ipv6 access-list standard distList
 seq 10 deny 2001:125:132:35::/64
 seq 20 deny 2001:54:131::/64
 seq 30 deny 2001:5409:2004::/64
 seq 40 permit any
!
ipv6 access-list standard ipv6_acl_std_1
 seq 10 deny 2001:2001::/64 count log
```

show running-config keychain

Displays the configuration details for a specified key chain.

Syntax

show running-config keychain *chain-name*

Parameters

chain-name

Specifies the name of the key chain for which you want to view configuration details.

Modes

Global configuration mode

Examples

The following example shows typical output for the command.

```
device(config)# show running-config keychain child

keychain child
 accept-tolerance 500
 key 1
  key-string $9$XutLBELmbQ765dsLycIP/A== encryption-level 4
  accept-lifetime local true 11:49:11|11/09/2017 11:45:16|11/10/2017
  key-algorithm HMAC-SHA-256
 !
```

show running-config lag hash

Displays non-default LAG hash values.

Syntax

show running-config lag hash [**bos**] [**hdr-count**] [**hdr-start**] [**normalize**] [**pwctrlword**] [**rotate**] [**speculate-mpls**] [**srcport**]

Parameters

bos

(is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.) Ignore the entire MPLS label stack and pick only the BOS label for hashing.

hdr-count *count*

Specifies the number of headers to be considered for LAG hashing. Values range from 1 through 3. The default is 1.

hdr-start

Specifies where to start picking headers for the key generation.

normalize

(is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.) Configures using the same hash in both directions. The default is disabled.

pwctrlword

(is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.) Include or exclude the PW control word in hashing.

rotate *rotate-number*

(is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.) Specify hashing randomness. Values range from 0 through 15. The default is 3.

speculate-mpls

(is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.) Enable MPLS speculate or Ethernet/IP.

srcport

Includes the source port in the hashing configuration. The default is not to include it.

Modes

Privileged EXEC mode

Usage Guidelines

To display all configured values (including defaults), enter the **show port-channel load-balance** command.

Examples

The following example displays the output of the basic **show running-config lag hash** command.

```
device# show running-config lag hash
lag hash hdr-start term
lag hash hdr-count 2
lag hash srcport
```

show running-config ldap-server

Displays the SSH server status in the running-config.

Syntax

show running-config ldap-server [**host** *ipaddr* | **host-name**]

Parameters

host

Identifies the IPv4 address of the host.
ipaddress

IPv4 address of the host.

host-name

Name of the host.

Modes

Privileged EXEC mode

Usage Guidelines

LDAP server configuration is placed at the beginning of the running-config and is part of the global configuration of the device. No entry is shown in the running-config when set to default.

Attributes with default values will not be displayed.

Examples

```
device# show running-config ldap-server host 10.24.65.6
ldap-server host 10.24.65.6 use-vrf mgmt-vrf
port 3890 retries 3 timeout 8 basedn security.extreme.com
device#
```

show running-config mac access-list

Displays a list of MAC ACLs defined on the switch, including the rules they contain.

Syntax

```
show running-config mac access-list [ { standard | extended }
   [ ACL_name ] ]
```

Parameters

standard

Specifies the standard ACL type.

extended

Specifies the extended ACL type.

ACL_name

Specifies the ACL name.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

Not specifying **standard** or **extended** displays a list of all MAC ACLs defined on the switch.

If you specify **standard** or **extended**, you can also specify an ACL.

To display details of all MAC ACLs bound to interfaces, use the **show access-list mac** command.

Examples

The following example displays all MAC ACLs defined on the switch.

```
device# show running-config mac access-list
mac access-list standard stdmacaclin
seq 11 permit 1111.1112.1113 7777.7777.7777 count log
seq 12 permit 1111.1112.1114 7777.7777.7777 count log
```

show running-config password-attributes

Displays global password attributes.

Syntax

show running-config password-attributes [**admin-lockout** | **history** | **login-notify-duration** | **max-retry** | **min-length** | **repeat** | **sequence**]

show running-config password-attributes character-restriction [**lower | numeric | special-char | upper**]

Parameters

admin-lockout

Displays lockout for admin role accounts.

history

Specifies the number of old passwords against which a newly configured password is to be checked.

login-notify-duration

Specifies the duration in hours for which the number of last successful attempts should be notified to administrator when logging in. Use value 0 to disable the notification.

max-retry

Displays the number of failed password logins permitted before a user is locked out. Values range from 0 through 16 attempted logins. The default value is 0.

min-length

Displays the minimum length of the password. Valid values range from 8 through 32 characters. The default is 8 characters.

repeat

Specifies the maximum number (n-1) of consecutive and repetitive characters allowed in a newly configured password.

sequence

Specifies the maximum number (n-1) of consecutive and sequential characters allowed in both forward and reverse direction in a newly configured password.

character-restriction

Displays the restriction on various types of characters.

lower

Displays the minimum number of lowercase alphabetic characters that must occur in the password. Values range from 0 through 32 characters. The default value is 0.

numeric

Displays the minimum number of numeric characters that must occur in the password. Values range from 0 through 32 characters. The default is 0.

special-char

Displays the number of punctuation characters that must occur in the password. All printable, nonalphanumeric punctuation characters, except colon (:) are allowed. Values range from 0 through 32 characters. The default value is 0.

upper

Displays the minimum number of uppercase alphabetic characters that must occur in the password. Values range from 0 through 32 characters. The default value is 0.

Modes

Privileged EXEC mode

Usage Guidelines

The attributes are not displayed when they hold default values.

Examples

The following example displays all global password attributes.

```
device# show running-config password-attributes

password-attributes max-retry 4
password-attributes character-restriction upper 1
password-attributes character-restriction lower 2
password-attributes character-restriction numeric 1
password-attributes character-restriction special-char 1
password-attributes history 3
password-attributes login-modify-duration 1
password-attributes repeat 1
password-attributes sequence 1
```

show running-config radius-server

Displays the local device configuration for the RADIUS server from the configuration database.

Syntax

show running-config radius-server host { *ip-address* | *hostname* }

Parameters

host

Identifies the RADIUS server by host name or IP address.

hostname

Specifies the host name of the RADIUS server.

ip-address

Specifies the IP address of the RADIUS server. IPv4 and IPv6 are supported.

Modes

Privileged EXEC mode

Examples

```
device# show running-config radius-server host 10.38.37.180

radius-server host 10.38.37.180
protocol   pap
key          changedsec
timeout    3
```

show running-config rmon

Displays Remote Monitor configuration information.

Syntax

show running-config rmon [**alarm** | **event**]

Parameters

alarm

Displays the Remote Monitor alarm configuration.

event

Displays the Remote Monitor event configuration

Modes

Privileged EXEC mode

show running-config role

Displays name and description of the configured roles.

Syntax

show running-config role [**name** *role_name* [**desc**]]

Parameters

name *role_name*

Displays roles defined for users.

desc

Displays role descriptions.

Modes

Privileged EXEC mode

Examples

The following example displays all roles configured on the device.

```
device# show running-config role

role name VLANAdmin desc "Manages security CLIs"
role name NetworkAdmin desc "Manages Network CLIs"
```

show running-config rule

Displays configured access rules.

Syntax

show running-config rule [*index*]

show running-config rule *index* { **action** | **command** *command_name* | **operation** | **role** }

show running-config rule { **action** { **reject** | **accept** } | **command** *command_name* | **operation** { **read-only** | **read-write** } | **role** *role-name* }

Parameters

index

Displays the rule with the specified index number. Values range from 1 through 512.

action reject | **accept**

Following the *index* parameter, indicates whether **reject** or **accept** is specified for that rule. If the *index* parameter is not specified, displays all rules with the specified action.

command *command_name*

Displays rule configuration for the specified command. To display a list of supported commands, type a question mark (?). This list varies according to whether or not you specify a rule index.

operation read-only | **read-write**

Following the *index* parameter, indicates whether **read-only** or **read-write** is specified for that rule. If the *index* parameter is not specified, displays all rules with the specified operation.

role *role-name*

Displays rule configuration for the specified role.

Modes

Privileged EXEC mode

Examples

The following example displays the configured roles and their rules.

```
device# show running-config rule

rule 30 action accept operation read-write role NetworkSecurityAdmin
rule 30 command role
!
```

```
rule 31 action accept operation read-write role NetworkSecurityAdmin
rule 31 command rule
!
rule 32 action accept operation read-write role NetworkSecurityAdmin
rule 32 command username
!
rule 33 action accept operation read-write role NetworkSecurityAdmin
rule 33 command aaa
!
rule 34 action accept operation read-write role NetworkSecurityAdmin
rule 34 command radius-server
!
rule 35 action accept operation read-write role NetworkSecurityAdmin
rule 35 command configure
```

The following example displays a single rule.

```
device# show running-config rule 30

rule 30
 action accept operation read-write role NetworkSecurityAdmin command role
```

show running-config sflow

Displays the sFlow configuration from the running configuration file.

Syntax

show running-config sflow

Parameters

None

Modes

Global Configuration Mode

Output

The command displays the following information:

Output Field	Description
sflow enable	Displays the enabled status of the sFlow service.
sFlow update-destination-mac	Displays the enabled status of the sFlow Update Destination MAC feature.
sflow collector (multiple rows)	Displays the configuration information for each configured sFlow collector. Displays IP Address, configured port, and the VRF on which the collector is found.

Examples

```
 SLX# configure terminal
SLX (config)# show run sflow
sflow enable
sflow update-destination-mac
sflow collector 10.1.3.2 6343 use-vrf default-vrf
sflow collector 172.22.108.57 6343 use-vrf mgmt-vrf
sflow collector 2001:10:1:4::2 6343 use-vrf default-vrf
```

show running-config ssh

Displays the Secure Shell (SSH) status in the running-config.

Syntax

show running-config ssh

Modes

Privileged EXEC mode

This example shows common output for the command.

```
device# show running-config ssh
ssh server key rsa 2048
ssh server key ecdsa 256
ssh server key dsa
ssh server use-vrf default-vrf
ssh server use-vrf mgmt-vrf
device#
```

show running-config ssh server

Displays the SSH server status in the running-config.

Syntax

show running-config ssh server

Modes

Privileged EXEC mode

Usage Guidelines

SSH server configuration is placed at the beginning of the running-config and is part of the global configuration of the device. By default, the SSH server listens on mgmt-vrf and default-vrf.

Output

The **show running-config ssh server** command displays the following information:

Output field	Description
algorithm	Whether the SSH server is configured to use the x509v3 digital certificate for SSH authentication.
certificate	Whether the SSH server is configured to use the server and user x509v3 certificate for SSH authentication.
cipher	Identifies the cipher configured for the SSH server.
key	Identifies the configured SSH crypto keys: DSA, ECDSA, RSA.
mac	Identifies the configured MAC algorithms. Supported algorithms are hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1, hmac-sha1-96, hmac-md5, hmac-md5-96, hmac-ripemd160, hmac-ripemd160@openssh.com, umac-64@openssh.com, umac-128@openssh.com, hmac-sha1-etm@openssh.com hmac-sha1-96-etm@openssh.com, hmac-md5-etm@openssh.com, hmac-ripemd160-etm@openssh.com, umac-64-etm@openssh.com, umac-128-etm@openssh.com, and hmac-ripemd160-etm@openssh.com. The default MACs supported in FIPS mode are hmac-sha1, hmac-sha2-256, and hmac-sha2-512.
max-auth-tries	Identifies the maximum number of times the user can attempt to authenticate to the SSH server.
max-idle-timeout	Identifies the maximum about of time that the SSH server can be idle after authentication.

Output field	Description
max-login-timeout	Identifies the maximum amount of time allowed for SSH authentication.
port	Identifies the designated SSH server port.
rekey-interval	Identifies the amount of time allowed for session rekeying.
rekey-volume	Identifies the maximum packet limit, in megabytes, for session rekeying.
use-vrf	Identifies the configured VRF name.

Examples

This example shows output when the SSH service is shutdown on the mgmt-vrf.

```
device# show running-config ssh server
ssh server key rsa 2048
ssh server key ecdsa 256
ssh server key dsa
ssh server use-vrf default-vrf
ssh server use-vrf mgmt-vrf shutdown
device#
```

This example shows output when the SSH service is enabled.

```
device# show running-config ssh server
ssh server key rsa 2048
ssh server key ecdsa 256
ssh server key dsa
ssh server use-vrf default-vrf
ssh server use-vrf mgmt-vrf
device#
```

show running-config ssh server key-exchange

Displays the SSH server key-exchange status in the running-config.

Syntax

show running-config ssh server key-exchange

Modes

Privileged EXEC mode

Examples

Typical command output:

```
device# show running-config ssh server key-exchange
 ssh server key-exchange dh-group-14
```

When SSH Server Key-exchange is configured to DH Group 14:

```
device# show running-config ssh server key-exchange
ssh server key-exchange dh-group-14
```

When SSH Server Key-exchange method has the default value:

```
device# show running-config ssh server key-exchange
% No entries found
```

show running-config system-monitor

Displays the system monitor configuration.

Syntax

show running-config system-monitor [**fan** | **power** | **temp** | **cid-card** | **compact-flash** | **MM** | **LineCard** | **SFM**]

Parameters

fan

Displays the threshold and alert setting for the FAN component.

power

Displays the threshold and alert setting for the power component.

temp

Displays the threshold for the temperature sensor component.

cid-card

Displays the threshold for the CID card component.

compact-flash

Displays the threshold for the compact flash device.

MM

Displays the threshold for the management module.

LineCard

Displays the threshold for the line card.

SFM

Displays the threshold for the switch fabric module.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local switch.

Examples

This example shows typical results. Results vary by device.

```
device# show running-config system-monitor
system-monitor fan threshold marginal-threshold 1 down-threshold 2
system-monitor fan alert state removed action raslog
system-monitor power threshold marginal-threshold 2 down-threshold 3
system-monitor power alert state removed action raslog
system-monitor temp threshold marginal-threshold 1 down-threshold 2
```

```
system-monitor cid-card threshold marginal-threshold 1 down-threshold 2
system-monitor cid-card alert state none action none
system-monitor compact-flash threshold marginal-threshold 1 down-threshold 0
system-monitor MM threshold marginal-threshold 1 down-threshold 0
system-monitor LineCard threshold marginal-threshold 1 down-threshold 2
system-monitor LineCard alert state none action none
system-monitor SFM threshold marginal-threshold 1 down-threshold 2
system-monitor port
```

show running-config telemetry collector

Displays the current configuration of one or all telemetry collectors.

Syntax

show running-config telemetry collector [*collector-name*]

Modes

Privileged EXEC mode

Parameters

collector-name

Specifies a telemetry collector.

Usage Guidelines

The output includes the settings for the currently configured collectors.

Examples

The following example is the basic command.

```
device# show running-config telemetry collector
telemetry collector <collector-profile-1>
  ip <ipv4address1> port <portNum>
  profile system-profile default_system_utilization_statistics
  profile interface-profile default_interface_statistics
  use-vrf mgmt-vrf
  encoding json
  activate
!
```

show running-config telemetry profile

Displays the current configuration settings of Telemetry profiles.

Syntax

show running-config telemetry profile [**enhanced-queue-discard-pkts** | **enhanced-queue-max-queue-depth** | **queue**]

Modes

Privileged EXEC mode

Parameters

enhanced-queue-discard-pkts

Displays a subset of the data highlighting discarded packet information.

enhanced-queue-max-queue-depth

Displays a subset of the data highlighting maximum queue depth information.

queue

Displays the field configuration information for the current telemetry profile queue.

Usage Guidelines

The output includes all default profiles and any custom defined telemetry profiles.

Output

The **show running-config telemetry profile** command displays the following information:

Output field	Description
profile-type	Each profile is identified by a unique profile type.
interval	Interval at which the profile information is streamed to interested clients or collectors.
add field-id	Indicates field identifier available for streaming.
interface intf-range	When applicable to a profile-type, will have additional required parameters.

Examples

Typical command example.

```
device# show running-config telemetry profile
telemetry profile system-utilization default_system_utilization_statistics
```

```
  interval 60
  add total-system-memory
  add total-used-memory
  …
 add uptime
telemetry profile interface default_interface_statistics
  interval 30
  interface 0/1-20
  add out-pkts
  add in-pkts
  …
  add out-discards
  add in-discards
!
```

Example using the **enhanced-queue-discard-pkts** keyword.

```
device# show running-config telemetry profile enhanced-queue-discard-pkts
telemetry profile enhanced-queue-discard-pkts
default_enhanced_queue_discard_pkts_statistics
interval 240
interface-range 0/1-2,0/3:1-2
add discard-pkts
```

Example using the **enhanced-queue-max-queue-depth** keyword.

```
device# show running-config telemetry profile enhanced-queue-max-queue-depth
telemetry profile enhanced-queue-max-queue-depth
default_enhanced_queue_max_queue_depth_statistics
interval 240
interface-range 0/4-5,0/6
add max-queue-depth
```

Example using the **queue** keyword.

```
device# show running-config telemetry profile queue
telemetry profile queue default_queue_statistics
interval 240
interface-range 0/1-2,0/3:1-2
add enq-pkt-count
add enq-byte-count
add discard-pkt-count
add discard-byte-count
add current-queue-size
add max-queue-depth-size
```

show running-config telemetry profile (MPLS)

Displays the attributes configured for MPLS traffic statistics data telemetry streaming.

Syntax

```
show running-config telemetry profile [ mpls-traffic-lsp | mpls-traffic-
   bypass | mpls-traffic-fec ]
```

Parameters

mpls-traffic-lsp

This profile captures the summary of Out-Bytes and Out-Packets for MPLS RSVP LSPs at Ingress.

mpls-traffic-bypass

This profile captures the summary of Out-Bytes and Out-Packets for the MPLS RSVP Bypass LSPs at Ingress.

mpls-traffic-fec

This profile captures the summary of Out-Bytes and Out-Packets for the specified MPLS LDP FEC.

Modes

Privileged EXEC mode

Usage Guidelines

The MPLS profile types are supported only on SLX 9540 and SLX 9640 devices.

The attributes used to gather the MPLS traffic statistics for the mpls-traffic-lsp, mpls-traffic-bypass, and mpls-traffic-fec type profiles are:

- interval
- out-packets
- out-bytes

Examples

In the following examples, default_mpls_traffic_lsp_statistics, default_mpls_traffic_bypass_statistics, and default_mpls_traffic_fec_statistics are the default profiles that are already present in the system.

Example of the attributes configured for the mpls-traffic-lsp profile.

```
device# show running-config telemetry profile mpls-traffic-lsp
default_mpls_traffic_lsp_statistics

telemetry profile mpls-traffic-lsp  default_mpls_traffic_lsp_statistics
interval 240
```

```
lsp lsp1
lsp lsp2
add out-packets
add out-bytes
```

Example of the attributes configured for the mpls-traffic-bypass profile.

```
device# show running-config telemetry profile mpls-traffic-bypass
default_mpls_traffic_bypass_statistics

telemetry profile mpls-traffic-bypass  default_mpls_traffic_bypass_statistics
interval 240
bypass-lsp byp1
bypass-lsp byp2
add out-packets
add out-bytes
```

Example of the attributes configured for the mpls-traffic-fec profile.

```
device# show running-config telemetry profile mpls-traffic-fec
default_mpls_traffic_fec_statistics

telemetry profile mpls-traffic-lsp  default_mpls_traffic_fec_statistics
interval 240
lsp lsp1
lsp lsp2
add out-packets
add out-bytes
```

show running-config telemetry profile (queue)

Displays the attributes configured for telemetry streaming queue statistics.

Syntax

```
show running-config telemetry profile [ enhanced-queue-discard-pkts |
   enhanced-queue-max-queue-depth | queue ]
```

Parameters

enhanced-queue-discard-pkts

This profile captures the summary of 32 queues having most number of packets discarded in descending order of the packet discards observed per device.

enhanced-queue-max-queue-depth

This profile captures the summary of 32 queues reaching the maximum max-queue-size in descending order of the max-queue-size observed per device.

queue

This profile captures the overall queue statistics per device in the system.

Modes

Privileged EXEC mode

Usage Guidelines

The queue profile types are supported only on SLX 9540 and SLX 9640 devices.

The system utilization statistics gathered by the enhanced-queue-discard-pkts profile are:

- interval
- interface range
- discard pkts

The system utilization statistics gathered by the enhanced-queue-max-queue-depth profile are:

- interval
- interface range
- max-queue-depth

The system utilization statistics gathered by the queue profile are:

- interval
- interface range
- enq-pkt-count
- enq-byte-count

- discard-pkt-count
- discard-byte-count
- current-queue-size
- max-queue-depth-size

Examples

Example of the attributes configured for the enhanced-queue-discard-pkts profile.

```
device# show running-config telemetry profile enhanced-queue-discard-pkts
telemetry profile enhanced-queue-discard-pkts
default_enhanced_queue_discard_pkts_statistics
interval 240
interface-range 0/1-2,0/3:1-2
add discard-pkts
```

Example of the attributes configured for the enhanced-queue-max-queue-depth profile.

```
device# show running-config telemetry profile enhanced-queue-max-queue-depth
telemetry profile enhanced-queue-max-queue-depth
default_enhanced_queue_max_queue_depth_statistics
interval 240
interface-range 0/4-5,0/6
add max-queue-depth
```

Example of the attributes configured for the queue profile.

```
device# show running-config telemetry profile queue
telemetry profile queue default_queue_statistics
interval 240
add enq-pkt-count
add enq-byte-count
add discard-pkt-count
add discard-byte-count
add current-queue-size
add max-queue-depth-size
```

show running-config telemetry server

Displays the current configuration of the telemetry server.

Syntax

show running-config telemetry server [**use-vrf**]

Parameters

use-vrf

Displays all VRF configurations. By default, only the default mgmt-vrf is displayed.

Modes

Privileged EXEC mode

Usage Guidelines

The output displays the current configuration for the telemetry server.

Examples

Typical command example.

```
kdevice# show running-config telemetry server
telemetry server use-vrf mgmt-vrf
 transport tcp
 port 50051
!
```

show running-config username

Displays the user accounts on the device.

Syntax

show running-config username [*username*] [**access-time**] [**desc**] [**enable**] [**encryption-level**] [**expire**] [**password**] [**role**]

Parameters

username

Displays the configuration of a specified username. The maximum number of characters is 40.

access-time

Displays access-time configuration.

desc

Displays the description of the user configuration.

enable

Displays the account enablement status.

encryption-level

Password encryption level. Valid values are 0, 7, and 10. The default is 0.

expire

Date until the password remains valid in YYYY-MM-DD format. Valid year values range from 1902 through 2037. By default, passwords do not expire.

password

Account password.

role

The role associated with the account.

Modes

Privileged EXEC mode

Usage Guidelines

To display details for one user only, specify *username* . Otherwise, this command displays all user accounts on the device.

Use the various parameters to query the specified account details.

This command does not display the root account.

Defaults are not displayed.

Examples

The following example displays the user accounts on the device.

```
device# show running-config username

username admin password $6$mAog0c./JxVGu1zy$6wFogQmek0KOEgTav.0DVKXz1vRodc1UCAbipYft/
DWnT5R6/Y3qpq7V3JHlhRNVtwguLgXnzdtBDKPKaXbBg/
 encryption-level 10 role admin desc Administrator
username user password $6$mAog0c./JxVGu1zy$6wFogQmek0KOEgTav.0DVKXz1vRodc1UCAbipYft/
DWnT5R6/Y3qpq7V3JHlhRNVtwguLgXnzdtBDKPKaXbBg/
 encryption-level 10 role user desc User
```

The following example displays a specific user account.

```
device# show running-config username admin

username admin password $6$mAog0c./JxVGu1zy$6wFogQmek0KOEgTav.0DVKXz1vRodc1UCAbipYft/
DWnT5R6/Y3qpq7V3JHlhRNVtwguLgXnzdtBDKPKaXbBg/
 encryption-level 10 role admin desc Administrator
```

The following example displays the enabled status for a specific user account.

```
device# show running-config username admin enable

username admin enable true
```

The following example displays user access on the device.

```
device# show running-config username access-time
username admin access-time ""
username extreme1 access-time 0000
username user access-time ""
username user1 access-time 1700
```

show sflow

Displays sFlow configuration information and statistics.

Syntax

show sflow { **interface** | **all** }

Command Default

sFlow is disabled on all interfaces.

Parameters

all

Displays all sFlow information and statistics.

interface

Displays sFlow information for an Ethernet interface.

Output

The command displays the following information:

Output Field	Description
sFlow services are	Displays the configured status of the sFlow service.
sFlow null0 sampling	Displays the configured status of the sFlow *null0* sampling function.
Global default sampling rate	Displays the configured default sampling rate applicable globally.
Global default counter polling interval	Displays the configured global polling interval for sFlow sampling.
sFlow Agent-ID address	The IP address of this sFlow Agent. This IP is used by the sFlow manager to uniquely identify this sFlow Agent over long periods of time for maintaining history.
sFlow update-destination-mac	Displays the configured status of the sFlow Update Destination MAC feature.
Collector server details	This table displays the following information: • Collector server address - IP address of a sFlow collector device. • Vrf-Name - The name of the VRF on which this collector device is situated. • sFlow datagrams - The number of sFlow datagrams sent to the collector.
ACL based samples collected (permit/deny)	These two rows display the number of *permit* and *deny* samples collected through ACLs.

Output Field	Description
VxLAN Visibility samples collected	Displays the number of VxLAN Visibility samples collected.
VxLAN Gateway samples collected	Displays the number of VxLAN Gateway samples collected.

Modes

Privileged EXEC mode

Examples

The following example displays sFlow information.

```
device# show sflow
sFlow services are:                      enabled
sFlow null0 sampling:                    enabled
Global default sampling rate:            2048 pkts
Global default counter polling interval: 20 secs
sFlow Agent-ID address:                  21.21.21.21
sFlow Source Interface:                  management 0
sFlow update-destination-mac:            enabled
Collector server address                        Vrf-Name      Sflow datagrams sent
-------------------------------------------------------------------------------
                          10.1.3.2:6343         default-vrf                  438
                     172.22.108.57:6343         mgmt-vrf                     438
                    2001:10:1:4::2:6343         default-vrf                  438

ACL based samples collected (permit):    0
ACL based samples collected (deny):      0
VxLAN Visibility samples collected:      0
VxLAN Gateway samples collected:         0
```

show span path session

Displays the SPAN path information.

Syntax

show span path session *session-number*

Parameters

session-number

Specifies the SPAN session.

Modes

Privileged EXEC mode

Examples

The following example displays the SPAN path information.

```
device# show span path session 1

Session                          :1
Path                       :Eth 0/10 -> Eth 0/1 (ISL-exit port) -> Eth 0/16
```

show spanning-tree

Displays Spanning Tree Protocol (STP) information.

Syntax

```
show spanning-tree [ brief | interface { ethernet slot/port | port-
   channel port_channel_number } | pvst | mst [ brief | detail |
   instance instance_id | interface ] mst-config | vlan vlan_id ]
```

Parameters

brief

Display brief spanning tree information.

interface

Display iinformation about the spanning tree configuration on an interface.

ethernet *slot/port*

Display spanning tree information about a specific Ethernet interface.

port-channel *port_channel_number*

Display spanning tree information about a port channel interface.

pvst

Display PVST+ information.

mst

Display MSTP information.

detail

Display detailed MSTP tree information.

instance *instance_id*

Display MSTP information about a specivic instance.

mst-config

Display MSTP region configuration information.

vlan *vlan_id*

Display spanning tree information about a specific VLAN.

Modes

Privileged EXEC mode.

Usage Guidelines

Note
Extreme Networks supports the PVST+ and R-PVST+ protocols. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

Examples

To display spanning tree information:

```
device# show spanning-tree brief

 Spanning-tree Mode: Spanning Tree Protocol

      Root ID      Priority 4096
                   Address 768e.f805.5800
                   Hello Time 8, Max Age 25, Forward Delay 20

      Bridge ID    Priority 4096
                   Address 768e.f805.5800
                   Hello Time 8, Max Age 25, Forward Delay 20

 Interface     Role  Sts  Cost       Prio  Link-type        Edge
 ------------------------------------------------------------------------
 Eth 2/32      DES   FWD  2000       128   P2P               No
 Eth 2/66      DES   FWD  2000       128   P2P               No
 Po 7          DES   FWD  2000       128   P2P               No
 Po 8          DES   FWD  2000       128   P2P               No
 Po 21         DES   LIS  500        128   P2P               No
 Po 141        BKUP  BLK  1000       128   P2P               No
 Po 151        DES   FWD  10000      128   P2P               No
 Po 154        DES   FWD  285        128   P2P               No
 Po 172        BKUP  BLK  1000       128   P2P               No
 Po 173        BKUP  BLK  500        128   P2P               No
```

show ssh client status

Displays the current Secure Shell (SSH) client status, including key-exchange, cipher, mac, and source interface details.

Syntax

show ssh client status

Modes

Privileged EXEC mode

Examples

This example shows the status when the SSH server is enabled.

```
device# show ssh client status
SSH Client Cipher: aes128-cbc,aes192-cbc
SSH Client Mac : hmac-sha1,hmac-sha1-96,hmac-md5
SSH Client Key Exchange Algorithm: diffie-hellman-group-exchange-sha256
device#
```

show ssh server status

Displays the current Secure Shell (SSH) server status.

Syntax

show ssh server status

Modes

Privileged EXEC mode

Global configuration mode

Examples

This example shows the output of the command from privileged EXEC mode.

```
device# show ssh server status
SSH Server Rekey Volume: 1024
SSH Server Auth Tries: 6
SSH Server Login Timeout: 120
VRF-Name: default-vrf    Status: Enabled
VRF-Name: mgmt-vrf    Status: Enabled
device#
```

This example shows the output of the command from global configuration mode.

```
device# configure terminal
device(config)# do show ssh server status
SSH Server Rekey Volume: 1024
SSH Server Auth Tries: 6
SSH Server Login Timeout: 120
VRF-Name: mgmt-vrf      Status: Enabled
VRF-Name: default-vrf   Status: Enabled
```

show startup-config

Displays the contents of the startup configuration.

Syntax

show startup-config

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local device.

Examples

The following example displays the contents of the startup configuration file.

```
device# show startup-config
```

show statistics access-list

Displays ACL statistics for an ACL type and inbound/outbound direction.

Syntax

show statistics access-list { **ip** | **ipv6** | **mac** } *acl-name* { **in** | **out** }

show statistics access-list interface { **ethernet** *slot* **/** *port* | **port-channel** *index* | **ve** *vlan_id* | **vlan** *vlan_id* } { **in** | **out** }

show statistics access-list interface management *mgmt-id* **in**

show statistics access-list { **ip** | **ipv6** } *acl-name* **interface** [**ethernet** *slot* **/** *port* | **port-channel** *index* | **ve** *vlan_id*] { **in** | **out** }

show statistics access-list { **ip** | **ipv6** } *name* **interface management** *mgmt-id* **in**

show statistics access-list mac *acl-name* **interface** [**ethernet** *slot* **/** *port* | **port-channel** *index* | **vlan** *vlan_id*] { **in** | **out** }

show statistics access-list receive { **ip** | **ipv6** } *acl-name*

show statistics access-list global-subnet-broadcast ip *acl-name*

show statistics access-list subnet-broadcast ip *acl-name* [**interface** { **ethernet** *slot* **/** *port* | **ve** *vlan-id* }]

Parameters

interface

Filter by interface.

ethernet

Specifies a physical Ethernet interface.

slot

Specifies a valid slot number. For devices that do not support line cards, specify **0**.

port

Specifies a valid port number.

port-channel *index*

Specifies a port-channel interface.

ve *vlan_id*

Specifies a virtual Ethernet (VE) interface.

vlan *vlan_id*

Specifies a VLAN interface.

management *mgmt-id*

Specifies the management interface. The only supported value is 0.

in | **out**

Specifies the ACL binding direction (incoming or outgoing).

ip | ipv6 | mac

Specifies the network protocol.

acl-name

Specifies the ACL name.

receive

Specifies an IPv4 or IPv6 rACL.

global-subnet-broadcast ip

Specifies an IP broadcast ACL (bACL) applied at device level.

subnet-broadcast ip

Specifies an IP broadcast ACL (bACL) applied at physical-interface or VE level.

Modes

Privileged EXEC mode

Usage Guidelines

You can show statistics for a specific ACL or only for that ACL on a specific interface. You can display statistical information for all ACLs bound to a device physical or management interface, VLAN or VE. You can display statistical information for IPv4 or IPv6 receive-path ACLs. You can display statistical information for IP broadcast ACLs (bACLs).

Statistics are displayed only for rules that contain the **count** keyword.

When ACLs of multiple types are applied to an interface, for multiple matches the counter is incremented only for the higher priority match. Processing priority is as follows: rACLs > PBR > Layer 3 ACLs > Layer 2 ACLs.

Output

The **show statistics access-list** command displays the following information:

Output field	Description
Unaccountable	The counter resource is not allocated. This is typically seen if counting is not supported or if the hardware resources limit is reached.
Unwritten	The rule is inactive and is not programmed in the hardware. This is typically seen when the hardware resources limit is reached.

Examples

The following example displays inbound ACL statistics for a named IPv4 ACL.

```
device# show statistics access-list ip l3ext in
ip access-list l3ext Ethernet 1/8 in
seq 76 deny ip 10.10.75.10 0.0.0.0 any count log (795239 frames)
seq 77 hard-drop ip 10.10.75.10 0.0.0.0 10.10.11.0 0.0.0.255 count log (0 frames)
seq 78 hard-drop ip any 10.10.11.0 0.0.0.255 count log (0 frames)
seq 79 hard-drop ip any 10.10.0.0 0.0.255.255 count log (0 frames)
seq 80 hard-drop ip 10.10.75.10 0.0.0.0 any count log (0 frames)
seq 81 hard-drop ip 10.10.75.0 0.0.0.0 10.10.0.0 0.0.255.255 count log (0 frames)
seq 91 hard-drop ip any any count (0 frames)
seq 100 deny udp 10.10.75.0 0.0.0.255 10.10.76.0 0.0.0.255 count log (0 frames)
seq 1000 permit ip any any count log (0 frames)
```

The following example displays inbound ACL statistics for a specific interface. The ACL named ipv6-std-acl is applied on interface 4/1 to filter incoming routed traffic only.

```
device# show statistics access-list interface ethernet 4/1 in
ipv6 routed access-list ipv6-std-acl on Ethernet 4/1 at Ingress (From User)
    seq 10 permit host 0:1::1
    seq 20 deny 0:2::/64
    seq 30 deny any count (100 frames)
```

The following example displays inbound statistics for all ACLs bound to a specific VE interface.

```
device# show statistics access-list interface ve 3010 in
ipv6 access-list ip_acl_3 on Ve 3010 at Ingress (From User)
    seq 10 deny ipv6 2001:3010:131:35::/64 2001:1001:1234:1::/64 count (0 frames)
    seq 20 permit ipv6 2001:3010:131:35::/64 2001:3001:1234:1::/64
```

The following example displays inbound statistics for ACLs on the management interface.

```
device# show statistics access-list interface management 0 in
ip access-list mgmt-acl on Management 0 at Ingress (From User)
    seq 1 deny tcp host 1.1.1.1 any count (12854 frames)
    seq 2 deny udp host 2.2.2.2 any count (94 frames)
    seq 3 permit tcp any any
    seq 4 permit udp any any

ipv6 access-list mgmt-aclv6 on Management 0 at Ingress (From User)
    seq 1 permit tcp host 2001:4888:a3f:8036:b1b::112 any
    seq 2 deny udp host 2001:4888:a3f:8036:b1c::113 any count (324 frames)
    seq 3 permit tcp any any count (4876 frames)
    seq 4 deny udp any any count (284 frames
```

This example displays statistics for packets that meet the permit and deny rules that are configured for control plane protection.

```
device# show statistics access-list receive ip ip-ssh
ip access-list extended ip-ssh
    seq 5 deny tcp any 14.14.14.14 0.0.0.0 eq 22 count (25 frames)
    seq 10 permit tcp 10.10.10.10 0.0.0.255 any eq 22 count (26 frames)
    seq 20 permit tcp 11.11.11.11 0.0.0.255 any eq 22 count (26 frames)
    seq 100 deny tcp any any eq 22 count (26 frames)
```

The following example displays an ACL definition that supports filtering non-fragmented packets.

```
device# show statistics access-list interface ethernet 0/7 in
ip access-list new_acl on Ethernet 0/7 at Ingress (From User)
    seq 10 permit ip any any non-fragment count (0 frames)
```

The following example displays an ACL definition that supports filtering fragmented packets.

```
device# show statistics access-list interface ethernet 0/7 in
ip access-list test on Ethernet 0/8 at Ingress (From User)
    seq 10 permit ip any any fragment
```

The following example displays an ACL definition that supports flow based ingress miroring.

```
device# show statistics access-list interface ethernet 0/2 in
ip access-list mac1 on Ethernet 0/2 at Ingress (From User)
    seq 10 permit any host 1111.2222.3333 count mirror (100 frames)
    seq 20 permit host 4444.5555.6666 any count (200 frames)
```

The following example displays an ACL definition that supports flow based egress miroring.

```
device# show statistics access-list interface ethernet 0/1 out
ip access-list mac1 on Ethernet 0/1 at Egress (From User)
    seq 10 permit any host 1111.2222.3333 count mirror (0 frames)
    seq 20 permit host 4444.5555.6666 any count (0 frames)
```

show statistics access-list overlay type vxlan

Displays statistics for rules—with count keywords—in a specific overlay VXLAN ACL.

Syntax

show statistics access-list overlay type vxlan *acl-name*

Parameters

acl-name

Specifies an overlay VXLAN ACL.

Modes

Privileged EXEC mode

Usage Guidelines

Overlay ACLs are not supported on SLX 9150 or SLX 9250 devices.

Examples

The following example displays statistics for a specific overlay ACL.

```
device# show statistics access-list overlay type vxlan abc_ext
Number of Rules: 2
seq 1000 permit  dst-vtep-ip-host 200.1.1.1 src-vtep-ip-host 150.1.1.1 vni 1 vni-mask 0
redirect Ethernet 2/65 sflow count 0(pkts)/0(bytes)
seq 1010 permit  dst-vtep-ip-host 200.1.1.2 src-vtep-ip-host 150.1.1.2 vni 2 vni-mask 0
redirect Ethernet 2/19 sflow count 44024773(pkts)/52829727600(bytes)
```

show statistics bridge-domain

Displays statistics for logical interfaces in bridge domains.

Syntax

show statistics bridge-domain *bd-id*

Parameters

bd-id

The bridge domain ID.

Modes

Privileged EXEC mode

Usage Guidelines

Enter the **show statistics bridge-domain** *bd- id* command to view the statistics for a specific bridge domain.

Output

The **show statistics bridge-domain** command displays the following information:

Field	Description
Interface	The interface whose counter statistics are displayed.
RxPkts	The number of packets received at the specified interface.
RxBytes	The number of bytes received at the specified interface.
TxPkts	The number of packets transmitted from the specified interface.
TxBytes	The number of bytes transmitted from the specified interface.

Examples

The following example displays statistics for all logical interfaces in all bridge domains.

```
device# show statistics bridge-domain

Bridge Domain 1 Statistics
Interface                    RxPkts           RxBytes          TxPkts
TxBytes
eth 1/1.100       821729           821729           95940360         95940360
eth 1/21.200      884484           885855           95969584         95484555
po  1.300           8884             8855               9684             9955

Bridge Domain 20 Statistics
Interface                    RxPkts           RxBytes          TxPkts
```

```
TxBytes
eth 1/6.400       821729           821729           95940360         95940360
eth 1/21.100        8884             8855              9684             9955
po  2.40          884484           885855           95969584         95484555
```

The following example displays statistics for all logical interfaces in the bridge domain 1.

```
device# show statistics bridge-domain 1

Bridge Domain 1 Statistics
Interface                    RxPkts           RxBytes          TxPkts
TxBytes
eth 1/1.100       821729           821729           95940360         95940360
eth 1/21.200      884484           885855           95969584         95484555
po  1.300           8884             8855              9684             9955
```

show statistics vlan

Displays the statistics for all ports and port channels on configured VLANs.

Syntax

show statistics vlan *vlan id*

Parameters

vlan ID

The specific VLAN ID.

Modes

Privileged EXEC mode

Usage Guidelines

Enter the **show statistics vlan** *vlan- id* command to view the statistics for all ports and port channels on a specific VLAN.

Output

The **show statistics vlan** command displays the following information:

Field	Description
Interface	The interface whose counter statistics are displayed.
RxPkts	The number of packets received at the specified port.
RxBytes	The number of bytes received at the specified port.
TxPkts	The number of packets transmitted from the specified port.
TxBytes	The number of bytes transmitted from the specified port.

Examples

The following example displays statistics for all ports and port channels on configured VLANs.

```
device# show statistics vlan

Vlan 10 Statistics
Interface     RxPkts           RxBytes          TxPkts           TxBytes
eth 1/1       821729           821729           95940360         95940360
eth 1/2       884484           885855           95969584         95484555
po  1        8884             8855              9684             9955

Vlan 20 Statistics
```

```
Interface     RxPkts           RxBytes          TxPkts           TxBytes
eth 1/6       821729           821729           95940360         95940360
eth 1/21     8884             8855              9684             9955
po  2      884484           885855           95969584         95484555
```

The following example displays statistics for all ports and port channels in the VLAN 10.

```
device# show statistics vlan 10

Vlan 10 Statistics
Interface     RxPkts           RxBytes          TxPkts           TxBytes
eth 1/1       821729           821729           95940360         95940360
eth 1/2       884484           885855           95969584         95484555
po  1        8884             8855              9684             9955
```

show statistics vpn

Displays the VPN statistics for a VRF.

Syntax

show statistics vpn vrf *vrf-id*

Modes

Privileged EXEC mode

Output

The **show statistics vpn** command displays the following information:

Output field	Description
Tnl In-Pkt	Displays in packets.
Tnl Out-Pkt	Displays out packets.

Examples

This example displays the VPN statistic for a VRF.

```
device# show statistics vpn
Output:
VRF Name              Tnl In-Pkt      Tnl Out-Pkt
red                        0               0
```

show storm-control

Displays all BUM (broadcast, unknown unicast and multicast)-related information in the system.

Syntax

show storm-control [**broadcast** | **multicast** | **unknown-unicast** | **interface ethernet** *slot/port* | system]

Parameters

storm-control

Displays all BUM-related information in the system.

broadcast

Displays all BUM-related information in the system for the broadcast traffic type.

multicast

Displays all BUM-related information in the system for the multicast traffic type.

unknown-unicast

Displays all BUM-related information in the system for the unknown-unicast traffic type.

interface ethernet *slot/port*

Displays all BUM-related information in the system for the specified interface.

system

Displays the global storm-control configured rate for the BUM traffic type on the device.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display BUM storm-control-related configuration for the entire system, for specified traffic types, for specified interfaces, or for specified traffic types on a specified interface or globally on the device.

When you specify an interface, the system parameter is not supported.

Examples

This example displays storm control information for broadcast traffic on an Ethernet interface.

```
device# show storm-control broadcast interface ethernet 2/1

Interface   Type             Rate (bps)   Operational Rate (bps) Conformed
```

```
Violated      Total
Et 2/1      broadcast        100000       <value>           12500000000  12500000000
25000000000
```

This example displays storm control information for all traffic on an Ethernet interface.

```
device# show storm-control interface ethernet 2/1
Interface   Type             Rate (bps)   Operational Rate (bps) Conformed
Violated     Total
Et 2/1      broadcast        100000       <value>                12500000000  12500000000
25000000000
Et 2/1      unknown-unicast  100000       <value>                12500000000  12500000000
25000000000
Et 2/1      multicast        100000       <value>                12500000000  12500000000
25000000000
```

This example displays storm control information for all BUM traffic configured globally on the device and specific interfaces.

```
device# show storm-control
Interface   Type             Rate (bps)   Operational Rate (bps) Conformed
Violated      Total
System      broadcast        100000       <value>            0           0           0
System      multicast        8000000000   <value>            0           0           0
Et 2/2      broadcast        100000       <value>           12500000000  12500000000
250000000000
```

This example displays storm control information for all BUM traffic configured globally on the device.

```
device# show storm-control system
Interface   Type             Rate (bps)   Operational Rate (bps) Conformed
Violated      Total
System      broadcast        100000       <value>            0           0           0
System      multicast        8000000000   <value>            0           0           0
```

show support

Displays a list of core files on the device.

Syntax

show support

Command Default

Displays information for the local device.

Modes

Privileged EXEC mode

Usage Guidelines

This command is supported only on the local device.

Pagination is not supported with this command. Use the **More** option to display the output one page at a time.

Examples

To display the core files:

```
device# show support
 No core or FFDC data files found!
```

show system maintenance

Displays details about system maintenance mode, including the current stage and the amount of time to enter and exit maintenance mode.

Syntax

show system maintenance

Modes

Privileged EXEC mode

Usage Guidelines

Maintenance operations such as software upgrade, SFP replacement, cable replacement, and node replacement require the device to be shut down, resulting in traffic disruption even if alternative paths are available. Maintenance mode provides graceful traffic diversion from the maintenance mode node, helping to minimize traffic loss during such planned operations.

Use this command to show the status of maintenance mode, stage information, and the configured time to enter and exit maintenance mode.

Examples

The following example shows sample output of the command.

```
SLX# show system maintenance
Maintenance Mode:
Enabled: True, MM is enabled and Completed

Total number of Stages: 2
Current Stage: 2
Max time required to complete MM enable operation: 60 seconds
Max time required to complete MM disable operation: 300 seconds

Daemon name                  Status (Stage 1)
bgp                          Completed
mct                          Completed
          Time Taken:  (16 secs)

Daemon name                  Status (Stage 2)
bgp                          Completed
mct                          Completed
          Time Taken:  (4 secs)
```

show system maintenance rate-monitoring

Displays the list of interfaces monitored for link utilization.

Syntax

show system maintenance rate-monitoring

Modes

Privileged EXEC mode

Usage Guidelines

The following example displays the usage of the **system maintenance rate-monitoring** command.

```
SLX(config)# interface e 0/1
SLX(conf-if-eth-0/1)# maintenance-mode
SLX(config-maintenance-mode)# rate-monitoring threshold 1000
SLX(config-maintenance-mode)# end
SLX# show system maintenance rate-monitoring
Rate monitored interfaces:
Default - 90% drop from initial traffic rate
Interface
SLX# show system maintenance rate-monitoring
Rate monitored interfaces:
Default - 90% drop from initial traffic rate
================================================================================
Interface              Description    Local State   Exception                 Rate
================================================================================
Ethernet 0/1           Down    Maintenance mode triggered cluster shutdown    100000 kbps
Port-channel 10        Down    Maintenance mode triggered cluster shutdown
Default
SLX#
```

show system monitor tm

Displays the system monitoring configuration for the Traffic Manager (TM) device deleted or discarded packets, or Virtual Output Queue (VOQ) discarded packets.

Syntax

show system monitor tm {**delete-packets** | **discard-packets** | **discard-voq-packets**}

Parameters

delete-packets

Displays the monitoring configuration of the TM device deleted packets.

discard-packets

Displays the monitoring configuration of the TM device discarded packets.

discard-voq-packets

Displays the monitoring configuration of the VOQ discarded packets.

Modes

Privileged EXEC

Output

The **show system monitor tm** command displays the following information:

Output field	Description
Logging-interval	Logging interval in minutes in which a RASlog message is generated.
Threshold	Threshold number of deleted or discarded packets. When the threshold is exceeded, a RASlog message is generated.

Examples

The following example displays the monitoring configuration of the VOQ discarded packets.

```
device# show system monitor tm discard-voq-packet
Discard VOQ packet count monitoring configuration:
Logging-interval :  60 minutes
Threshold        :  10 packets
```

show tech-support

Displays the technical support data using the set of SLX CLI and Linux commands.

Syntax

show tech-support

Usage Guidelines

The output of the show tech-support command is extensive. The information is displayed on the terminal in a telnet/SSH session. In the console session, the output of the command is saved to a file rather than displayed on the console due to the time required to display the results. The output is saved to the file "flash://SLX_show_techsupport.txt" where "SLX" is the hostname of the switch.

Output

The **show tech-support** command displays the technical support data using the following commands.

```
show arp
show bfd
show bfd neighbors vrf all
show bfd neighbors vrf all details
show bridge-domain
show bridge-domain brief
show buffmgr stats slot
show chassis
show clock
show cluster
show cluster member bridge-domain
show cluster member vlan
show environment fan
show environment history
show environment power
show environment sensor
show environment temp
show firmwaredownloadhistory
show firmwaredownloadstatus
show hardware profile current
show hw route-info
show interface
show interface stats brief
show interface status
show inventory
show ip bgp routes all-vrfs
show ip dhcp relay address
show ip dhcp relay statistics
show ip igmp groups detail
show ip igmp interface
show ip igmp snooping
show ip igmp snooping mrouter
show ip interface brief
show ip multicast snooping
show ip multicast snooping mcache
show ip pim bsr
show ip pim group
```

```
show ip pim interface
show ip pim mcache
show ip pim neighbor
show ip pim rp-map
show ip pim rp-set
show ip pim settings
show ip pim traffic
show ip route summary
show ipv6 bgp routes all-vrfs
show ipv6 dhcp relay address
show ipv6 dhcp relay statistics
show ipv6 neighbors
show ipv6 route summary
show lacp counter
show lacp sys-id
show license
show lldp neighbors
show logging auditlog
show logging raslog
show loop-detection
show loop-detection globals
show mac-address-table
show mcastss grange
show mcastss mrouter vlans
show mcastss mrt
show mcastss rp
show mcastss rte brief
show mcastss rte client
show mcastss vif
show mcastss vlangrp
show mcastss vlans
show media
show mpls summary
show overlay-gateway
show port-channel detail
show process cpu
show process cpu all-partitions
show process cpu history
show process memory
show process memory summary
show rmon
show running-config
show spanning-tree brief
show ssh client status
show ssh server status
show support
show system
show tm non-empty-queues
show tm statistics device all
show tunnel brief
show tunnel statistics
show tunnel status
show users
show version
show vlan brief
show vrf
```

Examples

The following example shows the output of the command when executed from the console.

```
device# show tech-support
%INFO: The output to the console is slow. It is saved to flash://
<hostname>_show_techsupport.txt
device#
```

The following example shows the output of the command in a telnet/ssh session as displayed on the terminal, and is truncated below for brevity.

```
device# show tech-support
******************************************************
SLXCLI "show clock"
******************************************************
2019-02-18 17:16:31 Etc/GMT

******************************************************
SLXCLI "show version"
******************************************************
SLX-OS Operating System Version: 19.1.00
Copyright (c) 1995-2019 Extreme Networks, Inc.
Firmware name:      19.1.00d
Build Time:         21:15:15 Feb 16, 2019
Install Time:       12:20:19 Feb 18, 2019
Kernel:             4.14.67
Control Processor:  GenuineIntel
Memory Size:        SLXVM: 23916 MB   System Total: 32079 MB
System Uptime:   0days 4hrs 52mins 22secs
Name     Primary/Secondary Versions
----------------------------------------
SLX-OS   19.1.00d
         19.1.00d
…
```

show telemetry client-cert

Displays the SSL public certificate which will be used for secure transport.

Syntax

show telemetry client-cert

Modes

Privileged EXEC mode

Usage Guidelines

There is no display if there are no certificates configured.

Examples

Typical command example.

```
device# show telemetry client-cert

-----BEGIN CERTIFICATE-----
MIIC2jCCAcICAQEwDQYJKoZIhvcNAQEFBQAwMzELMAkGA1UEBhMCQ0ExEDAOBgNV
BAoMB0Jyb2NhZGUxEjAQBgNVBAMMCWxvY2FsaG9zdDAeFw0xNzAzMjExNzQ1NDNa
Fw0xODAzMjExNzQ1NDNaMDMxCzAJBgNVBAYTAkNBMRAwDgYDVQQKDAdCcm9jYWRl
MRIwEAYDVQQDDAlsb2NhbGhvc3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC+YG/CkiNm/BO+u1mYLKP8cpz/0O9CE+fusO0spXxjKfjPAvK7kiogxABm
bg9MQeWl4SbFa5x3q5uyZJxApJ+tAnnWZa+cbj5pmNsQFfIbFOwSAmFyhh/NIp7Y
/wApskKjnVsMFkarqX8W2xKxZreapZFMa9DGpOeh8Jo2yvcTAimFfSJ4nyKlCr1C
DuuaTSvAttC8Z9mEqD9TOaSYwQI0pnfVO+ySgY8ndqDXYdRvl+bV1taghlKOgxMY
J78lyZxYf6CIn22BAaz/f9a5ffS13Hh5Cmurj2dUmmqDE49p2KEVtXQ3D6nuopli
V49ok+z93/40Uq4OVJZJk5Kx8ZuxAgMBAAEwDQYJKoZIhvcNAQEFBQADggEBAI1d
1VkMH9i3SorPIHpbVqbeDe7LPdaFmrT0COr3AFUECw3gBj1Zy82Kp8XkIJJdVCu8
MNm3wTARqeNBY2c3luw6QeA6l4qRIVM4FqNj6rvtqtNZQ9EEKRRwAm0GSVp+uSvu
E88XSXO+r6N+SXQemRIyhNQ7LJq+cDEaP5WfNtKg+zj085Xd0qiB94BKFt5Q+xAa
B7lwuUvT7Yt92aUVXIaZ6aY5oMv4t7+lPBBKjg8cNeywDa9h3yVZYIzSggghu0qu
GZO57qUh5agxqKiEVf9Ya325u5gj73UJsKOSsyVA1HB8RsPEEdz8j8FBAqMNSTQj
8UDtUGpYiYlzyiBUELc=
-----END CERTIFICATE-----
```

show telemetry collector name

Displays the status of the specified telemetry collector.

Syntax

show telemetry collector name *collector-name*

Parameters

collector-name

Specifies the name assigned to the telemetry collector.

Modes

Privileged EXEC mode

Output

The **show telemetry collector name** command displays the following information:

Output field	Description
Profiles Streamed	The name of the telemetry profile assigned to the collector.
Interval	The configured interval delay for the collector.
Uptime <DD/HH:MM:SS>	The current uptime for the collector.
Last Streamed	The last time the collector was executed.

Examples

The following example displays the status of a collector.

```
device# show telemetry collector name col1

Telemetry data is being streamed to  <col1>  on 10.24.12.96:8080

Profiles Streamed                     Interval  Uptime     Last Streamed
-----------------                     --------  ------     -------------------
default_interface_statistics          30 sec    0/0:12:52  2018-12-12 01:26:47
default_system_utilization_statistics 60 sec    0/0:12:52  2018-12-12 01:26:59
```

show telemetry collector summary

Displays a summary of the telemetry collector configuration.

Syntax

show telemetry collector summary

Modes

Privileged EXEC mode

Usage Guidelines

This command displays the status of the currently active telemetry collector sessions. These are initiated with collectors in the "activated" state.

Output

The **show telemetry collector summary** command displays the following information:

Output field	Description
Name	The collector name.
IP Address:Port	The IPv4 address and port assigned to the collector.
VRF Name	(SLX 9540 and SLX 9640 devices) The VRF name.
Streaming/Connection Status	The current status of the activated collector. Supported values are as follows: • starting_profiles—collector is activated. • streaming—profile data is currently streamed. • streaming_errored—streaming is stopped, for example, if the server is unreachable.

Examples

Example output of the collector configuration summary.

```
device# show telemetry collector summary
Activated Collectors:
--------------------
Name     IP Address:Port   VRF Name  Streaming/Connection Status
-------  ----------------  --------  ---------------------------
 col1    10.24.12.86:8080  mgmt-vrf  streaming
 col2    10.24.12.86:8080  mgmt-vrf  streaming_errored
```

show telemetry server status

Displays the status of the telemetry server.

Syntax

show telemetry server status

Modes

Privileged EXEC mode

Output

The **show telemetry server status** command displays the following information:

Output field	Description
Clients	Clients of the telemetry server.
Profiles Streamed	The profiles assigned to the telemetry server
Interval	The configured interval delay for the telemetry server.
Connected Time	The time when the connection between the telemetry server and the client was established.
Last Streamed	The last time the telemetry profile was streamed.

Examples

Example of typical command output with no errors.

```
device# show telemetry server status
Telemetry Server running on port 50051, with transport as tcp

Clients                  Profile Streamed                        Interval  Connected
Time    Last Streamed
 --------------------    --------------------                    --------
--------------    -------------
ipv4:10.37.73.180:39056  default_system_utilization_statistics  70  2018-12-05 14:11:13
2018-12-05 14:17:10
ipv4:10.37.73.180:39062  default_interface_statistics           30  2018-12-05 14:17:25
2018-12-05 14:17:55
```

show telnet server status

Displays the current Telnet server status.

Syntax

show telnet server status

Modes

Privileged EXEC mode

Examples

To display Telnet server status:

```
device# show telnet server status
VRF-Name: mgmt-vrf      Status: Enabled
VRF-Name: default-vrf   Status: Enabled
```

show threshold monitor

Displays the various threshold monitor statuses and statistics.

Syntax

show threshold monitor [**ecmp** | **host** | **nexthop** | **route** | **sfp**]

Parameters

ecmp

Displays the current threshold configurations for ECMP Table utilization and the hardware table usage.

host

Displays the current threshold configurations for Host Table utilization and the hardware table usage.

nexthop

Displays the current threshold configurations for Next Hop Table utilization and the hardware table usage.

route

Displays the current threshold configuration for Route Table utilization and the hardware table usage.

sfp

Displays the current threshold configurations for SFP monitoring .

Modes

Privilege Execution Mode

Usage Guidelines

None

Examples

This example lists the options available for the **show threshold monitor** command.

```
SLX# configure terminal
SLX (config)# do show threshold monitor ?
Description: Display profile limit and hardware table usage for each resource
Possible completions:
  ecmp      Displays current profile limit and hardware table usage for ECMP
  host      Display current profile limit and hardware table usage for hosts
  nexthop   Displays current profile limit and hardware table usage for nexthop
```

```
  route      Display current profile limit and hardware table usage for routes
  sfp        sfp monitoring
```

show threshold monitor ecmp

Displays details about the current ECMP profile limit and the hardware table usage.

Syntax

show threshold monitor ecmp

Parameters

None

Modes

Privilege Execution Mode

Usage Guidelines

None

Output

The **show threshold monitor ecmp** command displays the following information:

Output Field	Description
Current profile limit	This section contains information about the limits.
ECMP Next-hop	Displays the configured limit.
ECMP Count	This section contains the current statistics.
ECMP Entry	Displays the actual number of ECMP entries and the calculated percentage with respect to the configured maximum.
ECMP Table Usage	Displays the actual space used (in percentage) when compared to the space allocated for the ECMP table.

Examples

The following example shows the output of the **show threshold monitor ecmp** command.

```
SLX# show threshold monitor ecmp

Current profile limit
  ECMP Next-hop : 2000
ECMP count
  ECMP Entry       : 1325 (66%)
  ECMP Table Usage : 57%
```

show threshold monitor host

Displays details about the current Host entries limit and the hardware table usage.

Syntax

show threshold monitor host

Parameters

None

Modes

Privilege Execution Mode

Usage Guidelines

None

Output

The **show threshold monitor host** command displays the following information:

Output Field	Description
Current Profile Limit	This section contains information about the limits.
IPv4 ARP	Displays the configured number of IPv4 ARP entries.
IPv6 ND	Displays the configured number of IPv6 ND entries.
Host count	This section contains the current statistics.
ARP Entry	The actual number of IPv4 ARP entries and the calculated percentage with respect to the configured maximum.
ND Entry	The actual number of IPv6 ND entries and the calculated percentage with respect to the configured maximum.
Host Table Usage	Displays the actual space used (in percentage) when compared to the space allocated for the Host table.

Examples

```
SLX# show threshold monitor host

Current profile limit
  IPv4 ARP : 65024
  IPv6 ND  : 40960
Host count
  ARP Entry        : 13674 (21%)
  ND Entry         : 8759 (21%)
```

```
  Host Table Usage : 26%

SLX#
```

show threshold monitor nexthop

Displays details about the current Next Hop entry limit and the hardware table usage.

Syntax

show threshold monitor nexthop

Parameters

None

Modes

Privilege Execution Mode

Usage Guidelines

None

Output

The command displays the following information:

Output Field	Description
Current profile limit	This section contains information about the limits.
Next-hop	Displays the configured limit.
RH Flowset	Displays the configured limit.
Nexthop count	This section contains the current statistics.
Nexthop Entry	Displays the actual number of Next Hop entries and the calculated percentage with respect to the configured maximum.
RH Flowset Entry	Displays the actual number of RH Flowset entries and the calculated percentage with respect to the configured maximum.
Nexthop Table Usage	Displays the actual space used (in percentage) when compared to the space allocated for the Next Hop table.

Examples

The following example shows the output of the **show threshold monitor nexthop** command.

```
SLX# show threshold monitor nexthop

Current profile limit
  Next-hop   : 48000
  RH Flowset : 32768
```

```
Nexthop count
  Nexthop Entry       : 3673 (7%)
  RH Flowset Entry    : 1878 (6%)
  Nexthop Table Usage : 28%

SLX#
```

show threshold monitor route

Displays details about the current route table limits and the hardware table usage.

Syntax

show threshold-monitor route

Parameters

None

Modes

Privilege Execution Mode

Usage Guidelines

None

Output

The **show threshold monitor route** command displays the following information:

Output Field	Description
Current profile limit	This section contains information about the limits.
IPv4 Route	Displays the configured limit.
IPv6 Route	Displays the configured limit.
Route count	This section contains the current statistics.
IPv4 Route	Displays the actual number of IPv4 Route entries and the calculated percentage with respect to the configured maximum.
IPv6 Route	Displays the actual number of IPv6 Route entries and the calculated percentage with respect to the configured maximum.
Route Table Usage	Displays the actual space used (in percentage) when compared to the space allocated for the Route table.

Examples

The following example shows the output of the **show threshold monitor route** command.

```
SLX# show threshold monitor route

Current profile limit
  IPv4 Route : 163840
  IPv6 Route : 64512
```

```
Route count
  IPv4 Route        : 126741 (77%)
  IPv6 Route        : 19731 (30%)
  Route Table Usage : 45%

SLX#
```

show threshold monitor sfp

Displays details about SFP monitoring limits and their actual values.

Syntax

show threshold monitor sfp all area [**current** | **rxp** | **temperature** | **txp** | **voltage**]

Parameters

current

Displays the status of the current supplied to the SFP transceiver.

rxp

Displays the status of the incoming laser power in microWatts (µW).

temperature

Displays the temperature in degree Celsius.

txp

Displays the status of the outgoing laser power in microWatts (µW).

voltage

Displays the voltage supplied to the SFP in microVolts (µV).

Modes

Privilege Execution Mode

Usage Guidelines

None

Examples

The following example displays the output of the **show threshold-monitor sfp all area current** command.

```
SLX#show threshold monitor sfp all area current

Interface       Type            Area            Value           Status        Monitoring
Status
-------------------------------------------------------------------------------------------
------
Eth 0/20        40GSR           Current         7 mAmps         In Range      Monitoring
Eth 0/5         40GSR           Current         6 mAmps         In Range      Monitoring
Eth 0/18        40GSR           Current         6 mAmps         In Range      Monitoring
Eth 0/9         100GSR          Current         7 mAmps         In Range      Monitoring
```

The following example displays the output of the **show threshold-monitor sfp all area rxp** command.

```
SLX# show threshold monitor sfp all area rxp

Interface       Type            Area            Value           Status        Monitoring
Status
-------------------------------------------------------------------------------------------
------
Eth 0/20        40GSR           Rxp             708 uWatts      In Range      Monitoring
Eth 0/5         40GSR           Rxp             599 uWatts      In Range      Monitoring
Eth 0/18        40GSR           Rxp             833 uWatts      In Range      Monitoring
Eth 0/9         100GSR          Rxp             700 uWatts      In Range      Monitoring
```

The following example displays the output of the **show threshold-monitor sfp all area temperature** command.

```
SLX# show threshold monitor sfp all area temperature

Interface       Type            Area            Value           Status        Monitoring
Status
-------------------------------------------------------------------------------------------
------
Eth 0/28        40GSRINT        Temperature     25 Centigrade   In Range      Monitoring
Eth 0/30        40GSR           Temperature     24 Centigrade   In Range      Monitoring
Eth 0/31        40GSR           Temperature     24 Centigrade   In Range      Monitoring
Eth 0/1         40GSRINT        Temperature     22 Centigrade   In Range      Monitoring
Eth 0/20        40GSR           Temperature     27 Centigrade   In Range      Monitoring
Eth 0/5         40GSR           Temperature     23 Centigrade   In Range      Monitoring
Eth 0/18        40GSR           Temperature     27 Centigrade   In Range      Monitoring
Eth 0/21        40GSR           Temperature     24 Centigrade   In Range      Monitoring
Eth 0/9         100GSR          Temperature     26 Centigrade   In Range      Monitoring
```

The following example displays the output of the **show threshold-monitor sfp all area txp** command.

```
SLX# show threshold monitor sfp all area txp

Interface       Type            Area            Value           Status        Monitoring
Status
-------------------------------------------------------------------------------------------
------
Eth 0/9         100GSR          Txp             1180 uWatts     In Range      Monitoring
```

The following example displays the output of the **show threshold-monitor sfp all area voltage** command.

```
SLX# show threshold monitor sfp all area voltage

Interface       Type            Area            Value           Status        Monitoring
Status
-------------------------------------------------------------------------------------------
------
```

```
Eth 0/28        40GSRINT        Voltage         3296 mVolts     In Range      Monitoring
Eth 0/30        40GSR           Voltage         3278 mVolts     In Range      Monitoring
Eth 0/31        40GSR           Voltage         3283 mVolts     In Range      Monitoring
Eth 0/1         40GSRINT        Voltage         3279 mVolts     In Range      Monitoring
Eth 0/20        40GSR           Voltage         3274 mVolts     In Range      Monitoring
Eth 0/5         40GSR           Voltage         3274 mVolts     In Range      Monitoring
Eth 0/18        40GSR           Voltage         3270 mVolts     In Range      Monitoring
Eth 0/21        40GSR           Voltage         3286 mVolts     In Range      Monitoring
Eth 0/9         100GSR          Voltage         3240 mVolts     In Range      Monitoring
```

show tm voq-stat ingress-device all discards

Displays a summary of the traffic management VOQ discard count for all towers.

Syntax

show tm voq-stat ingress-device all discards [**priority** *traffic_class*] [**max-display** *max_display_number*]

Parameters

priority *traffic_class*

Displays discards for the specified traffic class priority. Enter an integer from 0 through 7.

max-display *max_display_number*

Displays the specified maximum number of discard entries. Enter an integer from 1 through 32.

Modes

Privileged EXEC mode

Usage Guidelines

This command does not apply to SLX 9150 and SLX 9250 devices.

The entries are sorted by the highest number of discards.

If you do not enter the **max-display** *max_display_number* option, a maximum of eight entries is displayed.

Examples

The following example displays the traffic management VOQ ingress discard statistics.

```
device# show tm voq-stat ingress-device all discards

---------------SLOT 3 TOWER 2-------------------
Dest Port  |  Prio  |  Queue  |    Discards
------------------------------------------------
3/1        |   0    |   320   |     2473804
2/4        |   0    |   224   |     1867789
4/2        |   2    |   434   |     1023452
4/8        |   4    |   487   |      920349
1/2        |   1    |   120   |      858723
1/3        |   1    |   128   |       75328
2/5        |   0    |   260   |       22234
2/6        |   0    |   268   |        5248
```

The following example displays the traffic management VOQ ingress discard statistics for a specific traffic class priority.

```
device# show tm voq-stat ingress-device all discards priority 0

---------------SLOT 3 TOWER 2-------------------
Dest Port  |  Prio  |  Queue  |    Discards
------------------------------------------------
3/1        |   0    |   320   |     2473804
2/4        |   0    |   224   |     1867789
2/5        |   0    |   260   |       22234
2/6        |   0    |   268   |        5248
```

show tm voq-stat ingress-device all egress-port ethernet

Displays traffic management Virtual output queue (VOQ) statistics for all towers of an egress Ethernet interface. This command does not apply to the SLX 9150 device.

Syntax

show tm voq-stat ingress-device all egress-port ethernet *slot/port*
[**priority** *number*]

Parameters

slot/port

Specifies the slot and port of the interface.

priority *number*

Optionally specifies the traffic-class priority of the VOQ statistics. Enter an integer from 0 through 7. If you do not include this option, all priorities are displayed.

Modes

Privileged EXEC

Output

The **show tm voq-stat ingress-device all egress-port ethernet** command displays the following information:

Output field	Description
Priority	Traffic-class priority number of the VOQ statistics.
EnQue Pkt Count	The count of all packets entering ingress queues on this traffic manager.
EnQue Bytes Count	The count of all bytes entering ingress queues on this traffic manager.
Total Discard Pkt Count	The count of all packets failing to enter ingress queues on this traffic manager.
Total Discard Bytes Count	The count of all bytes failing to enter ingress queues on this traffic manager.
Current Queue Depth	The current queue depth.
Maximum Queue Depth since Last read	The maximum queue depth since last access to read.

Examples

The following example displays the VOQ statistics for traffic-class priority 0 on Ethernet interface 1/4.

```
show tm voq-stat ingress-device all egress-port ethernet 1/4 priority 0

VOQ-Counters:
==================================================

Priority 0
------------------------------------------------
EnQue Pkt Count                          0
EnQue Bytes Count                        0
Total Discard Pkt Count                  0
Total Discard Bytes Count                0
Current Queue Depth                      0
Maximum Queue Depth since Last read      0
```

show tm voq-stat ingress-device all max-buffer-util

Displays the traffic management VOQ maximum buffer size and utilization statistics for all towers.

Syntax

show tm voq-stat ingress-device all max-buffer-util

Modes

Privileged EXEC mode.

Usage Guidelines

This command does not apply to SLX 9150 and SLX 9250 devices.

Examples

The following example displays the VOQ maximum buffer utilization statistics.

```
device# show tm voq-stat ingress-device all max-buffer-util

--------- Slot 1 Tower 1 ---------
  Max Buffer Size |  Max Buffer Util
-----------------------------------
       6007013804 |       96%
....
```

show tm voq-stat ingress-device all max-queue-depth

Displays the traffic management VOQ max-queue-depth statistics for all towers. This command does not apply to the SLX 9150 device.

Syntax

show tm voq-stat ingress-device all max-queue-depth [**max-display** *max_display_number*] [**min-threshold** *filter_number*] [**priority** *traffic_class*]

Parameters

max-display *max_display_number*

Specifies the maximum displayed entries. Enter an integer from 1 to 32.

min-threshold *filter_number*

Ignores the maximum queue depths below the specified min-threshold filter in bytes. Enter an integer from 1 through 1048640.

priority *traffic_class*

Displays only the specified traffic-class priority. Enter an integer from 0 through 7.

Modes

Privileged EXEC mode.

Usage Guidelines

The entries are sorted by the highest number of discards.

If you do not enter the **max-display** *max_display_number* option, a maximum of eight entries is displayed.

Examples

The following example displays the traffic management VOQ maximum queue depth statistics.

```
device# # show tm voq-stat ingress-device all max-queue-depth

------------------ Slot 1 Tower 1 --------------------
Dest Port   |  Prio  |  Queue  |   Max Depth  |  Max Util
-----------------------------------------------------------
3/1         |   0    |   320   |     1013804  |     96%
2/4         |   0    |   224   |      902789  |     86%
4/2         |   2    |   434   |      543440  |     51%
4/8         |   4    |   487   |      220349  |     21%
1/2         |   1    |   120   |      138723  |     13%
1/3         |   1    |   128   |       97328  |      9%
2/5         |   0    |   260   |       34234  |      3%
2/6         |   0    |   268   |       11723  |      1%
```

```
. . . .
```

show tm voq-stat ingress-device ethernet

Displays traffic management VOQ statistics for a specific ingress Ethernet interface.

Syntax

show tm voq-stat ingress-device ethernet *slot/port* { **discards** [**max-display** *max_display_number* | **priority** *traffic_class*] | **egress-port ethernet** *slot/port* [**priority** *traffic_class*] | **max-buffer-util** | **max-queue-depth** [**max-display** *max_display_number* | **min-threshold** *minimum_threshold* [**max-display** *max_display_number* | **priority** *traffic_class*] | **priority** *traffic_class*] }

Parameters

slot/port

The Ethernet slot and port

discards

Specifies discarded

max-display *max_display_number*

Limits the display of discards. The values range from 1 to a maximum of 32.

priority *traffic_class*

Displays discards by their traffic class priority. Priority values range from 0 through 7.

egress-port *slot/port*

The outbound port.

max-buffer-util

Displays a summary of traffic management VOQ maximum buffer utilization.

max-queue-depth

Displays a summary of traffic management VOQ maximum queue depth statistics.

max-display *max_display_number*

Limits the output to a maximum number of display entries. Values range from 1 to 64 entries.

min-threshold *minimum_threshold*

Specifies that the results omit max-queue-depths values below the minimum byte threshold. The minimum threshold values range from 1 to 1048640 bytes.

Modes

Privileged EXEC mode.

Usage Guidelines

This command does not apply to SLX 9150 and SLX 9250 devices.

Examples

This example displays traffic management VOQ statistics for an egress interface.

```
device# show tm voq-stat ingress-device ethernet 2/1 egress-port ethernet 2/7 priority 2

VOQ-Counters:
=================================================

Priority 2
-----------------------------------------------
EnQue Pkt Count                          67404602
EnQue Bytes Count                        1768413221
Total Discard Pkt Count                  0
Total Discard Bytes Count                0
Current Queue Depth                      0
Maximum Queue Depth since Last read      160
```

This example displays a summary of traffic management VOQ maximum queue depth statistics for a specific ingress interface.

```
device# show tm voq-stat ingress-device 2/1 max-queue-depth

------------------ Ports 1/1 - 1/36 --------------------
Dest Port   |  Prio  |  Queue  |   Max Depth  |  Max Util
-----------------------------------------------------------
3/1         |   0    |   320   |     1013804  |     96%
2/4         |   0    |   224   |      902789  |     86%
4/2         |   2    |   434   |      543440  |     51%
4/8         |   4    |   487   |      220349  |     21%
1/2         |   1    |   120   |      138723  |     13%
1/3         |   1    |   128   |       97328  |      9%
2/5         |   0    |   260   |       34234  |      3%
2/6         |   0    |   268   |       11723  |      1%
```

This example displays a summary of traffic management VOQ maximum buffer utilization for a specific ingress interface.

```
device# show tm voq-stat ingress-device 2/1 max-buffer-util

--------- Ports 1/1 - 1/36 ---------
  Max Buffer Size |  Max Buffer Util
-----------------------------------
       6007013804 |       96%
```

This example displays a summary of traffic management VOQ discards for a specific ingress interface.

```
device# show tm voq-stat ingress-device 2/1 discards

---------------- Ports 1/1 - 1/36 --------------------
Dest Port   |  Prio  |  Queue  |    Discards
-----------------------------------------------------
3/1         |   0    |   320   |     2473804
```

```
2/4         |   0    |   224   |     1867789
4/2         |   2    |   434   |     1023452
4/8         |   4    |   487   |      920349
1/2         |   1    |   120   |      858723
1/3         |   1    |   128   |       75328
2/5         |   0    |   260   |       22234
2/6         |   0    |   268   |        5248
```

show tm voq-stat slot

Displays the traffic management VOQ statistics for a line card in a named slot.

Syntax

show tm voq-stat slot *slot_number* [**cpu-group** [*cpu_group_id* | **all**]]

Parameters

slot_number

The number of the line card slot. For devices that do not support line cards, specify 0 for the slot.

cpu-group *cpu_group_id*

The ID number for the CPU group.

Modes

Privileged EXEC mode

Examples

The following example displays information about the VOQ for the line card in slot 1 CPU group 1.

```
device# show tm voq-stat slot 1 cpu-group 1
CPU Group 1 Prio 0
    EnQue Pkt Count                                        100
    EnQue Bytes Count                                    22400
    Total Discard Pkt Count                              0
    Total Discard Bytes Count                            0
    Current Queue Depth                                     0
    Maximum Queue Depth since last read         0

  CPU Group 1 Prio 1
    EnQue Pkt Count                                        100
    EnQue Bytes Count                                    22400
    Total Discard Pkt Count                           0
    Total Discard Bytes Count                         0
    Current Queue Depth                                  0
    Maximum Queue Depth since last read        0

  CPU Group 1 Prio 2
    EnQue Pkt Count                                        100
    EnQue Bytes Count                                    22400
    Total Discard Pkt Count                           0
    Total Discard Bytes Count                         0
    Current Queue Depth                                  0
    Maximum Queue Depth since last read        0

  CPU Group 1 Prio 3
    EnQue Pkt Count                                        100
    EnQue Bytes Count                                    22400
    Total Discard Pkt Count                           0
    Total Discard Bytes Count                         0
```

```
  Current Queue Depth                                 0
  Maximum Queue Depth since last read        0

CPU Group 1 Prio 4
  EnQue Pkt Count                                   100
  EnQue Bytes Count                               22400
  Total Discard Pkt Count                     0
  Total Discard Bytes Count                   0
  Current Queue Depth                               0
  Maximum Queue Depth since last read        0

CPU Group 1 Prio 5
  EnQue Pkt Count                                   100
  EnQue Bytes Count                               22400
  Total Discard Pkt Count                     0
  Total Discard Bytes Count                   0
  Current Queue Depth                               0
  Maximum Queue Depth since last read        0

CPU Group 1 Prio 6
  EnQue Pkt Count                                   100
  EnQue Bytes Count                               22400
  Total Discard Pkt Count                     0
  Total Discard Bytes Count                   0
  Current Queue Depth                               0
  Maximum Queue Depth since last read        0

CPU Group 1 Prio 7
  EnQue Pkt Count                                   100
  EnQue Bytes Count                               22400
  Total Discard Pkt Count                     0
  Total Discard Bytes Count                   0
  Current Queue Depth                               0
  Maximum Queue Depth since last read        0
```

show topology-group

Displays topology group information.

Syntax

show topology-group [*group-id*]

Parameters

group-id

Displays the information of the topology group of the specified ID.

Modes

Privileged EXEC mode

Output

The **show topology-group** command displays the following information.

Output field	Description
master-vlan	The master VLAN for the topology group. The settings for STP, MRP, or VSRP on the control ports in the master VLAN apply to all control ports in the member VLANs within the topology group.
member-vlan	The member VLANs in the topology group.
Common control ports	The master VLAN ports that are configured with Layer 2 protocol information. The Layer 2 protocol configuration and state of these ports in the master VLAN applies to the same port numbers in all the member VLANs.
Per vlan free ports	The ports that are not controlled by the Layer 2 protocol information in the master VLAN.

show tpm

Displays the various certificates stored within the TPM chip.

Syntax

show tpm [**ekcert** | **iakcert** | **idevidcert**]

Parameters

ekcert

Displays the Endorsement Key (EK) certificate stored within the TPM chip. EK certificate is provided by the manufacturer of the TPM chip.

iakcert

Displays the Initial Attestation Key (IAK) certificate stored within the TPM chip.

idevidcert

Displays the Initial Device Identifier (IDevID) certificate stored within the TPM chip.

Modes

EXEC mode

Examples

This example uses the **show system** command to view the current state of the provisioning state of the TPM chip on the device.

```
SLX# show system

Stack MAC : 40:88:2f:c1:b4:1d

-- UNIT 0 --
Unit Name : SLX
Up Time : up 23 min
Current Time : 21:32:02 GMT
SLX-OS Version : 20.2.3
Jumbo Capable : yes

Burned In MAC : 40:88:2f:c1:b4:18
.
.

-- Fan Status --
Fan 1 is Ok, speed is 6400 RPM
Fan 2 is Ok, speed is 6400 RPM
Fan 3 is Ok, speed is 6560 RPM
Fan 4 is Ok, speed is 6400 RPM
Fan 5 is Ok, speed is 6400 RPM
Fan 6 is Ok, speed is 6400 RPM

-- TPM Status --
```

```
TPM Provision status: Provisioned

SLX#
```

This example displays the options available for the **show tpm** command.

```
SLX# show tpm

Possible completions:
    ekcert      Show Endorsement Key (EK) certificate
    iakcert     Show Initial Attestation Key (IAK) certificate
    idevidcert  Show Initial Device Identifier (IDevID) certificate
```

This example displays the EK certificate

```
SLX# show tpm ekcert

SHA1 Fingerprint=5C:7D:FE:A7:95:DD:01:44:99:3C:14:F1:A1:AA:50:7D:E3:44:15:11
Issuer: C=DE, O=Infineon Technologies AG, OU=OPTIGA(TM) TPM2.0, CN=Infineon OPTIGA(TM)
RSA Manufacturing CA 034
Not Before: Jul 18 20:01:45 2020 GMT
Not After : Jul 18 20:01:45 2035 GMT
```

This example displays the IAK certificate

```
SLX# show tpm iakcert

SHA1 Fingerprint=59:B8:FE:E2:73:5A:35:B5:D6:B9:F8:B3:BB:7B:04:FD:9A:E7:6D:5E
Subject: C=US, O=Fake, OU=Trusted Delivery, CN=8720-32C:TH012045Q-40001
Issuer: C=US, O=Fake, OU=Trusted Delivery, CN=Fake TD E-0 Switch LCA 20200731
Not Before: Nov 23 14:24:21 2020 GMT
Not After : Nov 23 14:23:21 2035 GMT
```

This example displays the IDevID certificate

```
SLX# show tpm idevidcert

SHA1 Fingerprint=2F:1A:B8:E7:CB:D7:67:D2:3B:81:FB:F8:60:16:06:AF:21:FE:D9:AF
Subject: C=US, O=Fake, OU=Trusted Delivery, CN=8720-32C:TH012045Q-40001
Issuer: C=US, O=Fake, OU=Trusted Delivery, CN=Fake TD E-0 Switch LCA 20200731
Not Before: Nov 23 14:24:22 2020 GMT
Not After : Nov 23 14:23:22 2035 GMT
```

show tpvm

Displays status of Third-Party Virtual Machine (TPVM) applications.

Syntax

show tpvm [**disk** { **add name** { *disk_name* | **auto** *disk_size* } | **remove name** { *disk_name* | **auto** }

show tpvm ip-address

show tpvm status [**clear-tag** *tag-name*]

Command Default

This feature is not enabled.

Parameters

install

Installs TPVM.

disk

Displays disk information.

disk_name

Specifies a disk.

all

Specifies all disks.

ip-address

Displays IPv4 and IPv6 addresses that are configured on TPVM.

status

Displays TPVM information.

Modes

Privileged EXEC mode

Usage Guidelines

This command **show tpvm status** displays the installed TPVM version and the status of Passwordless SSH configuration, AutoStart, and TPVM.

If TPVM is installed on older SLX images or if firmware download is done multiple times, SLX cannot retrieve the TPVM version. If SLX cannot retrieve the TPVM version, the “Version Not Found” message will be displayed.

Examples

To display the installed TPVM version and status of Passwordless SSH configuration, AutoStart and TPVM or any errors:

```
device# show tpvm status
SSH and Sudo passwordless       :Disabled
AutoStart                       :Disabled
Tpvm status                     :Installed
Tpvm version                    :4.1.1
device# show tpvm status
SSH and Sudo passwordless       :Disabled
AutoStart                       :Disabled
Tpvm status                     :Installed
Tpvm version                    :Version Not Found
```

To display disk information, by using either the all keyword or specifying a disk name:

```
[SLX]# show tpvm disk all
disk: vdb
Capacity: 70.00 GiB
Allocation: 196.00 KiB

disk: vdc
Capacity: 30.00 GiB
Allocation: 196.00 KiB

total:
Capacity: 100.00 GiB
Allocation: 100.00 GiB
Available: 0.00 B

[SLX]# show tpvm disk blade vdb
disk: vdb
Capacity: 70.00 GiB
Allocation: 196.00 KiB

total:
Capacity: 100.00 GiB
Allocation: 100.00 GiB
Available: 0.00 B
```

To display IPv4 and IPv6 addresses that are configured on TPVM, in this example on MM1:

```
[SLX]# show tpvm ip-address mm1
[ TPVM running on MM1 ]
IPv4:
eth0 10.24.7.80
IPv6:
eth0 fe80::5054:ff:fe9c:446d
eth1 fe80::7:d0ff:fe02:100
```

Note
The show ip-address keywords require the *qemu-guest-agent* package on TPVM. If this package is removed, the keyword fails.

Note
This section is a new addition and will be used to track changes made to this command from SLX-OS 20.2.2 release. It will not record command change history previous to this release.

show tpvm config

Displays the configuration of DNS, Hostname, LDAP, NTP, Timezone and Trusted-Peer for a Third-Party VM (TPVM) and now gets/display IPv6 configurations with IPv4 configurations.

Syntax

show tpvm config {**dns** | **hostname** | **ldap** | **ntp** | **timezone** | **trusted-peer** }

Parameters

dns | **hostname** | **ldap** |**ntp** |**timezone** |**trusted-peer**

Specifies the type of configuration you want to display: DNS, Hostname, LDAP, NTP, Timezone and Trusted-Peer.

Modes

Privileged EXEC mode

Examples

This example shows sample DNS output.

```
device# show tpvm config dns

nameserver 1.2.3.4
nameserver 1.1.1.1
search example.com
```

This example shows sample Hostname output.

```
device# show tpvm config hostname tpvm
```

This example shows sample LDAP output.

```
device# show tpvm config ldap

ldaps server: 10.24.15.200:636;
ldaps server: 1.1.1.1:234;
Base DN: dc=ldap,dc=hc-fusion,dc=in
Root DN: cn=admin,dc=ldap,dc=hc-fusion,dc=in
Root Password: Configured
Certificate Exists: Yes
```

This example shows sample NTP output.

```
device# show tpvm config ntp

NTP Servers: time.google.com 10.20.232.222
    Local time: Sat 2020-04-11 08:33:20 UTC
    Universal time: Sat 2020-04-11 08:33:20 UTC
    RTC time: Sat 2020-04-11 08:33:21
    Time zone: Etc/UTC (UTC, +0000)
System clock synchronized: yes
systemd-timesyncd.service active: yes
```

```
    RTC in local TZ: no

systemd-timesyncd.service - Network Time Synchronization
Loaded: loaded (/lib/systemd/system/systemd-timesyncd.service; enabled;
    vendor preset: enabled)
Active: active (running) since Sat 2020-04-11 08:33:13 UTC; 7s ago
Docs: man:systemd-timesyncd.service(8)
Main PID: 3717 (systemd-timesyn)
Status: "Synchronized to time server 216.239.35.12:123 (time.google.com)."
Tasks: 2 (limit: 4638)
CGroup: /system.slice/systemd-timesyncd.service
    3717 /lib/systemd/systemd-timesyncd
Apr 11 08:33:13 tpvm systemd[1]: Starting Network Time Synchronization...
Apr 11 08:33:13 tpvm systemd[1]: Started Network Time Synchronization.
Apr 11 08:33:13 tpvm systemd-timesyncd[3717]: Synchronized to time server
    216.239.35.12:123 (time.google.com).
```

This example shows sample Timezone output.

```
device# show tpvm config timezone
Etc/GMT
```

This example shows sample Trusted-Peer output.

```
device# show tpvm config trusted-peer
root@10.24.11.233
```

show tpvm config password-policy

Displays the configured password policy for the default TPVM user.

Syntax

show tpvm config password-policy { **character-restrictions** | **min-length** }

show tpvm config password-policy min-length

show tpvm config password-policy character-restriction {lower | numeric | special-char | upper}

Parameters

min-length

Displays the configured minimum length of the TPVM password.

character-restriction

Configures the constraints on use of various types of characters in the TPVM password.

lower

Displays the minimum number of lower case characters that must be included in the TPVM password.

number

Displays the minimum number of digits [0-9] that must be included in the TPVM password.

special-char

Displays the minimum number of special characters that must be included in the TPVM password.

upper

Displays the minimum number of upper case characters that must be included in the TPVM password.

Modes

Privileged EXEC mode

Examples

This example shows the current configuration of the password policy applied for the TPVM user password.

```
SLX# show tpvm config password-policy min-length
12
SLX# show tpvm config password-policy character-restriction lower
4
SLX# show tpvm config password-policy character-restriction numeric
3
SLX# show tpvm config password-policy character-restriction special-char
```

```
2
SLX# show tpvm config password-policy character-restriction upper
3
SLX#
```

show tunnel

Displays information pertaining to a tunnel interface.

Syntax

show tunnel [*tunnel-id* | **brief** | **replicator** | **statistics** | **status**]

show tunnel brief [*tunnel-id* | **dst-ip** *< ip address >* | **mode** [**gre** | **vxlan** [**unicast** | **multicast**]] | **overlay-gateway** | **src-ip** *<ip address>*]

show tunnel statistics [*tunnel-id* | **dst-ip** *< ip address >* | **mode** [**gre** | **vxlan** [**unicast** | **multicast**]] | **overlay-gateway** | **src-ip** *<ip address>*]

show tunnel status [*tunnel-id* | **count** | **dst-ip** *< ip address >* | **mode** [**gre** | **vxlan** [**unicast** | **multicast**]] | **overlay-gateway** | **src-ip** *<ip address>*]

show tunnel replicator

Parameters

tunnel-id

Specifies the tunnel ID.

brief

Displays brief information of tunnels.

count

Displays tunnels count.

dst-ip

Filters by tunnel destination IP address.

gre

Filters by GRE tunnels.

vxlan

Filters by vxlan tunnels.

mode

Filters by tunnel mode.

multicast

Displays multicast tunnels.

overlay-gateway

Filters by Overlay gateway name.

replicator

Displays tunnels to NSX replicators.

src-ip

Filters by tunnel source IP address.

statistics

Displays tunnel statistics.

status

Displays listing of tunnel id and states.

unicast

Displays uinicast tunnels.

Modes

Privileged EXEC Mode

Examples

This example display tunnel information.

```
SLX# show tunnel brief
Tunnel 61441, mode VXLAN, node-ids 1
Admin state up, Oper state up, unicast
Source IP 25.25.25.25 ( Loopback 2 ), Vrf default-vrf
Destination IP 30.30.30.30

Tunnel 61442, mode VXLAN, node-ids 1
Admin state up, Oper state up, multicast
Source IP 25.25.25.25 ( Loopback 2 ), Vrf default-vrf
Destination IP 239.0.0.1
SLX# show tunnel 61442
Tunnel 61442, mode VXLAN, node-ids 1
Ifindex 0x7c00f002, Admin state up, Oper state up, multicast
Overlay gateway "gw", ID 1
Source IP 25.25.25.25 ( Loopback 2 ), Vrf default-vrf
Destination IP 239.0.0.1
Configuration source PIM-SSM/MDT
MAC learning N/A
Tunnel QOS mode  TTL: PIPE, DSCP: PIPE
Active next hops on node 1: #here we list all outgoing ports(2 in this case)
IP: 10.3.6.3, Vrf: default-vrf
Egress L3 port: Ve 36, Outer SMAC: 609c.9f5a.3d15
Outer DMAC: 609c.9fde.7715, ctag: 36
BUM forwarder: yes

IP: 20.3.6.3, Vrf: default-vrf
Egress L3 port: Ve 37, Outer SMAC: 609c.9f5a.3e26

Outer DMAC: 609c.9fde.8815, ctag: 37
BUM forwarder: yes

Packet count: RX 0    TX 1066031994
Byte count : RX 0    TX 127923839280
```

show udld

Shows global UDLD information.

Syntax

show udld

Modes

Privileged EXEC mode

Usage Guidelines

This command displays global unidirectional link detection (UDLD) protocol configuration values such as whether the protocol is enabled on the switch and the *hello* time and timeout values.

Examples

The following example displays global UDLD information for the device.

```
device# show udld
UDLD Global Information
  Admin State:       UDLD enabled
  UDLD hello time:   500 milliseconds
  UDLD timeout:      2500 milliseconds
```

show udld interface

Displays unidirectional link detection (UDLD) protocol information for the specified interface.

Syntax

show udld interface [**ethernet** *slot/port*]

Parameters

ethernet

Specifies a physical Ethernet interface.

slot

Specifies a valid slot number. For devices that do not support line cards, specify **0**.

port

Specifies a valid port number.

Modes

Privileged EXEC mode.

Usage Guidelines

The following describes the values that appear in the output headings for this command.

Table 20: Description UDLD headings

Heading	Description
State	Describes if UDLD is enable or disabled.
Mode	Describes if the mode is Receive, Transmit, or Both (Transmit/Receive).
Advertise Transmitted	Describes how often the advertisement is transmitted.
Hold time for advertise	Describes the hold time for receiving devices before discarding.
Re-init Delay Timer	The timer for the reinitializing delay
Tx Delay Timer	The timer for transmission
DCBX Version	The current DCBX version
Auto-Sense	States whether Auto-Sense is active.
Transmit TLVs	Describes what information is being transmitted for the TLV.
DCBX FCoE Priority Bits	Describes the current FCoE priority bit for DCBX.

Examples

To display UDLD information for a specific Ethernet interface:

```
device# show udld interface ethernet 2/6
Global Admin State:  UDLD enabled

UDLD information for Ethernet 2/6
  UDLD Admin State:                 Enabled
  Interface Operational State:      Bidirectional link
  Remote hello time:                Unknown
  Remote MAC Addr:                  0024.3890.0d81
  Local system id:  0x9f01fee0      Remote system id: 0x24900c00
  Local port :      2/6             Remote port :     9/2
  Local link id:    0x0             Remote link id:   0x0
  Last Xmt Seq Num: 43849           Last Rcv Seq Num: 43880
```

show udld statistics

Shows UDLD statistics.

Syntax

show udld statistics [**interface ethernet** *slot/port*]

Parameters

ethernet

Specifies a physical Ethernet interface.

slot

Specifies a valid slot number. For devices that do not support line cards, specify **0**.

port

Specifies a valid port number.

Modes

Privileged EXEC mode

Usage Guidelines

This command displays all unidirectional link detection (UDLD) protocol statistics or shows the statistics on a specified por

Examples

To show UDLD statistics on a specific Ethernet interface:

```
device# show udld statistics interface ethernet 5/1
UDLD Interface statistics for Ethernet 5/1
Frames transmitted: 310
Frames received: 301
Frames discarded: 0
Frames with error: 0
Remote port id changed: 0
Remote MAC address changed: 0
```

show users

Displays the users logged in to the system and locked user accounts.

Syntax

show users

Modes

Privileged EXEC mode

Examples

The following example displays active user sessions and locked user accounts.

```
device# show users
**USER SESSIONS**
Username    Role    Host IP       Device    Time Logged In
jsmith      user    192.0.2.0     Cli       2016-04-30 01:59:35
jdoe        admin   192.0.2.1     Cli       2016-05-30 01:57:41

**LOCKED USERS**
testUser
```

show version

Displays the current firmware version and other

Syntax

show version [**all-partitions**] [**brief**]

Parameters

all-partitions

Displays firmware information for both the primary and the secondary partitions.

brief

Displays the installed SLX-OS versions.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display firmware version information and build dates. The default command output includes the following information:

- SLX-OS Version—The firmware version number
- Firmware name—The label of the firmware image
- Build Time—The build date and time of the firmware
- Install time—The date and time of the firmware installation
- Kernel—The Linux kernel version
- Control Processor—The control processor model and memory
- Microcode Version—The Intel CPU Microcode version installed
- Memory Size—The amount of memory available on the device
- System Uptime—The device uptime information

The command also displays the versions of the SLX-OS software installed in the primary and secondary partitions on the device.

Examples

The following example displays all firmware version information.

```
device# show version

SLX-OS Operating System Version: 20.6.2
Copyright (c) 1995-2024 Extreme Networks, Inc.
Firmware name:      20.6.2_240406_0800
Build Time:         15:18:41 Apr  6, 2024
Install Time:       08:30:57 Apr  8, 2024
Kernel:             4.14.67
```

```
Control Processor:  Intel(R) Atom(TM) CPU C3758 @ 2.20GHz,  8 cores
Microcode Version:  0x38
Memory Size:        System Total: 15631 MB
System Uptime:      12days 15hrs 21mins 44secs

Name     Primary/Secondary Versions
----------------------------------------
SLX-OS   20.6.2_240406_0800
         20.6.2_240406_0800
```

The following example displays a brief version of the firmware information.

```
device# show version brief

Name     Primary/Secondary Versions
----------------------------------------
SLX-OS   20.6.2_240406_0800
         20.6.2_240406_0800
```

show vlan brief

Displays basic information about the VLAN interfaces on the device. You can also filter to display only provisioned or unprovisioned VLANs.

Syntax

show vlan brief [**provisioned** | **unprovisioned**]

Parameters

provisioned

Displays provisioned VLANs.

unprovisioned

Displays unprovisioned VLANs.

Modes

Privileged EXEC mode

Output

The **show vlan brief** command displays the following information:

Output field	Description
VLAN	Displays the *vlan_ID*.
Name	Displays one of the following strings: • "default" • A name assigned to the VLAN using the **name** command • A default name automatically assigned to the VLAN, composed of "VLAN" and the *vlan_ID*. For example, if the *vlan_ID* is 1000, the default name is VLAN1000.
State	Displays "ACTIVE" for provisioned VLANs or "INACTIVE" for unprovisioned VLANs.
Config status	Displays the configuration status for the VLANs.
Ports	Displays the ports on which the VLAN is applied.
Classification	(Available only for provisioned).

Examples

The following example displays the status all VLANs, including MVRP VLANs.

```
device# show vlan brief
Total Number of VLANs configured    : 4
```

```
VLAN             Name            State      Config status         Ports
Classification
                                                                  (u)-Untagged
                                                                  (t)-Tagged
================ =============== ========== ===================== ===============
==============
1                default         ACTIVE     Static                Eth 1/5(t)
                                                                  Po 60(t)

10               VLAN0010        ACTIVE     Static                Eth 1/5(t)

100              VLAN0100        ACTIVE     Dynamic (MVRP)        Po 60(t)
```

show vlan detail

Displays detailed information on statically configured and dynamically created VLANs.

Syntax

show vlan detail

Modes

Privileged EXEC mode

Usage Guidelines

This command also displays endpoint tracking or MVRP status, including the configuration status of each Ethernet or port-channel interface, specifying whether the VLAN was added statically or learned dynamically.

Examples

```
device# show vlan detail
VLAN: 1, Name: default
Admin state: ACTIVE, Config status: Static
Number of interfaces: 7
      Eth 0/4, tagged, Static
      Eth 0/3, tagged, Static
      Eth 0/2, tagged, Static
      Eth 0/8, tagged, Static
      Eth 0/6, tagged, Static
      Eth 0/9, untagged, Static
      Po 20, tagged, Static
VLAN: 10, Name: VLAN0010
Admin state: ACTIVE, Config status: Static
Number of interfaces: 3
      Eth 0/3, tagged, Static
      Eth 0/2, tagged, Static
      Eth 0/4, tagged, Static
      Po 20, tagged, Static
VLAN: 11, Name: VLAN0011
Admin state: ACTIVE, Config status: Static
Number of interfaces: 3
      Eth 0/3, tagged, Static
      Eth 0/2, tagged, Static
      Eth 0/4, tagged, Dynamic (MVRP)
VLAN: 12, Name: VLAN0012
Admin state: ACTIVE, Config status: Dynamic (MVRP)
Number of interfaces: 1
      Eth 0/4, tagged, Dynamic (MVRP)
VLAN: 13, Name: VLAN0013
Admin state: ACTIVE, Config status: Dynamic (EP tracking)
Number of interfaces: 1
      Eth 0/6, tagged, Dynamic (EP tracking)
VLAN: 14, Name: VLAN0014
Admin state: INACTIVE(member port down), Config status: Static
Number of interfaces: 1
      Eth 0/8, tagged, Static
```

show vrf

Displays Virtual Routing and Forwarding (VRF) configuration information for the management VRF, the default VRF, or a user-defined VRF.

Syntax

show vrf { **mgmt-vrf** | **default-vrf** |*vrf-name* }[**detail** | **interface** *interface*]

Parameters

mgmt-vrf

Specifies the management VRF.

default-vrf

Specifies the default-vrf.

vrf-name

Specifies a named VRF.

detail

Displays detailed information for all VRFs configured.

interface *interface*

Displays VRF information for the specified interface.

Modes

Privileged EXEC mode

Examples

This example displays basic information for the default VRF.

```
device# show vrf default-vrf
VRF-Name: default-vrf, VRF-Id: 1
IP Router-Id: 50.50.50.1
Interfaces:
                Ve 40, Ve 84, Ve 85, Ve 150, Ve 211,
                Ve 501, Ve 503, Ve 504, Ve 505, Ve 1025,
                Ve 1059, Ve 2000, Lo 50
Address-family IPV4 unicast
                Max routes: -   Route count:134
   No import route-maps
   No export route-maps

Address-family IPV6 unicast
                Max routes: -   Route count:51
   No import route-maps
   No Export route-maps
```

This example displays basic information for all VRFs.

```
device# show vrf
Total number of VRFs configured: 4
VrfName                          VrfId  V4-Ucast  V6-Ucast
blue                             3      Enabled     -
default-vrf                      1      Enabled   Enabled
mgmt-vrf                         0      Enabled   Enabled
red                              2        -       Enabled
```

This example displays detailed information for all VRFs.

```
device# show vrf detail
Total number of VRFs configured: 4

VRF-Name: blue, VRF-Id: 3
IP Router-Id: 10.1.1.10
Interfaces:
    Ve 200
Address-family IPV4 unicast
    Max routes:-   Route count:134
   No import route-maps
   No export route-maps

VRF-Name: default-vrf, VRF-Id: 1
IP Router-Id: 30.1.1.1
Interfaces:
    Ve 300
Address-family IPV4 unicast
    Max routes:-   Route count:51
   No import route-maps
   No export route-maps

Address-family IPV6 unicast
    Max routes:-   Route count:2
   No import route-maps
   No Export route-maps

VRF-Name: mgmt-vrf, VRF-Id: 0
IP Router-Id: 0.0.0.0
Interfaces:
    mgmt 1, Null0
Address-family IPV4 unicast
    Max routes:-   Route count:3
   No import route-maps
   No export route-maps

Address-family IPV6 unicast
    Max routes:-   Route count:2
   No import route-maps
   No Export route-maps

VRF-Name: red, VRF-Id: 2
IP Router-Id: 0.0.0.0
Interfaces:
        Ve 100
Address-family IPV6 unicast
    Max routes:-   Route count:2
   No import route-maps
   No Export route-maps
```

This example indicates which VRFs are available on which interfaces.

```
device# show vrf interface
VrfName                          Interfaces
blue                             Ve 200
default-vrf                      Ve 300
mgmt-vrf                         mgmt 1, Null0
red                              Ve 100
```

This example displays name of length upto 64 characters for all VRFs.

```
device# show vrf
  <WORD:1-64>   Name of VRF: mgmt-vrf, default-vrf(default), <user VRF>
  detail        detail
  interface     interface
  |             Output modifiers
  <cr>
```

show vrrp

Displays information about IPv4 VRRP and VRRP-E sessions.

Syntax

show vrrp

show vrrp *VRID* [**detail** | **summary**]

show vrrp detail

show vrrp interface { **ethernet** *slot*/*port* | **port-channel** *number* | **ve** *vlan_id* } [**detail** | **summary**]

show vrrp summary [**vrf** { *vrf-name* | **all** }]

Parameters

VRID

The virtual group ID about which to display information. The range is from 1 through 16.

detail

Displays all session information in detail, including session statistics.

summary

Displays session-information summaries.

interface

Displays information for an interface that you specify.

ethernet *slot port*

Specifies a valid, physical Ethernet interface with a slot and port number.

port-channel *number*

Specifies a port-channel interface number.

ve *vlan_id*

Specifies the VE VLAN number.

vrf

Specifies a VRF instance or all VRFs.

vrf-name

Specifies a VRF instance. For the default vrf, enter **default-vrf**.

all

Specifies all VRFs.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to display information about VRRP and VRRP-E sessions, either in summary or full-detail format. You can also specify a particular virtual group ID or interface for which to display output.

This command is for VRRP and VRRP-E. VRRP-E supports only the VE interface type.

To display information for VRRP sessions using the default VRF, you can use the **show vrrp summary** command syntax (with no additional parameters).

For the default or a named VRF, you can use the **show vrrp summary vrf** command syntax with the *vrf-name* option.

To display information for all VRFs, use the **show vrrp summary vrf all** command.

Examples

The following example shows all VRRP session information in detail, including session statistics.

```
device# show vrrp detail

Total number of VRRP session(s)   : 2

VRID 14
  Interface: Ve 2018;  Ifindex: 1207961570
  Mode: VRRP
  Admin Status: Enabled
  Description :
  Address family: IPv4
  Version: 2
  Authentication type: No Authentication
  State: Master
  Session Master IP Address: Local
  Virtual IP(s): 10.18.1.100
  Virtual MAC Address: 0000.5e00.0112
  Configured Priority: unset (default: 100); Current Priority: 100
  Advertisement interval: 1 sec  (default: 1 sec)
  Preempt mode: ENABLE  (default: ENABLE)
  Hold time: 0 sec  (default: 0 sec)
  Master Down interval: 4 sec
  Trackport:
    Port(s)                   Priority  Port Status
    =======                   ========  ===========

  Global Statistics:
  ==================
    Checksum Error : 0
    Version Error  : 0
    VRID Invalid   : 0

  Session Statistics:
  ===================
    Advertisements             : Rx: 0, Tx: 49
    Gratuitous ARP             : Tx: 1
    Session becoming master    : 1
    Advts with wrong interval  : 0
    Prio Zero pkts             : Rx: 0, Tx: 0
    Invalid Pkts Rvcd          : 0
```

```
    Bad Virtual-IP Pkts        : 0
    Invalid Authenticaton type : 0
    Invalid TTL Value          : 0
    Invalid Packet Length      : 0

VRID 15
  Interface: Ve 2019;  Ifindex: 1207961571
  Mode: VRRP
  Admin Status: Enabled
  Description :
  Address family: IPv4
  Version: 2
  Authentication type: No Authentication
  State: Master
  Session Master IP Address: Local
  Virtual IP(s): 10.19.1.100
  Virtual MAC Address: 0000.5e00.0113
  Configured Priority: unset (default: 100); Current Priority: 100
  Advertisement interval: 1 sec  (default: 1 sec)
  Preempt mode: ENABLE  (default: ENABLE)
  Hold time: 0 sec  (default: 0 sec)
  Master Down interval: 4 sec
  Trackport:
    Port(s)                    Priority  Port Status
    =======                    ========  ===========

  Global Statistics:
  ==================
    Checksum Error : 0
    Version Error  : 0
    VRID Invalid   : 0

  Session Statistics:
  ===================
    Advertisements             : Rx: 0, Tx: 81
    Gratuitous ARP             : Tx: 1
    Session becoming master    : 1
    Advts with wrong interval  : 0
    Prio Zero pkts             : Rx: 0, Tx: 0
    Invalid Pkts Rvcd          : 0
    Bad Virtual-IP Pkts        : 0
    Invalid Authenticaton type : 0
    Invalid TTL Value          : 0
    Invalid Packet Length      : 0
```

The following example displays summary information for VRRP statistics on the VRF named Marketing.

```
device# show vrrp summary vrf Marketing

Total number of VRRP session(s)   : 1
Master session count  : 1
Backup session count  : 0
Init session count    : 0

VRID  Session  Interface  Admin   Current   State    Short-path  Revert    SPF
                          State   Priority           Forwarding  Priority  Reverted
====  =======  =========  =====   ========  =====    ==========  ========  ========
14    VRRP     Ve 2018    Enabled   100     Master
```

The following example displays summary information for VRRP statistics on all VRFs.

```
device# show vrrp summary vrf all
```

```
Total number of VRRP session(s)   : 2
Master session count  : 2
Backup session count  : 0
Init session count    : 0

VRID  Session  Interface   Admin   Current   State    Short-path  Revert    SPF
                           State   Priority           Forwarding  Priority  Reverted
====  =======  =========   =====   ========  =====    ==========  ========  ========
14    VRRP     Ve 2018     Enabled 100       Master
15    VRRP     Ve 2019     Enabled 100       Master
```

The following example displays summary information for VRRP statistics on the default VRF. (This command is equivalent to **show vrrp summary**.)

```
device# show vrrp summary vrf default-vrf

Total number of VRRP session(s)   : 1
Master session count  : 1
Backup session count  : 0
Init session count    : 0

VRID  Session  Interface  Admin   Current   State    Short-path  Revert    SPF
                          State   Priority           Forwarding  Priority  Reverted
====  =======  =========  =====   ========  =====    ==========  ========  ========
15    VRRP     Ve 2019    Enabled 100       Master
```

The following example displays information for VRRP-E tracked networks.

```
device# show vrrp detail

Total number of VRRP session(s)   : 1

VRID 3
  Interface: Ve 100;  Ifindex: 1207959652
  Mode: VRRPE
  Admin Status: Enabled
  Description :
  Address family: IPv4
  Version: 2
  Authentication type: No Authentication
  State: Master
  Session Master IP Address: Local
  Virtual IP(s): 10.1.1.100
  Virtual MAC Address: 02e0.523d.750a
  Configured Priority: unset (default: 100); Current Priority: 100
  Advertisement interval: 1 sec  (default: 1 sec)
  Preempt mode: DISABLE  (default: DISABLED)
  Advertise-backup: DISABLE  (default: DISABLED)
  Backup Advertisement interval: 60 sec  (default: 60 sec)
  Short-path-forwarding: Disabled
  Revert-Priority: unset; SPF Reverted: No
  Hold time: 0 sec  (default: 0 sec)
  Master Down interval: 4 sec
  Trackport:
    Port(s)                   Priority  Port Status
    =======                   ========  ===========

  Tracknetwork:
    Network(s)                Priority  Status
    =========                 ========  ==========
    10.20.1.0/24              50        Up

  Global Statistics:
  ==================
```

```
    Checksum Error : 0
    Version Error  : 0
    VRID Invalid   : 0

  Session Statistics:
  ===================
    Advertisements              : Rx: 0, Tx: 35
    Neighbor Advertisements           : Tx: 19
    Session becoming master     : 1
    Advts with wrong interval   : 0
    Prio Zero pkts              : Rx: 0, Tx: 0
    Invalid Pkts Rvcd           : 0
    Bad Virtual-IP Pkts         : 0
    Invalid Authenticaton type  : 0
    Invalid TTL Value           : 0
    Invalid Packet Length       : 0
    VRRPE backup advt sent      : 0
    VRRPE backup advt recvd     : 0
```

show ztp status

Shows the status of Zero Touch Provisioning.

Syntax

show ztp status

Modes

Privileged EXEC mode

Usage Guidelines

This command displays the status of Zero Touch Provisioning (ZTP) on the device. When an attribute is unavailable or not applicable, the status is "None."

The ZTP History attribute shows the last 10 ZTP processes. However, if you run the **fullinstall firmware download** command, the ZTP history is deleted and the ZTP History Countvalue attribute is reset.

Examples

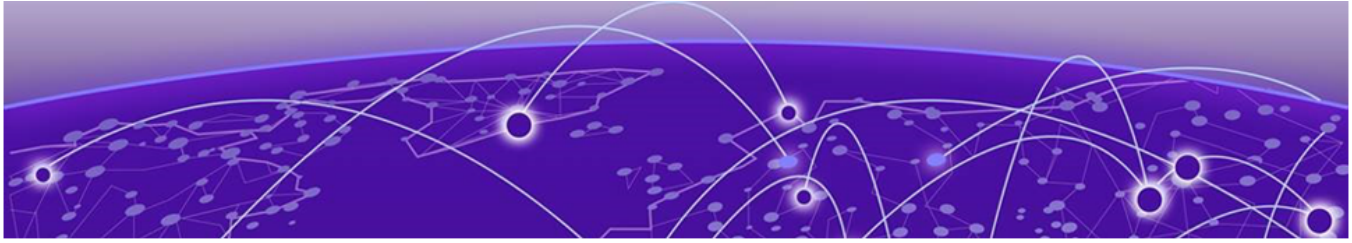
The following example shows output when the ZTP process is running.

```
device# show ztp status

ZTP Status                    :IN-PROGRESS
ZTP Interface up              :eth0
IP Address Assigned           :10.x.x.x
ftp Server IP Address         :10.x.x.x
Transfer Mode                 :ftp
ZTP Configuration File        :ztp.conf
clientid                      :EXTREMENETWORKS##SLX9150-48XT##XXXXXXXXXX
Switch Configuration File     :snowball_vlan.cfg , rootenable.py
Firmware Directory            :[/fw/slxos20.1.1_bld16/]
firmware download state       :start
firmware fullinstall          :no]
ZTP Description msg           :fwdl start

ZTP History
...
ZTP history countvalue:1
**1)
ZTP firmware upgrade...
ZTP fwdir [..x.x,anonymous,/fw/slxos20.1.1_bldxx/,a] proto [ftp]
```

The following example shows status when the ZTP process is not running and there is no history.

```
device# show ztp status

ZTP Status                    :None
ZTP Interface up              :None
IP Address Assigned           :None
ftp Server IP Address         :None
```

```
Transfer Mode                 :None
ZTP Configuration File        :None
clientid                      :None
Switch Configuration File     :None
Firmware Directory            :None
firmware download state       :None
firmware fullinstall          :None
ZTP Description msg           :No status available
ZTP History              :No history available
```



Commands Shu - Z

shortcuts ospf on page 2427
shutdown on page 2428
shutdown (link-oam) on page 2430
shutdown (STP) on page 2431
shutdown-time on page 2432
shutdown (cluster) on page 2433
shutdown (interface) on page 2434
shutdown (LIF) on page 2435
shutdown-time on page 2436
shutdown-time on page 2437
site on page 2438
snmp trap link-status disable on page 2440
snmp-server community on page 2443
snmp-server contact on page 2444
snmp-server context on page 2445
snmp-server enable trap on page 2447
snmp-server engineid local on page 2448
snmp-server group on page 2450
snmp-server host on page 2452
snmp-server location on page 2455
snmp-server mib community-map on page 2456
snmp-server preserve-statistics disable on page 2458
snmp-server sys-descr on page 2459
snmp-server trap on page 2460
snmp-server use-vrf on page 2461
snmp-server user on page 2463
snmp-server v3host on page 2466
snmp-server view on page 2468
soft-preemption on page 2470
soft-preemption cleanup-timer on page 2471
source on page 2472
source (monitor session) on page 2474
source-interface (LDAP) on page 2479
source-interface (RADIUS) on page 2481

spanning-tree autoedge on page 2483
spanning-tree bpdu-mac on page 2484
spanning-tree cost on page 2485
spanning-tree edgeport on page 2486
spanning-tree guard root on page 2488
spanning-tree link-type on page 2489
spanning-tree portfast on page 2490
spanning-tree priority on page 2492
spanning-tree restricted-role on page 2493
spanning-tree restricted-tcn on page 2494
spanning-tree shutdown on page 2495
speed (Ethernet) on page 2496
spf-interval on page 2498
spt-threshold infinity on page 2500
ssh on page 2501
ssh client cipher on page 2504
ssh client cipher non-cbc on page 2505
ssh client key-exchange on page 2506
ssh client mac on page 2507
ssh server algorithm on page 2508
ssh server certificate on page 2509
ssh server cipher on page 2510
ssh server key on page 2511
ssh server key-exchange on page 2513
ssh server mac on page 2514
ssh server max-auth-tries on page 2515
ssh server max-idle-timeout on page 2516
ssh server max-login-timeout on page 2517
ssh server rekey-interval on page 2518
ssh server rekey-volume on page 2519
ssh server use-vrf shutdown on page 2520
ssl-profile on page 2521
ssm-enable on page 2522
start (CFM) on page 2524
start (Y1731) on page 2525
start-shell on page 2526
static-network on page 2528
statistics on page 2529
statistics (bridge domain) on page 2530
statistics (VLAN) on page 2531
stop (CFM) on page 2532
stop (Y1731) on page 2534

storm-control ingress (global) on page 2535
storm-control ingress (interface) on page 2537
subnet on page 2539
sub-ring on page 2540
summary-address (IS-IS) on page 2541
summary-address (OSPFv2) on page 2543
summary-address (OSPFv3) on page 2545
summary-prefix on page 2547
support autoupload-param on page 2549
suppress-arp on page 2550
suppress-nd on page 2551
switch-attributes on page 2552
switchport on page 2553
switchport access on page 2554
switchport mode on page 2555
switchport mode trunk-no-default-native on page 2556
switchport port-security on page 2558
switchport port-security mac-address on page 2559
switchport port-security max on page 2560
switchport port-security shutdown-time on page 2561
switchport port-security sticky on page 2562
switchport port-security violation on page 2564
switchport trunk allowed on page 2565
switchport trunk native-vlan-untagged on page 2566
switchport trunk native-vlan-xtagged on page 2567
switchport trunk tag native-vlan on page 2569
sync-interval on page 2570
sysmon fe-acces-check on page 2572
sysmon link-crc-monitoring on page 2574
sysmon sfm-walk on page 2575
system maintenance on page 2577
system maintenance turn-off on page 2579
system-description on page 2580
system-monitor tm on page 2581
system-monitor-mail on page 2582
system-monitoring power alert state removed action raslog on page 2584
system power-cycle-db-shutdown on page 2585
system-name on page 2586
table-map on page 2587
tacacs-server on page 2589
tag-type on page 2592
tdpa on page 2594

telemetry client-cert on page 2596
telemetry collector on page 2597
telemetry profile on page 2598
telemetry profile (MPLS) on page 2602
telemetry server on page 2604
telnet on page 2605
telnet server on page 2607
terminal on page 2608
test-profile on page 2610
threshold on page 2611
threshold (ETH-DM) on page 2613
threshold (ETH-SLM) on page 2614
threshold-monitor on page 2616
threshold-monitor acl on page 2618
threshold-monitor Cpu on page 2621
threshold-monitor memory on page 2623
threshold-monitor bfd-sessions on page 2625
threshold-monitor ecmp on page 2627
threshold-monitor hardware-resources on page 2629
threshold-monitor host on page 2631
threshold-monitor lif on page 2633
threshold-monitor mac-table on page 2635
threshold-monitor nexthop on page 2637
threshold-monitor route on page 2639
threshold-monitor sfp on page 2641
threshold-monitor vxlan-tunnel on page 2645
threshold-timer (management-heartbeat) on page 2647
tie-breaking on page 2648
timeout (link-oam) on page 2650
timeout (RADIUS) on page 2651
timeout (Y1731) on page 2652
timer on page 2653
timers (BGP) on page 2655
timers (OSPFv2) on page 2657
timers (OSPFv3) on page 2659
tls min-version on page 2661
tlv-type on page 2663
to on page 2664
topology-group on page 2665
tpvm on page 2666
tpvm config dns on page 2670
tpvm config hostname on page 2671

tpvm config ldap on page 2672
tpvm config ldap ca-cert on page 2675
tpvm config ntp on page 2677
tpvm config timezone on page 2678
tpvm config trusted-peer on page 2679
tpvm deploy on page 2682
tpvm download on page 2685
tpvm fileinfo on page 2687
tpvm (mode) on page 2688
ldap host on page 2689
ldap ca-cert on page 2692
ntp (tpvm mode) on page 2694
tpvm dns on page 2695
hostname (tpvm mode) on page 2697
timezone (tpvm mode) on page 2698
trusted-peer (tpvm mode) on page 2699
auto-boot (tpvm mode) on page 2702
disk (tpvm mode) on page 2703
password (tpvm mode) on page 2705
allow-pwless (tpvm mode) on page 2706
interface management (tpvm mode) on page 2707
interface insight (tpvm mode) on page 2709
deploy (tpvm mode) on page 2710
tpvm upgrade on page 2713
tpvm snapshot on page 2716
traceroute on page 2717
track (VRRP) on page 2719
traffic-engineering (LSP) on page 2721
traffic-engineering (MPLS) on page 2724
transit-session-accounting on page 2726
transport on page 2727
trigger on page 2728
trigger-function on page 2730
trigger-mode on page 2732
trustpoint sign on page 2734
ttl on page 2735
tunable-optics on page 2736
tunneled-arp-trap enable on page 2741
tx-frame-count on page 2742
tx-interval on page 2743
tx-label-silence-timer on page 2744
type on page 2745

shortcuts ospf

Syntax

shortcuts ospf [**ignore-lsp-metric**]

no shortcuts ospf

Parameters

ignore-lsp-metrics

Ignores Label Switched Path (LSP) metrics.

Modes

MPLS LSP Configuration mode

Examples

This example shows how to enable OSPF Shortcuts within the LSP context. It also enables ignoring the configured LSP metrics.

```
SLX(config-router-mpls)# lsp test-lsp
SLX(config-router-mpls-lsp-test-lsp)# shortcuts ospf ignore-lsp-metric
```

shutdown

Physically disable out-of-band access to the BMC Management Interfaces. This prevents access to the interface from outside. Only BMC Management Interface 0 is supported.

Syntax

shutdown

no shutdown

Parameters

None

Modes

BMC Interface Configuration Mode

Usage Guidelines

The **no** format of this command enables this interface to be accessed from out-of-band ports.

Examples

This example shuts down the existing BMC Management Interface with ID 0.

```
SLX # configure terminal
SLX (config)# bmc
SLX (config-bmc)# interface management 0
SLX (config-bmc-mgmt-0)# do show running-config bmc
bmc
 user-id 1
  password $9$VaXhc9WCy+1IwRU2ZaS2vQ==
 !
 user-id 2
  password $9$VaXhc9WCy+1IwRU2ZaS2vQ==
 !
 user-id 3
 !
 interface management 0
  no shutdown
 !
!
SLX (config-bmc-mgmt-0)# shutdown
SLX (config-bmc-mgmt-0)# do show running-config bmc
bmc
 user-id 1
  password $9$VaXhc9WCy+1IwRU2ZaS2vQ==
 !
 user-id 2
  password $9$VaXhc9WCy+1IwRU2ZaS2vQ==
 !
 user-id 3
```

```
 !
 interface management 0
  shutdown
 !
!
```

This example enables the BMC Management Interface to be accessible from out-of-band.

```
SLX # configure terminal
SLX (config)# bmc
SLX (config-bmc)# interface management 0
SLX (config-bmc-mgmt-0)# no shutdown
SLX (config-bmc-mgmt-0)# do show running-config bmc
bmc
 user-id 1
  password $9$VaXhc9WCy+1IwRU2ZaS2vQ==
 !
 user-id 2
  password $9$VaXhc9WCy+1IwRU2ZaS2vQ==
 !
 user-id 3
 !
 interface management 0
  no shutdown
 !
!
SLX (config-bmc-mgmt-0)# exit
SLX (config-bmc)#
```

shutdown (link-oam)

Allows you to enable or disable the link-oam protocol.

Syntax

shutdown

no shutdown

Command Default

This command is executed on the local switch.

Modes

Link OAM configuration mode

Usage Guidelines

By default, link oam protocol is enabled when protocol link-oam is configured. Using this command, the protocol can be disabled or enabled.

Examples

```
device(config-link-oam)# shutdown
```

shutdown (STP)

Disables Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), Per-VLAN Spanning Tree+ (PVST+), or Rapid PVST+ (R-PVST+) globally.

Syntax

shutdown

no shutdown

Command Default

STP is not enabled as it is not required in a loop-free topology.

Modes

Any of the supported spanning tree configuration modes (STP, RSTP, MSTP, PVST+, R-PVST+)

Usage Guidelines

Enter **no shutdown** to re-enable any of the supported versions of STP.

Examples

To disable RSTP globally:

```
device# configure terminal
device(config)# protocol spanning-tree rstp
device(conf-rstp)# shutdown
```

To enable MSTP globally:

```
device# configure terminal
device(config)# protocol spanning-tree mstp
device(conf-mstp)# no shutdown
```

shutdown-time

Specifies a shutdown time for loopback detection (LD).

Syntax

shutdown-time *minutes*

no shutdown-time

Command Default

The default is 0.

Parameters

minutes

Shutdown time in minutes. Range is from 0 through 1440.

Modes

Protocol Loop Detection configuration mode

Usage Guidelines

By default the shutdown time is 0, which means that an LD-disabled logical interface (LIF) is never auto-enabled.

If the shutdown time is configured with a nonzero value, the LD-disabled LIF is auto-enabled following the specified shutdown time.

Use the no form of this command to revert to the default interval.

Examples

This example specifies a shutdown time of 20 minutes.

```
device# configure terminal
device(config)# loop-detection
device(config-loop-detect)# shutdown-time 1
2017/10/20-16:04:48, [ELD-1005], 3749, M2 | Active | DCE, INFO, SLX, Loop is detected on Ethernet 2/2
VLAN 20, the LIF (logical interface) is shutdown.
2017/10/20-16:05:46, [ELD-1007], 3750, M2 | Active | DCE, INFO, SLX, Loop detection disabled LIF
(Logical interface) on Ethernet 2/2 VLAN 20 is auto-enabled.
```

This example reverts to the default interval.

```
device# configure terminal
device(config)# loop-detection
device(config-loop-detect)# no shutdown-time
```

shutdown (cluster)

Isolates the MCT node by shutting down all components.

Syntax

shutdown { *all* | *clients* }

no shutdown { *all* | *clients* }

Command Default

The MCT node is disabled.

Modes

Cluster configuration mode

Parameters

all

Shuts down all client interfaces, VxLAN and L2VPN tunnels, and the peer-interface. Any CCP and keepalive sessions are brought down as well.

all

Shuts down all client interfaces, VxLAN and L2VPN tunnels, and the peer-interface. Any CCP and keepalive sessions are brought down as well.

client

Shuts down all client interfaces while keeping the peer-interface up.

Usage Guidelines

Enter **no shutdown** to enable the peers/clients.

Examples

To shutdown all access to an MCT:

```
device# configure terminal
device(config)# cluster MCT1
device(config-cluster-MCT1)# shutdown all
```

To redirect all traffic to the peer node:

```
device# configure terminal
device(config)# cluster MCT1
device(config-cluster-MCT1)# shutdown clients
```

shutdown (interface)

Disables the current interface.

Syntax

shutdown

no shutdown

Command Default

The interface is disabled.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no shutdown** to enable the interface.

If you use in-band management only, you may choose to shut down the management interface (which is considered out of band). When the management interface is shut down, all services (such as ping, scp, telnet, ssh, snmp, firmwaredownload, and supportsave) through the management interface IP. Management interface shutdown is a persistent configuration, meaning that the interface remains down after a system reboot or failover.

Examples

To disable a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# shutdown
```

To enable a specific Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# no shutdown
```

shutdown (LIF)

Removes a physical or port-channel interface on an edge port from participating in logical interface (LIF) data traffic without the need to shut down the interface.

Syntax

shutdown

no shutdown

Command Default

The LIF service instance is not shut down.

Modes

LIF configuration mode on a physical port or port-channel

Usage Guidelines

Use the **no** form of this command to restore the service instance status to the default.

Examples

The following example removes a service instance on an Ethernet port from participating in data traffic.

```
device(config)# interface ethernet 2/6
device(conf-if-eth-2/6)# logical-interface ethernet 2/6.120
device(conf-if-eth-lif-2/6.120)# shutdown
```

shutdown-time

Specifies a shutdown time for loopback detection (LD).

Syntax

shutdown-time *minutes*

no shutdown-time

Command Default

The default is 0.

Parameters

minutes

Shutdown time in minutes. Range is from 0 through 1440.

Modes

Protocol Loop Detection configuration mode

Usage Guidelines

By default the shutdown time is 0, which means that an LD-disabled logical interface (LIF) is never auto-enabled.

If the shutdown time is configured with a nonzero value, the LD-disabled LIF is auto-enabled following the specified shutdown time.

Use the no form of this command to revert to the default interval.

Examples

This example specifies a shutdown time of 20 minutes.

```
device# configure terminal
device(config)# loop-detection
device(config-loop-detect)# shutdown-time 1
2017/10/20-16:04:48, [ELD-1005], 3749, M2 | Active | DCE, INFO, SLX, Loop is detected on Ethernet 2/2
VLAN 20, the LIF (logical interface) is shutdown.
2017/10/20-16:05:46, [ELD-1007], 3750, M2 | Active | DCE, INFO, SLX, Loop detection disabled LIF
(Logical interface) on Ethernet 2/2 VLAN 20 is auto-enabled.
```

This example reverts to the default interval.

```
device# configure terminal
device(config)# loop-detection
device(config-loop-detect)# no shutdown-time
```

shutdown-time

Specifies a shutdown time to ensure convergence when maintenance mode is enabled on a SLX-OS device.

Syntax

shutdown-time *seconds*

no shutdown-time

Command Default

The default is 60 seconds.

Parameters

seconds

Shutdown time in seconds. Range is from 30 through 500.

Modes

System Maintenance mode

Usage Guidelines

Use the no form of this command to revert the shutdown time to the default interval of 60 seconds.

Examples

This example configures the shutdown time to 100 seconds.

```
SLX # configure terminal
SLX (config) # system maintenance
SLX (config-system-maintenance) # shutdown-time 100
SLX (config-system-maintenance) # exit
```

This example resets the shutdown time to the default value of 60 seconds.

```
SLX # configure terminal
SLX (config) # system maintenance
SLX (config-system-maintenance) # no shutdown-time
SLX (config-system-maintenance) # exit
```

site

Creates a remote Layer 2 extension site in a VXLAN overlay gateway context and accesses site configuration mode.

Syntax

site *name*

no site *name*

Parameters

name

Site identifier. An ASCII character string up to 63 characters long, including the alphabet, numbers 0 through 9, hyphens (-), and underscores (_).

Modes

Overlay gateway configuration mode

Usage Guidelines

The VXLAN overlay gateway type must first be configured for Layer 2 extension, by means of the **type layer2-extension** command.

A site represents a remote fabric or the other end of the VXLAN tunnel. A site is associated with a "container," as data structure that includes the destination IPv4 address of the tunnel, the switchport VLANs, bridge domain, and the administrative state.

Use the **no site** command with a specified name to remove the tunnel that corresponds to the site.One you create the site instance, you enter VXLAN overlay

gateway site configuration mode, where you can configure other properties for the site. The key commands available in this mode are summarized below:

Table 21: Key commands available in VXLAN overlay gateway site configuration mode

Command	Description
bfd	Configures Bidirectional Forwarding Detection (BFD) on a tunnel in VXLAN overlay gateway configurations.
bfd interval	Configures BFD session parameters on a tunnel in VXLAN overlay gateway configurations.
extend bridge-domain	Configures a bridge domain for the tunnels to the containing site in a VXLAN overlay gateway configurations.
extend vlan	Configures switchport VLANs for the tunnels to the containing site in a VXLAN overlay gateway configurations.
ip address	Specifies the IPv4 address of a destination tunnel in VXLAN overlay gateway configurations.
shutdown	Administratively shuts down tunnels to a VXLAN overlay gateway site.

Examples

The following example creates a VXLAN overlay gateway site and enters site configuration mode.

```
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# site mysite
switch(config-site-mysite)#
```

snmp trap link-status disable

Disables SNMP traps for the interface link status change.

Syntax

snmp trap link-status disable { **ethernet***slot/port* | **loopback** *port* | **port-channel** *channel* | **ve** *vlan-id* }

no snmp trap link-status disable { **ethernet***slot/port* | **loopback** *port* | **port-channel** *channel* | **ve** *vlan-id* }

By default, the SNMP trap for link-status is enabled for all interfaces.

Parameters

ethernet *slot/port*

Specifies a physical Ethernet interface and a valid slot and port number.

loopback *port*

Specifies a loopback interface and a valid port number.

port-channel *channel*

Specifies a port-channel.

ve *vlan-id*

Specifies a virtual interface.

Modes

Interface sub-mode

Usage Guidelines

Use the **no** form of this command to enable SNMP traps for the interface link-status change. Use the **show running-config interface** command to view the SNMP traps link-status. SNMP traps are disabled for "Ethernet 0/1" and Ethernet 0/2" and by default enabled for "Ethernet 0/3" and "Ethernet 0/4". SNMP traps are disabled for Port-channel 21 and 22 and by default enabled for Port-channel 23. SNMP traps are disabled for Loopback 11 and 12 and by default enabled for loopback 13. SNMP traps are disabled for VE 1 and 2 and by default enabled for VE 3.

Examples

The following example displays the SNMP traps are disabled for "Ethernet 0/1" and Ethernet 0/2". Enabled by default for "Ethernet 0/3" and "Ethernet 0/4" :

```
device# show running-config interface Ethernet
interface Ethernet 0/1
snmp trap link-status disable
shutdown
```

```
!

interface Ethernet 0/2
snmp trap link-status disable
shutdown
!

interface Ethernet 0/3
shutdown
!

interface Ethernet 0/4
shutdown
!
```

The following example displays the SNMP traps are disabled for Port-channel 21 and 22. Enabled by default for Port-channel 23:

```
device# show running-config interface Port-channel

interface Port-channel 21
snmp trap link-status disable
shutdown
!

interface Port-channel 22
snmp trap link-status disable
shutdown
!

interface Port-channel 23
shutdown
!
```

The following example displays the SNMP traps are disabled for Loopback 11 and 12. Enabled by default for loopback 13:

```
device# show running-config interface Loopback
interface Loopback 11
snmp trap link-status disable
shutdown
!

interface Loopback 12
snmp trap link-status disable
shutdown
!

interface Loopback 13
shutdown
!
```

The following example displays the SNMP traps are disabled for VE 1 and 2. Enabled by default for VE 3:

```
device# show running-config interface ve
interface Ve 1
snmp trap link-status disable
shutdown
!

interface Ve 2
snmp trap link-status disable
```

```
shutdown
!

interface Ve 3
shutdown
!
```

snmp-server community

Sets the community string and associates it with the user-defined group name to restrict the access of MIB for SNMPv1 and SNMPv2c requests.

Syntax

snmp-server community *string* [**group** *group-name*]

no snmp-server community *string* [**group** *group-name*]

Command Default

None

Parameters

string

Specifies the community name string. Enter an alphanumeric string with 2 to 16 characters.

group *group-name*

Specifies the group name associated with the community name.

Modes

Global configuration mode

Usage Guidelines

Use a **no** form of this command to remove an community string or the group from the community.

The maximum number of SNMP communities supported is 256.

Examples

The following example adds the community string named public and associates the group name named user with it.

```
device(config)# snmp-server community public groupname user
```

snmp-server contact

Sets the SNMP server contact string.

Syntax

snmp-server contact *string*

no snmp-server contact

Command Default

The default contact string is "Operator 12345".

Parameters

string

Specifies the server contact. Enter an alphanumeric string from 4 to 255 characters. You must enclose the text in double quotes if the text contains spaces.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to reset the default value.

Examples

The following example sets the SNMP server contact string to "Operator 12345".

```
device(config)# snmp-server contact "Operator 12345"
```

snmp-server context

Maps the context name in an SNMPv3 packet protocol data unit (PDU) to the name of a VPN routing and forwarding (VRF) instance.

Syntax

snmp-server context *context_name* [**vrf-name** *vrf_name*]

no snmp-server context *context_name* [**vrf-name** *vrf_name*]

Command Default

None

Parameters

context_name

Specifies the context name that is passed in the SNMP PDU.

vrf-name *vrf_name*

Specifies the VRF instance that can be retrieved when an SNMP request is sent with the context name.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of the command to delete the SNMP server context.

For SNMPv1 and SNMPv2, you must map the context with the community string. The SNMP agent supports 256 contexts to support context-to-VRF mapping.

For SNMPv3, you only need to map the context with the VRF. The SNMPv3 request PDU itself provisions for the context. Only one context is allowed for each VRF instance.

Examples

The following example configures an SNMP server context to a VRF for SNMPv1 or SNMPv2.

```
device# configure terminal
device(config)# snmp-server community public groupname admin
device(config)# snmp-server context mycontext vrf myvrf
device(config)# snmp-server mib community-map public context mycontext
```

The following example configures an SNMP server context to a VRF for SNMPv3.

```
device# configure terminal
device(config)# snmp-server context mycontext1 vrf myvrf1
```

snmp-server enable trap

Enables the SNMP traps.

Syntax

snmp-server enable trap

no snmp-server enable trap

Command Default

The SNMP server traps are enabled by default.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to disable the SNMP traps.

Examples

The following example disables the SNMP traps.

```
device# configure terminal
device(config)# no snmp-server enable trap
```

The following example enables the SNMP traps.

```
device# configure terminal
device(config)# snmp-server enable trap
```

snmp-server engineid local

Configures an SNMP engine ID for the SNMP agent.

Syntax

snmp-server engineid local *engine_id*

no snmp-server engineid local

Command Default

A default engine ID is generated during system start up.

Modes

Global configuration mode

Usage Guidelines

SNMP agent Engine ID can be 12 or 13 bytes in hexadecimal format. Each byte must be separated by colons. When using a 12 byte engine ID, each byte must be entered as 2 char per octet. For example, the value *1* must be entered as *01*. However, for the 13 byte engine ID, each byte can be entered as 1 or 2 char per octet. For example, the value *1* can be entered as *1* or as *01*.

Note the following:

- The Default SNMP Engine ID is 13 bytes long.
- You can view the Default SNMP Engine ID using the **show running config** command. You can also fetch this SNMP Engine ID through Netconf query and **snmpget** commands.
- Manually configured SNMP Engine ID is reflected within the running configuration and immediately accessible with the netconf query. The manually configured SNMP Engine ID will only be available through **snmpget** command and in the traps only after a successful reboot.
- When you un-configure the Default SNMP Engine ID, the running configuration will still retain the Default SNMP Engine ID. However, when you un-configure a Manually configured SNMP Engine ID, the running configuration will show the Default SNMP Engine ID. This change will happen only after a successful reboot.
- When a device is reloaded with a default configuration, the running configuration will display the Default SNMP Engine ID.
- When a manually configured SNMP Engine ID is reset, a syslog is generated. For example,

```
2020/12/18-03:00:56, [SNMP-1005], 77,, INFO, SLX, SNMP configuration attribute,
LocalEngineId, has changed from [a1:b1:c1:d1:e1:a1:b1:c1:d2:a1:a1:b1] to
[80:0:6:34:b2:4:0:0:10:aa:9a:b7:96].
```

- A syslog is not generated when the Default SNMP Engine ID is reset.
- When a 12 byte SNMP Engine ID is configured in version 20.2.3 and the device is then downgraded to a lower firmware release, this SNMP Engine ID is retained in the lower release post downgrade.
- When a 13 byte SNMP Engine ID is configured in version 20.2.3 and the *full install* downgrade is performed, this 13 byte SNMP Engine ID will not be available after downgrade. However, you can view this 13 byte SNMP Engine ID immediately after a *coldboot* downgrade and will be lost on subsequent file replays, config rollback, or copy of startup configuration.
- When the Default SNMP Engine ID is reset using the **no snmp-server engineID local** command, a warning message is displayed. This warning message is, however, not displayed when it is reset using the REST/Netconf query.

```
SLX(config)# no snmp-server engineID local
80:0:6:34:b2:4:0:0:10:aa:9a:b7:96

%Warning: SNMP engine id is currently default. Removing default engine id would again
set it to default value%.
```

A reboot is necessary for the configured engine ID to become active.

Use the **no** form of the command to remove the configured engine ID from database.

Examples

The following example configures an engine ID for the SNMP agent.

```
device(config)# snmp-server engineid local 10:00:00:05:33:51:A8:65:05:33:51:A8
```

The following example removes the configured engine ID from the database.

```
device(config)# no snmp-server engineid local
```

snmp-server group

Creates user-defined groups for SNMPv1/v2/v3 and configures read, write, and notify permissions to access the MIB view.

Syntax

snmp-server group *groupname* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } }
[**read** *viewname*] [**write** *viewname*] [**notify** *viewname*]

no snmp-server group *groupname* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } }
[**read** *viewname*] [**write** *viewname*] [**notify** *viewname*]

Command Default

None

Parameters

groupname

Specifies the name of the SNMP group to be created.

v1 | **v2c** | **v3**

Specifies the version of SNMP.

auth | **noauth** | **priv**

Specifies the various security levels for SNMPv3.

auth

Specifies the authNoPriv security level. Password authentication is used based on either MD5 or SHA hash authentication and no encryption is used for communications between the devices.

noauth

Specifies the noAuthNoPriv security level. If no security level is specified, noauth is the default. This security level means that there is no authentication password exchanged and the communications between the agent and the server are not encrypted. The SNMP requests are authorized based on a username string match similar to the community string for SNMPv1/v2c.

priv

Specifies the authPriv security level. Password authentication is used based on either MD5 or SHA hash authentication and the communication between the agent and the server are also encrypted.

read *viewname*

Specifies the name of the view that enables you to provide read access.

write *viewname*

Specifies the name of the view that enables you to provide both read and write access.

notify *viewname*

Specifies the name of the view that enables you to provide access to the MIB for trap or inform.

Modes

Global configuration mode

Usage Guidelines

Maximum number of SNMP groups supported is 10.

SNMP SET is no longer allowed. Therefore, when configured, the write view will not take effect.

Examples

The following example creates SNMP server group entries for SNMPv3 user group with auth or noauth permission.

```
device(config)# snmp-server group group1 v3 auth read myview write myview notify myview
device(config)# snmp-server group group2 v3 noauth read all write all notify all
device(config)# snmp-server group group3 v3 auth
```

The following example removes the configured SNMP server groups.

```
device(config)# no snmp-server group test1 v3 auth
device(config)# no snmp-server group TEST1 v3 auth read myview write myview
device(config)# no snmp-server group TEST2 v3 noauth read all write all notify all
```

The following examples shows the message that is displayed when trying to use the *write* configuration on a group.

```
 SLX(config)# snmp-server group group2_test v2c read view_all write view_all notify
view_all
% Info: SNMP set operation is not supported. write view configured will not take effect.
```

snmp-server host

Configures the SNMP trap server host attributes.

Syntax

snmp-server host { **ipv4_host** | **ipv6_host** | **dns_host** } *community_string* [**version** { **1** | **2c** }] [**udp-port** *port*] [**severity-level** | { **none** | **debug** | **info** | **warning** | **error** | **critical** }] [**use-vrfvrf-name**] [**source-interface** { **loopback** | **management** { *chassis-ip* | *mgmt-ip* } | **ve**]

no snmp-server host { **ipv4_host** | **ipv6_host** | **dns_host** } *community_string* [**version** { **1** | **2c** }] [**udp-port** *port*] [**severity-level** | { **none** | **debug** | **info** | **warning** | **error** | **critical** }] [**use-vrf vrf-name**] [**source-interface** { **loopback** | **management** { *chassis-ip* | *mgmt-ip* } | **ve**]

Parameters

host { **ipv4_host** | **ipv6_host** | **dns_host** }

Specifies the IP address of the host. IPv4, IPv6, and DNS hosts are supported.

community_string

Specifies the community string associated with the host entry. The number of characters available for the string ranges from 1 through 64.

version { **1** | **2c** }

Selects version 1 or 2c traps to be sent to the specified trap host.

udp-port *port*

Specifies the UDP port where SNMP traps will be received. Valid port IDs range from 0 through 65535. The default port is 162.

severity-level { **none** | **debug** | **info** | **warning** | **error** | **critical** }

Provides the ability to filter traps based on severity level on both the host and the SNMPv3 host. Only RASLog (swEvent) traps can be filtered based on severity level. The configured severity level marks the reporting threshold. All messages with the configured severity or higher are displayed. If the severity level of **none** is specified, all traps are filtered and no RASLog traps are received.

use-vrf *vrf-name*

Specifies a VRF though which to communicate with the SNMP host. By default, all management services are enabled on the management VRF ("mgmt-vrf") and the default VRF ("default-vrf").

source-interface { **loopback** | **management** { *chassis-ip* | *mgmt-ip* } | **ve**

Specifies whether to use a loopback, management, or VE interface as a source address for notifications. For management, specifies the chassis or management IP address.

Modes

Global configuration mode

Usage Guidelines

This command sets the trap destination IP addresses and SNMP version, associates a community string with a trap host community string (for v1 and v2c), and specifies the UDP destination port where SNMP traps will be received.

To configure SNMP trap hosts associated with community strings, you must create the community string using the **snmp-server community** command before configuring the host.

The host supports six communities and their associated trap recipients and trap recipient severity levels. The default value for the trap recipient of each community is 0.0.0.0. The length of the community string should be between 2 and 64 characters.

The **no snmp-server host** *host community-string* **version 2c** command brings version 2c down to version 1.

The **no snmp-server host** *host community-string* command removes the SNMP server host from the device configuration altogether.

The **no** form of the command can be used to remove the following configuration for a given host: **version**, **udp-port**, **severity-level**, and **use-vrf**.

Examples

The following example creates an entry for trap host 1050:0:0:0:5:600:300c:326b associated with community “public.” The trap host receives traps from the configured device.

```
device(config)# snmp-server host 1050:0:0:0:5:600:300c:326b public severity-level Info
```

The following example creates an entry for trap host brcd.extremenetworks.com associated with community “public.” The trap host receives traps from the configured device.

```
device(config)# snmp-server host brcd1.extremenetworks.com public severity-level info
```

The following example associates “commaccess” as a read-only community and set 10.32.147.6 as a trap recipient with SNMP version 2c on target port 162.

```
device(config)# snmp-server host 10.32.147.6 commaccess version 2c udp-port 162
```

The following example creates a trap host (10.23.23.45) associated with the community “public”, which will receive all traps with the severity level of Info.

```
device(config)# snmp-server host 10.23.23.45 public severity-level info
```

The following example resets the severity level to None.

```
device(config)# snmp-server host 10.23.23.45 public severity-level None
```

The following example specifies a VRF to communicate with the host.

```
device(config)# snmp-server host 10.24.61.10 public use-vrf myvrf
```

The following example removes the SNMP host.

```
device(config)# no snmp-server host 10.24.61.10 public
```

The following example removes the udp-port configuration and resets the default to 162.

```
device(config)# no snmp-server host 10.24.61.10 public udp-port
```

snmp-server location

Sets the SNMP server location string.

Syntax

snmp-server location *string*

no snmp-server location

Command Default

The default location string is "Building 3 Room 214".

Parameters

location *string*

Specifies the SNMP server location string. Enter an alphanumeric string from 4 to 255 characters. You must enclose the text in double quotes if the text contains spaces.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to reset the default value.

Examples

The following example sets the SNMP server location string to "Building 3 Room 214".

```
device(config)# snmp-server location "Building 3 Room 214"
```

snmp-server mib community-map

Maps an SNMP community string to an SNMP context.

Syntax

snmp-server mib community-map *community-name* **context** *context-name*

no snmp-server mib community-map *community-name* **context** *context-name*

Command Default

None

Parameters

community-name

Specifies an SNMP community name.

context *context-name*

Specifies an SNMP context.

Modes

Global configuration mode

Usage Guidelines

Use the no form of this command to remove a community string and its associated context name.

Any incoming SNMPv1/v2c requests with the specified community name uses the context name specified by this command. The context name can be used in SNMP requests for "ipCidrRouteTable."One community can be mapped to only one context. However, a single context can be mapped to multiple communities.

Before mapping the community to context, a valid context should be configured by using the **snmp-server context** command and a valid community string should be configured by using the **snmp-server community** command.

Examples

The following example maps an SNMP community string to a context name.

```
device# configure terminal
device(config)# snmp-server mib community-map public context mycontext
```

The following example removes an SNMP community string and its associated context name.

```
device(config)# no snmp-server mib community-map public context mycontext
```

snmp-server preserve-statistics disable

Enables and disables the preservation of SNMP MIB statistics.

Syntax

snmp-server preserve-statistics disable

no snmp-server preserve-statistics disable

Command Default

SNMP MIB statistics are preserved by default.

Parameters

disable

Disables the preservation of SNMP MIB statistics.

Modes

Global configuration mode

Examples

This following example disables the preservation of statistics.

```
device(config)# snmp-server preserve-statistics disable
```

snmp-server sys-descr

Sets the Management Information Base (MIB-2) object identifier (OID) system description.

Syntax

snmp-server sys-descr *string*

no snmp-server sys-descr

Command Default

The system description varies with the device.

Parameters

string

The text for the system description. The string must be between 4 and 255 characters in length.

Modes

Global configuration mode

Usage Guidelines

Enter **no snmp-server sys-descr** to return to the default system description.

Examples

To set the system description OID to "Extreme Networks BR-SLX9640, use:

```
device(config)# snmp-server sys-descr "Extreme Networks BR-SLX9640"
```

To restore the system description OID to the default:

```
device(config)# no snmp-server sys-descr
```

snmp-server trap

Switches between standard and enterprise MIB to generate the BFD traps. When this CLI is configured, the BFD traps defined in standard MIB get generated.

Syntax

snmp-server trap bfd-std-mib

[no] snmp-server trap bfd-std-mib

Modes

Global configuration mode

Usage Guidelines

The `no` form of this command will reset to default behavior. i.e., the BFD traps defined in enterprise MIB get generated.

Examples

The following example provides an option to switch between standard and enterprise MIB.

```
SLX(config)# snmp-server trap ?
    Possible completions:
    bfd-std-mib Set standard MIB for BFD trap
    SLX(config)# snmp-server trap bfd-std-mib?
    Possible completions:
    <cr>

SLX(config)# show run snmp-server snmp-server
    sys-descr "Extreme SLX9540 Switch/Router"
    snmp-server engineID local 80:0:6:34:b2:9c:60:0:10:14:70:5a:9f
    snmp-server trap bfd-std-mib

    SLX(config)# no snmp-server trap bfd-std-mib ?
     Possible completions:
     <cr>
    SLX(config)# no snmp-server trap bfd-std-mib
```

snmp-server use-vrf

Configures SNMP Listening Service on a VRF. SNMP listening service over `mgmt-vrf` and `default-vrf` will be enabled by default. Also the Listening service *enable/disable* related CLI is applicable for SNMP Get related operations and it will not impact notification operations.

Syntax

snmp-server use-vrf *vrf-name* **shutdown**

no snmp-server use-vrf *vrf-name* **shutdown**

Parameters

use-vrf *vrf-name*

Specifies a user-defined VRF or `default-vrf` or `mgmt-vrf`

shutdown

Disables the SNMP Listening Service on VRF.

Modes

Global configuration mode

Usage Guidelines

Use the **snmp-server** command with the **use-vrf** parameter to enable the SNMP Listening Service and associate it with the specified VRF. The **use-vrf** parameter configures the SNMP service for not only the specified user-defined VRF but also for `default-vrf` and `mgmt-vrf`. The service for that VRF is enabled or disabled with no effect on service for other VRFs.

Use the **snmp-server** command with the **use-vrf** and **shutdown** parameters to disable SNMP Listening Service for the specified VRF.

Use the **no snmp-server** command with the **use-vrf** parameter to disable the SNMP Listening Service and remove its association with the specified VRF. You can disable service for any VRF, including the management VRF. Disabling service for the management VRF is allowed, but removing the server's association with the management VRF is not allowed.

Examples

The following example creates and enables the SNMP Listening Service on a user-defined VRF or `default-vrf` .

```
device# configure terminal
SLX(config)# snmp-server use-vrf vrf-name
```

The following example disables the SNMP Listening Service on a user-defined VRF or `default-vrf` or `mgmt-vrf`.

```
device# configure terminal
device(config)# snmp-server use-vrf vrf-name shutdown
```

The following example enables the SNMP Listening Service on a user-defined VRF, or `default-vrf` or `mgmt-vrf`.

```
device# configure terminal
device(config)# no snmp-server use-vrf vrf-name shutdown
```

The following command will delete the SNMP service over the specified VRF.

```
device# configure terminal
SLX(config)# no snmp-server use-vrf vrf-name
```

snmp-server user

Creates or changes the attributes of SNMPv3 users, and allows the SNMPv3 user to be associated with the user-defined group name.

Syntax

snmp-server user *username* [**groupname** *group-name*] [**auth** { **md5** | **sha** | **noauth** }] [**auth-password** *string* [**encrypted**]] [**priv** { **DES** | **AES128** | **nopriv** }] [**priv-password** *string* [**encrypted**]

no snmp-server user *username*

Command Default

None

Parameters

username

The name of the user that connects to the agent. The name must be between 1 and 16 characters long.

groupname *group-name*

The name of the group to which the user is associated. The configured user is allowed to be associated with the user-defined groups created using the **snmp-server group** command.

auth

Initiates an authentication level setting session. The default level is **noauth** .

noauth

Specifies "No Authentication Protocol".

md5

The HMAC-MD5-96 authentication level.

sha

The HMAC-SHA-96 authentication level.

auth-password *string*

A string that enables the agent to receive packets from the host. Passwords are plain text and must be added each time for each configuration replay. The password must be between 1 and 32 characters long. If a password contains supported special characters (such as !, @, #, $, %), enclose the password in double quotes (").

priv

Initiates a privacy authentication level setting session. The default level is **nopriv** .

DES

Specifies the DES privacy protocol.

AES128

Specifies the AES128 privacy protocol.

nopriv

Specifies "No Privacy Protocol".

priv-password *string*

Specifies a string (not to exceed 32 characters) that enables the host to encrypt the contents of the message that it sends to the agent. Passwords are plain text and must be added each time for each configuration replay. The privacy password alone cannot be configured. You configure the privacy password with the authentication password. If a password contains supported special characters (such as, !, @, #, $, %), enclose the password in double quotes (").

encrypted

Encrypts the input for auth/priv passwords. The encrypted key should be used only while entering the encrypted auth/priv passwords.

Modes

Global configuration mode

Usage Guidelines

This command configures SNMPv3 users that can be associated with a trap and inform response functionality. This command also allows configured user to be associated with user-defined SNMP groups created using the **snmp-server group** command. The maximum number of SNMP users that can be configured is 10. Optional encryption for **auth-password** and **priv-password** is also provided.

When creating a new SNMPv3 user without group name, by default there is no group name mapped with the SNMPv3 user. You must map the configured SNMPv3 user with any non-existing or existing group name available in the group CLI configuration to contact the device through SNMPv3.

This command may not be successful where encrypted passwords are generated by third-party or open-source tools.

Use the **no** form of the command to remove an SNMP user.

It is recommended not to delete users without stopping the SNMP service. If SNMP service is running, and a user is deleted, then a device restart is required.

Examples

The following example configures a basic authentication policy.

```
device(config)# snmp-server user extreme groupname snmpadmin auth md5 auth-password
user123 priv AES128 priv-password user456
```

The following example configures plain-text passwords.

```
device(config)# snmp-server user snmpadmin1 auth md5 auth-password private123 priv  DES
priv-password public123
```

The following example configures configure encrypted passwords.

```
device(config)# snmp-server user snmpadmin2 groupname snmpadmin auth md5 auth-password
"MVb+360X3kcfBzug5Vo6dQ==\n" priv DES priv-password "ckJFoHbzVvhR0xFRPjsMTA==\n" encrypted
```

The following example creates the SNMP users "user1" and "user2" associated with used-defined group "group1" under global configuration mode.

```
device(config)# snmp-server user user1 groupname group1
device(config)# snmp-server user user2 groupname group1 auth md5 auth-password password
priv DES priv-password password
```

The following example deletes a SNMP user.

```
SLX(config)# no snmp-server user user3
% Info: SNMP user delete operation is recommended when SNMP agent is not running, else it
requires system reload to take effect.
```

snmp-server v3host

Specifies the host recipient for SNMPv3 trap notification.

Syntax

snmp-server v3host { **ipv4_host** | **ipv6_host** | **dns_host** } *user_name* [**notifytype** { **traps** | **informs** }] [**engineid** *engine-id*] [**udp-port** *port_number*] [**severity-level** | { **none** | **debug** | **info** | **warning** | **error** | **critical** }] [**use-vrf** { **vrf-name**}] [**source-interface** { **loopback** | **management** { *chassis-ip* | *mgmt-ip* } | **ve**]

no snmp-server v3host { **ipv4_host** | **ipv6_host** | **dns_host** } *user_name* [**notifytype** {**traps** | **informs**}] [**engineid** *engine-id*] [**udp-port** *port_number*] [**severity-level** | {**none** | **debug** | **info** | **warning** | **error** | **critical** }] [**use-vrf**] [**source-interface** { **loopback** | **management** { *chassis-ip* | *mgmt-ip* } | **ve**]

Parameters

ipv4_host | **ipv6_host** | **dns_host**

Specifies the IP address of the host. IPv4, IPv6, and DNS hosts are supported.

user_name

Specifies the SNMPv3 user name to be associated with the SNMPv3 host entry.

notifytype traps | **informs**

Specifies the type of notification traps that are sent for the host. Traps and informs are supported. The default notify type is traps.

engineID *engine-id*

Configures the remote engine ID to receive informs on a remote host.

udp-port *port_number*

Specifies the UDP port of the host. The default UDP port number is 162.

severity-level { **none** | **debug** | **info** | **warning** | **error** | **critical** }

Provides the ability to filter traps based on severity level on both the host and the SNMPv3 host. Only RASLog (swEvent) traps can be filtered based on severity level. The configured severity level marks the reporting threshold. All messages with the configured severity or higher are displayed. If the severity level of None is specified, all traps are filtered and no RASLog traps are received. The default severity level is none.

use-vrf *vrf-name*

Configures SNMP to use the specified VRF to communicate with the host. The default is mgmt-vrf.

source-interface { **loopback** | **management** { *chassis-ip* | *mgmt-ip* } | **ve**

Specifies whether to use a loopback, management, or VE interface as a source address for notifications. For management, specifies the chassis or management IP address.

Modes

Global configuration mode

Usage Guidelines

You can associate a global SNMPv3 host only with global SNMPv3 users and the local SNMPv3 host only with local SNMPv3 users. You cannot create a SNMPv3 host by associating with the local SNMPv3 users and vice versa.

The **no** form of the command can be used to remove the following entities: **notifytype**, **engineID**, **udp-port**, **severity-level**, and **use-vrf**.

Examples

The following example creates an entry for SNMPv3 trap IPv4 host 10.23.23.45 associated with SNMP user "snmpadmin1."

```
device(config)# snmp-server v3host 10.23.23.45 snmpadmin1 severity-level info
```

The following example creates an entry for SNMPv3 trap IPv6 host 1050:0:0:0:5:600:300c:326b associated with SNMP user "snmpadmin2." The trap host receives SNMPv3 traps from the configured device.

```
device(config)# snmp-server v3host 1050::5:600:300c:326b snmpadmin2 severity-level Info
```

The following example associates the default-vrf VRF for a trap host recipient.

```
device(config)# snmp-server v3host 10.24.61.10 public use-vrf default-vrf
```

The following example removes the SNMP v3 host.

```
device(config)# no snmp-server v3host 10.24.61.10 public
```

snmp-server view

Creates a view entry with MIB object IDs to be included or excluded for user access.

Syntax

snmp-server view *view-name mib_tree* {**included** | **excluded** }

no snmp-server view *view-name mib_tree* {**included** | **excluded** }

Command Default

No SNMP server views are defined.

Parameters

view-name

Specifies the alphanumeric name to identify the view. The name should not contain spaces.

mib_tree

Specifies the MIB object ID called Object Identifiers (OIDs) that represent the position of the object or sub-tree in the MIB hierarchy.

included | **excluded**

Specifies whether the specified MIB object ID must be included in the view or excluded from the view.

Modes

Global configuration mode

Usage Guidelines

The maximum number of views supported with MIB tree entries is 10. Either a single view name associated with 10 different MIB object IDs or 10 different view names associated with each one of the MIB object IDs is allowed.

Examples

The following example creates an SNMP view entry "view1" with excluded permission for the MIB object ID "1.3.6.1.2.1.1.3."

```
device(config)# snmp-server view view1 1.3.6.1.2.1.1.3 excluded
```

The following example creates an SNMP view entry "view2" with included permission for the MIB object ID "1.3.6.1."

```
device(config)# snmp-server view view2 1.3.6.1 included
```

The following example removes the SNMP view entry "view1" from the configuration list.

```
device(config)# no snmp-server view view1 1.3.6.1.2.1.1.3 excluded
```

soft-preemption

The **soft-preemption** command enables soft preemption functionality. This command must be used on both the primary and secondary paths.

Syntax

soft-preemption

no soft-preemption

Command Default

The soft-preemption function is disabled.

Modes

MPLS LSP configuration mode

Usage Guidelines

The **no** function disables soft preemption for the path on which the command is executed.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example shows how configure a primary path.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp test
device(config-router-mpls-lsp-test)# soft-preemption
```

The following example shows how to configure a secondary path.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp test
device(config-router-mpls-lsp-test)# secpath sec
device(config-router-mpls-lsp-test-secpath-sec)# soft-preemption
```

soft-preemption cleanup-timer

Sets the amount of time that the point of preemption must wait to receive the path tear notification from the ingress LSR before sending a hard preemption path error.

Syntax

soft-preemption { **cleanup-timer** | *value* }

no soft-preemption { **cleanup-timer** | *value* }

Command Default

The soft-preemption cleanup-timer is disables on the router.

Parameters

cleanup-timer *value*

The *value* is the time the point of preemptionmust wait to receive the path tear notification from the ingress LSR, before sending a hard preemption path error. Values ranging from 1 - 29 are not valid values for this timer. The default setting is 30 seconds. The acceptable range for this timer is 30 - 300. A value of 0 indicates soft preemption is disabled on the router.

Modes

MPLS policy mode

Usage Guidelines

The **no** function returns the timer value settings to the default setting (30 seconds).

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures the soft-preemption cleanup-timer to 30 seconds, which is the default setting.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# soft-preemption cleanup-timer 30
```

source

Configures the source address or a source interface for a tunnel interface.

Syntax

source { *ip-address* | **ethernet** *slot/port* | **loopback** *number* | **ve** *vlan_id* }

no source

Command Default

No source address or interface is configured.

Parameters

ip-address

Specifies the IPv4 address of an interface.

ethernet *slot/port*

Specifies an Ethernet interface.

loopback *number*

Specifies a loopback port.

ve *vlan_id*

Specifies a VE interface.

Modes

Interface tunnel configuration mode

Usage Guidelines

The maximum number of tunnel source supported is 16.

Use the **no source** command to remove the configured source for the tunnel interface.

The tunnel source address should be one of the router IP addresses configured on a physical, loopback, or VE interface, through which the other end of the tunnel is reachable. The source interface must have at least one IP address configured on it.

When the physical/ve interface is specified as the source of the GRE tunnel, the lowest IP address of that interface is used as the tunnel source IP address. If the smallest IP address is removed from the interface, the next smallest IP address is used as the tunnel source.

Examples

This example configures the source address for the tunnel interface.

```
device# configure terminal
device(config)# interface tunnel 5
device(config-intf-tunnel-5)#  source 10.1.2.4
```

This example sets an Ethernet interface as a source tunnel.

```
device# configure terminal
device(config)# interface tunnel 3
device(config-intf-tunnel-3)# source ethernet 3/1
```

source (monitor session)

Configures the mirroring parameters.

Syntax

[no] source { **ethernet** *<interface-id>* | **port-channel** *<port-channel-id>* | **vlan** { *<vlan-id>* | *<vlan-range>* } | **ve** { *<ve-id>* | *<ve-range>* } } **destination** { **ethernet** *<interface-id>* | **port-channel** *<port-channel-id>* } **direction** { *rx* | *tx* | *both* } [**flow-based**]

[no] source { **ethernet** *<interface-id>* | **port-channel** *<port-channel-id>* **vlan** { *<vlan-id>* | *<vlan-range>* } | **ve** { *<ve-id>* | *<ve-range>* } } **destination rspan-vlan** *<vlan-id>* { **ethernet** *<interface-id>* | **port-channel** *<port-channel-id>* } **direction** { *rx* | *tx* | *both* } [**flow-based**]

[no] source { **ethernet** *<interface-id>* | **port-channel** *<port-channel-id>* **vlan** { *<vlan-id>* | *<vlan-range>* } | **ve** { *<ve-id>* | *<ve-range>* } } **destination erspan** *<erspan-id>* **source-ip** *<ip-address>* **destination-ip** *<ip-address>* [**vrf** *<user-vrf>*] **direction** { *rx* | *tx* | *both* } [**flow-based**]

Command Default

There are no defaults for these commands

Parameters

ethernet *<interface-id>*

The source interface ID in the format *0/3*.

port-channel *<port-channel-id>*

The source Port Channel ID.

vlan { *<vlan-id>* | *<vlan-range>* }

The VLAN ID or range of VLANs for the source of the traffic. VLAN is only available for use with Flow Based Mirroring.

ve { *<ve-id>* | *<ve-range>* }

The VE ID or range of VEs for the source of the traffic. VE is only available for use with Flow Based Mirroring.

destination

Indicates that the configurations following this keyword define the settings for the destination of the mirrored traffic.

rspan-vlan *<vlan-id>*

This keyword indicates that the mirroring is RSPAN. Provide the VLAN ID for the VLAN to mirror traffic to.

erspan *<erspan-id>*

This keyword indicates that the mirroring is ERSPAN. Provide a unique ERSPAN ID for this entry.

source-ip *<ip-address>*

The source IP address for the GRE tunnel. This configuration is only available for ERSPAN mirroring.

destination-ip *<ip-address>*

The destination IP address for the GRE tunnel. This configuration is only available for ERSPAN mirroring

vrf *<user-vrf>*

The user created VRF instance. This configuration is only available for ERSPAN mirroring.

direction { *rx* | *tx* | *both* }

Sets the traffic direction to apply mirroring on. You can apply mirroring on ingress, egress, or bi-directional traffic.

flow-based

Indicates that Flow Based Mirroring is being applied. For Flow Based Mirroring to work, it is recommended that ACLs with the *mirror* action be applied to the source interface before configuring Flow Based Mirroring with this command. Flow Based Mirroring will activate only when ACLs are applied to the source interface.

Modes

Monitor Session Mode

Examples

The following are examples for SPAN mirroring.

The following example shows the configuration of SPAN mirroring from a *Port Channel* interface to an *Ethernet* interface. Traffic from both directions is mirrored.

```
SLX# configure terminal
SLX (config)# interface ethernet 0/2
SLX (conf-if-eth-0/2)# lldp disable
SLX (conf-if-eth-0/2)# exit
SLX (config)# monitor session 23
SLX (config-session-23)# source port-channel 1 destination ethernet 0/1 direction both
```

The following example shows the configuration of mirroring from a *Port Channel* to a destination that is a *Port Channel*. Traffic from both directions is mirrored.

```
SLX# configure terminal
SLX (config)# monitor session 24
SLX (config-session-24)# source port-channel 1 destination port-channel 11 direction both
```

The following are examples of Flow Based Mirroring.

This example displays the complete configuration for Flow Based SPAN mirroring.

```
SLX # configure terminal
SLX (config)# interface ethernet 0/3
SLX (conf-if-eth-0/3)# lldp disable
SLX (conf-if-eth-0/3)# exit
SLX (config)#ip access-list extended mirror-my-port
SLX (config-ipacl-std)#
SLX (config-ipacl-std)#seq 5 permit ip host 10.10.10.1 any count mirror
SLX (config-ipacl-std)# exit
SLX (config)# interface ethernet 0/1
SLX (config-eth-0/1)# ip access-group mirror-my-port in
SLX (config-eth-0/1)# ip access-group mirror-my-port out
SLX (config-eth-0/1)# exit
SLX (config)# monitor session 25
SLX (config-session-25)# source ethernet 0/1 destination ethernet 0/3 direction both flow-
based
SLX (config-session-25)# exit
```

This examples show a configuration for Flow Based Mirroring from a *Port Channel* port to an *Ethernet* port.

```
SLX (config)# monitor session 26
SLX (config-session-26)# source port-channel 1 destination ethernet 0/3 direction rx flow-
based
```

This example shows a configuration for Flow Based Mirroring from an *Ethernet* port to a *Port Channel* port.

```
SLX (config)# monitor session 27
SLX (config-session-27)# source ethernet 0/1 destination port-channel 3 direction tx flow-
based
```

This example shows a configuration for Flow Based Mirroring from a *VE* to an *Ethernet* port.

```
SLX (config)# monitor session 28
SLX (config-session-28)# source ve 1 destination ethernet 0/3 direction both flow-based
```

This example show a configuration for Flow Based Mirroring from a *VLAN* to an *Ethernet* port.

```
SLX (config)# monitor session 29
SLX (config-session-29)# source vlan 100 destination ethernet 0/3 direction tx flow-based
```

The following are examples of RSPAN mirroring.

This example mirrors the ingress traffic on ethernet port 0/1 to the destination RSPAN VLAN through the configured ethernet port.

```
SLX# configure terminal
SLX (config)# interface ethernet 0/3
SLX (conf-if-eth-0/3)# lldp disable
SLX (conf-if-eth-0/3)# exit
SLX (config)# monitor session 28
SLX (config-session-28)# source ethernet 0/1 destination rspan-vlan 120 ethernet 0/3
direction rx
```

This example shows the configuration of RSPAN mirroring from a source ethernet port to a destination RSPAN VLAN on a port channel.

```
SLX (config)# monitor session 30
SLX (config-session-30)# source ethernet 0/1 destination rspan-vlan 120 port-channel 2
direction tx
```

The following example shows the complete configuration of Flow Based Mirroring of an *ethernet* port to a RSPAN VLAN.

```
SLX # configure terminal
SLX (config)# interface ethernet 0/3
SLX (conf-if-eth-0/3)# lldp disable
SLX (conf-if-eth-0/3)# exit
SLX (config)#ip access-list extended mirror-my-port
SLX (config-ipacl-std)#
SLX (config-ipacl-std)#seq 5 permit ip host 10.10.10.1 any count mirror
SLX (config-ipacl-std)# exit
SLX (config)# interface ethernet 0/1
SLX (config-eth-0/1)# ip access-group mirror-my-port in
SLX (config-eth-0/1)# ip access-group mirror-my-port out
SLX (config-eth-0/1)# exit
SLX (config)# monitor session 25
SLX (config-session-25)# source ethernet 0/1 destination rspan-vlan 120 ethernet 0/3
direction both flow-based
SLX (config-session-25)# exit
```

The following example shows the configuration of Flow Based Mirroring of a *VLAN* to a RSPAN VLAN accessible on a port channel.

```
SLX # configure terminal
SLX (config)#mac access-list extended mirror-my-port
SLX (config-ipacl-std)#
SLX (config-ipacl-std)#seq 5 permit ip host 10.10.10.1 any count mirror
SLX (config-ipacl-std)# exit
SLX (config)# vlan 100
SLX (config-vlan-100)# mac access-group mirror-my-port in
SLX (config-vlan-100)# mac access-group mirror-my-port out
SLX (config-vlan-100)# exit
SLX (config)# monitor session 31
SLX (config-session-31)# source vlan 100 destination rspan-vlan 120 port-channel 2
direction both flow-based
SLX (config-session-31)# exit
```

The following are examples of ERSPAN mirroring.

This example configures ERSPAN mirroring of the ingress traffic on ethernet port 0/1 to the destination IP address over GRE.

```
SLX# configure terminal
SLX (config)# interface ethernet 0/3
SLX (conf-if-eth-0/3)# lldp disable
SLX (conf-if-eth-0/3)# exit
SLX (config)# monitor session 32
SLX (config-session-32)# source ethernet 0/1 destination erspan 1 source-ip 10.10.10.1
        destination-ip 10.20.20.1 vrf vrf-for-erspan direction both
```

This example shows the configuration of ERSPAN mirroring from a source port channel port to a destination IP over GRE.

```
SLX (config)# monitor session 33
SLX (config-session-33)# source port-channel 1 destination erspan 1 source-ip 10.10.10.1
        destination-ip 10.20.20.1 vrf vrf-for-erspan direction both
```

This example shows the configuration of ERSPAN mirroring from a VE (ve 1) to an specific destination IP(10.20.20.1). This traffic is directed over IP GRE tunnel with a source IP (10.10.10.1).

```
SLX (config)# monitor session 34
SLX (config-session-34)# source ve 1 destination erspan 1 source-ip 10.10.10.1
destination-ip 10.20.20.1
        direction rx vrf vrf-for-erspan flow-based
SLX (config-session-34)# exit
```

This example shows the configuration of ERSPAN mirroring from a VLAN (vlan 100) to an specific destination IP(10.20.20.1). This traffic is directed over IP GRE tunnel with a source IP (10.10.10.1).

```
SLX (config)# monitor session 34
SLX (config-session-34)# source vlan 100 destination erspan 1 source-ip 10.10.10.1
destination-ip 10.20.20.1
        direction rx vrf vrf-for-erspan flow-based
SLX (config-session-34)# exit
```

source-interface (LDAP)

Configures the LDAP server on specific VRF with source interface.

Syntax

source-interface [**ethernet** | **loopback** | **management** | **ve**]

no source-interface

Parameters

ethernet

Uses Ethernet interface as source interface.

loopback

Uses Loopback interface as source interface.

management

Uses Management (chassis IP) as source address.

ve

Uses VE interface as source interface.

Modes

Global configuration mode

Usage Guidelines

If the source-interface is not up or the IP address is not configured for the source-interface, the device acts like the source-interface is not configured.

no source-interface removes the configured source interface on the LDAP server.

You must configure a source interface number for the given source-interface name which is the interface number configured and viewed using the **show ip interface brief** command.

Examples

The following example shows configuration of IP address for source-interface.

```
SLX(config-host-10.1.1.100/mgmt-vrf)# source-interface ethernet 0/1
SLX(config-host-10.1.1.100/mgmt-vrf)# do show running-config ldap-server
ldap-server host 10.1.1.100 use-vrf mgmt-vrf
port 389
source-interface ethernet 0/1
!
SLX(config-host-10.1.1.100/mgmt-vrf)# source-interface ve 10
SLX(config-host-10.1.1.100/mgmt-vrf)# do show running-config ldap-server
ldap-server host 10.1.1.100 use-vrf mgmt-vrf
port 389
```

```
source-interface ve 10
!
SLX(config-host-10.1.1.100/mgmt-vrf)# source-interface loopback 5
SLX(config-host-10.1.1.100/mgmt-vrf)# do show running-config ldap-server
ldap-server host 10.1.1.100 use-vrf mgmt-vrf
port 389
source-interface loopback 5
!
SLX(config-host-10.1.1.100/mgmt-vrf)# no source-interface
SLX(config-host-10.1.1.100/mgmt-vrf)# do show running-config ldap-server
ldap-server host 10.1.1.100 use-vrf mgmt-vrf
port 389
!
```

source-interface (RADIUS)

Configures a source IP address for Remote Authentication Dial-In User Service (RADIUS) packets that originate on the device.

Syntax

source-interface { **ethernet** | **loopback** | **management** { **0** | **1** } | **ve** *ve-num* }

no source-interface

Command Default

When a source interface is not configured for a RADIUS host, the IP address of the interface through which a RADIUS packet exits the device is used in the IP header as the source IP address.

Parameters

ethernet

Causes the ethernet interface to be used as the source interface for RADIUS packets that originate on the device.

loopback

Causes the loopback interface to be used as the source interface for RADIUS packets that originate on the device.

management

Causes the management interface to be used as the source interface for RADIUS packets that originate on the device.

0

Causes the chassis IP address to be used as the source IP address.

1

Causes the MM1 IP address to be used as the source IP address.

ve *ve-num*

Specifies a virtual ethernet interface value to be used as the source interface for RADIUS packets that originate on the device.

Modes

RADIUS server host VRF configuration mode

Usage Guidelines

Note
When an interface without an IP address is configured as the source interface, the egress interface IP address is used as the source interface.

Note
The source interface configuration should not conflict with the VRF specified for communications with the RADIUS server host; when the specified source interface is not part of the VRF configured for communications with the RADIUS server host, the egress interface IP address is used as the source interface.

Modifications to the interface (such as changing the IP address, VRF, and so on) that is configured as the source interface, do not affect existing connections unless the corresponding link is dropped due to these changes.

The **no** form of the command restores the command default value.

Examples

The following example shows how to configure an Ethernet interface (0/2) as the source interface for RADIUS packets that originate on the device and are destined for the RADIUS server host 10.37.73.180.

```
device# configure terminal
device(config)# radius-server host 10.37.73.180 use-vrf green-vrf
device(config-host-10.37.73.180/green-vrf)# source-interface ethernet 0/2
```

spanning-tree autoedge

Enables automatic edge detection.

Syntax

spanning-tree autoedge

no spanning-tree autoedge

Command Default

Auto detection is not enabled.

Modes

Interface configuration mode

Usage Guidelines

The port can become an edge port if no Bridge Protocol Data Unit (BPDU) is received.

Examples

To enable automatic edge detection:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree autoedge
```

spanning-tree bpdu-mac

Sets the MAC address of the Bridge Protocol Data Unit (BPDU).

Syntax

spanning-tree bpdu-mac [**0100.0ccc.cccd** | **0304.0800.0700**]

no spanning-tree bpdu-mac [**0100.0ccc.cccd** | **0304.0800.0700**]

Parameters

0100.0ccc.cccd

Cisco Control Mac

0304.0800.0700

Extreme Control Mac

Modes

Interface configuration mode

Usage Guidelines

This command will only take effect when the protocol is PVST+ or R-PVST+.

Extreme devices support PVST+ and R-PVST+only. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

Enter **no spanning-tree bpdu-mac 0100.0ccc.cccd** to remove the address.

Examples

To set the MAC address of the BPDU:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree bpdu-mac 0100.0ccc.cccd
```

spanning-tree cost

Changes an interface's spanning-tree port path cost.

Syntax

spanning-tree cost *cost*

no spanning-tree cost *cost*

Command Default

The default path cost is 200000000.

Parameters

cost

Specifies the path cost for the Spanning Tree Protocol (STP) calculations. Valid values range from 1 through 200000000.

Modes

Interface configuration mode

Usage Guidelines

Lower path cost indicates a greater chance of becoming root.

Examples

To set the port cost to 128:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree cost 128
```

spanning-tree edgeport

Enables the edge port on an interface to allow the interface to quickly transition to the forwarding state.

Syntax

spanning-tree edgeport [**bpdu-guard**]

no spanning-tree edgeport [**bpdu-guard**]

Command Default

Edge port is disabled.

Parameters

bpdu-guard

Guards the port against the reception of BPDUs.

Modes

Interface subtype configuration mode

Usage Guidelines

This command is only for RSTP and MSTP. Use the **spanning-tree portfast** command for STP

Note the following details about edge ports and their behavior:

- A port can become an edge port if no BPDU is received.
- A port must become an edge port before it receives a BPDU.
- When an edge port receives a BPDU, it becomes a normal spanning-tree port and is no longer an edge port.
- Because ports directly connected to end stations cannot create bridging loops in the network, edge ports directly transition to the forwarding state, and skip the listening and learning states

Examples

To enable a port to quickly transition to the forwarding state:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree edgeport
```

To guard the port against reception of BPDUs:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree edgeport
device(conf-if-eth-1/5)# spanning-tree edgeport bpdu-guard
```

spanning-tree guard root

Enables the guard root to restrict which interface is allowed to be the spanning tree root port or the device's path-to-the-root.

Syntax

spanning-tree guard root [**vlan** *vlan_id*]

no spanning-tree guard root

Command Default

Guard root is disabled.

Parameters

vlan *vlan_id*

Specifies a VLAN.

Modes

Interface configuration mode

Usage Guidelines

Guard root protects the root bridge from malicious attacks and unintentional misconfigurations where a bridge device that is not intended to be the root bridge becomes the root bridge. This causes severe bottlenecks in the data path. Guard root ensures that the port on which it is enabled is a designated port. If the guard root enabled port receives a superior Bridge Protocol Data Unit (BPDU), it goes to a discarding state.

If the VLAN parameter is not provided, the guard root functionality is applied globally for all per-VLAN instances. But for the VLANs which have been configured explicitly, the per-VLAN configuration takes precedence over the global configuration.

The root port provides the best path from the switch to the root switch.

Examples

To enable guard root:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree guard root
```

spanning-tree link-type

Enables and disables the rapid transition for the Spanning Tree Protocol (STP).

Syntax

spanning-tree link-type [**point-to-point** | **shared**]

Command Default

The **spanning-tree link-type** is set to **point-to-point**.

Parameters

point-to-point

Enables rapid transition.

shared

Disables rapid transition.

Modes

Interface subtype configuration mode

Usage Guidelines

This command overrides the default setting of the link type.

Examples

To specify the link type as shared:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree link-type shared
```

spanning-tree portfast

Enables the Port Fast feature on an interface to allow the interface to quickly transition to forwarding state.

Syntax

spanning-tree portfast [**bpdu-guard**]

no spanning-tree portfast [**bpdu-guard**]

Command Default

Port Fast is disabled.

Parameters

bpdu-guard

Guards the port against the reception of BPDUs.

Modes

Interface subtype configuration mode

Usage Guidelines

This command is applicable the only for the Spanning Tree Protocol (STP). Port Fast immediately puts the interface into the forwarding state without having to wait for the standard forward time. Use the **spanning-tree edgeport** command for MSTP and RSTP.

BPDU guard disables all portfast-enabled ports should they ever receive BPDU frames. It does not prevent transmitting of BPDU frames.

If you enable **spanning-tree portfast bpdu-guard** on an interface and the interface receives a BPDU, the software disables the interface and puts the interface in the ERR_DISABLE state.

Enable Port Fast on ports connected to host. Enabling Port Fast on interfaces connected to switches, bridges, hubs, and so on can cause temporary bridging loops, in both trunking and nontrunking mode.

Examples

To enable a port to quickly transition to the forwarding state:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree portfast
```

To guard the port against reception of BPDUs:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree portfast
device(conf-if-eth-1/5)# spanning-tree portfast bpdu-guard
```

spanning-tree priority

Changes an interface's spanning-tree port priority.

Syntax

spanning-tree priority *priority*

no spanning-tree priority

Command Default

The default value is 128.

Parameters

priority

Specifies the interface priority for the spanning tree. The range of valid values is from 0 through 240. Port priority is in increments of 16.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no spanning-tree priority** to return to the default setting.

Examples

To configure the port priority to 16:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree priority 16
```

spanning-tree restricted-role

Restricts the role of the port from becoming a root port.

Syntax

spanning-tree restricted-role

no spanning-tree restricted-role

Command Default

The restricted role is disabled.

Modes

Interface configuration mode

Usage Guidelines

Enter **no spanning-tree restricted-role** to return to the default setting.

Examples

To configure the port from becoming a root port:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree restricted-role
```

spanning-tree restricted-tcn

Restricts the Topology Change Notification (TCN) Bridge Protocol Data Units (BPDUs) sent on the port.

Syntax

spanning-tree restricted-tcn

no spanning-tree restricted-tcn

Command Default

The restricted TCN is disabled.

Modes

Interface configuration mode

Usage Guidelines

Enter **no spanning-tree restricted-tcn** to disable this parameter.

Examples

To restrict the TCN on a specific interface:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree restricted-tcn
```

spanning-tree shutdown

Enables or disables spanning tree on the interface or VLAN.

Syntax

spanning-tree shutdown

no spanning-tree shutdown

Command Default

Spanning tree is disabled by default.

Modes

Interface (Ethernet or VLAN) configuration mode

Usage Guidelines

Enter **no spanning-tree shutdown** to enable spanning tree on the interface or VLAN.

Once all of the interfaces have been configured for a VLAN, you can enable Spanning Tree Protocol (STP) for all members of the VLAN with a single command. Whichever protocol is currently selected is used by the VLAN. Only one type of STP can be active at a time.

A physical interface (port) can be a member of multiple VLANs. For example, a physical port can be a member of VLAN 1002 and VLAN 55 simultaneously. In addition, VLAN 1002 can have STP enabled and VLAN 55 can have STP disabled simultaneously.

Vlan 1002 can not be enabled with the **spanning-tree shutdown** command.

Examples

To disable spanning tree on a specific interface:

```
device# configure terminal
device(config)# interface ethernet 1/5
device(conf-if-eth-1/5)# spanning-tree shutdown
```

speed (Ethernet)

Sets the speed negotiation value on an Ethernet interface.

Syntax

speed { **100** | **1000** | **1000-auto** | **1000-auto-full-duplex** | **1000-master-full-duplex** | **1000-master-half-duplex** | **1000-slave-full-duplex** | **1000-slave-half-duplex** | **10000** | **25000** | **40000** | **100000** | **auto** }

Command Default

The speed is set to **auto** .

Parameters

100

Forces the speed to 100 Mbps.

1000

Forces the speed to 1 Gbps.

1000-auto

Forces the speed to 1 Gbps and auto negotiation of clock parameters. (802.3 Clause 37 Auto-Negotiation)

1000-auto-full-duplex

(Supported only on SLX 9150-XT and Extreme 8520-XT) Forces the speed to be 1Gbps in full duplex mode with auto negotiation of clock parameters.

1000-master-full-duplex

(Supported only on SLX 9150-XT and Extreme 8520-XT) Forces the speed to 1 Gbps with full duplex capability and as a clock master.

1000-master-half-duplex

(Supported only on SLX 9150-XT and Extreme 8520-XT) Forces the speed to 1 Gbps with half duplex capability and as a clock master.

1000-slave-full-duplex

(Supported only on SLX 9150-XT and Extreme 8520-XT) Forces the speed to 1 Gbps with full duplex capability and as a clock slave.

1000-slave-half-duplex

(Supported only on SLX 9150-XT and Extreme 8520-XT) Forces the speed to 1 Gbps with half duplex capability and as a clock slave.

10000

Forces the speed to 10 Gbps.

25000

Forces the speed to 25 Gbps.

40000

Forces the speed to 40 Gbps.

100000

Forces the speed to 100 Gbps.

auto

Allows the interface to negotiate the speed setting, advertising its full capabilities and clock type.

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **auto** keyword or the **no speed** command to reset to the default setting.

Examples

The following example changes the speed to 1G.

```
device# configure terminal
device(config)# interface Ethernet 0/1
device(config-if-eth-0/1)# speed 1000-auto-full-duplex
device(config-if-eth-0/1)# no shutdown
```

The following example changes the speed of the interface to 1G, half duplex, and in the slave clock mode.

```
device# configure terminal
device(config)# interface Ethernet 0/2
device(config-if-eth-0/1)# speed 1000-slave-half-duplex
device(config-if-eth-0/1)# no shutdown
```

spf-interval

Changes the shortest path first (SPF) interval.

Syntax

spf-interval { **level-1** | **level-2** } *max-wait initial-wait second-wait*

no spf-interval

Parameters

level-1

Specifies Level 1 packets only.

level-2

Specifies Level 2 packets only.

max-wait

Specifies the maximum interval between SPF recalculations in seconds. The range is from 0 through 120 seconds. The default is 5 seconds.

initial-wait

Specifies the initial SPF calculation delay in milliseconds after an LSP change. The range is from 0 through 120000 milliseconds. The default is 5000 milliseconds (5 seconds).

second-wait

Indicates the hold time between the first and second SPF calculations in milliseconds. The range is from 1 through 120000 milliseconds. The default is 5000 milliseconds (5 seconds).

Modes

IS-IS router configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command restores the defaults.

Examples

The following example specifies that the maximum interval in seconds between SPF recalculations is 15 seconds for Level 1 packets. The initial SPF calculation delay is 10000

milliseconds, and the hold time between the first and second SPF calculations is 15000 milliseconds.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# spf-interval level-1 15 10000 15000
```

The following example restores the defaults.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# no spf-interval
```

spt-threshold infinity

Configures all sources to use the shared rendezvous point (RP) tree instead of the Shortest Path Tree (SPT).

Syntax

spt-threshold infinity

no spt-threshold

Command Default

By default, the SPT is used for sending packets.

Modes

Router PIM configuration mode

Usage Guidelines

This command uses only the RP to send packets and does not switch over to SPT.

The **no spt-threshold infinity** form of the command resets the default setting and uses SPT for sending packets.

Examples

This example configures all sources to use the shared RP tree for IPv4 PIM.

```
device(config)# router pim
device(config-pim-router)# spt-threshold infinity
```

This example configures all sources to use the shared RP tree for IPv6 PIM.

```
device(config)# ipv6 router pim
device(config-ipv6-router-pim-vrf-default-vrf)# spt-threshold infinity
```

ssh

Connects to a remote server by means of the Secure Shell (SSH) protocol.

Syntax

ssh { *IP_address* | *hostname* } [**-c** | **-l** | **-m** | **interface** {**ethernet** *slot/port* | **management** | **ve** *vlan-id* } | **vrf** *vrf-name*] }

Command Default

SSH connects to port 22.

Parameters

IP_address

Specifies the server IP address in IPv4 or IPv6 format.

hostname

Specifies the host name, a string from 1 through 253 characters.

-c

Specifies the encryption algorithm for the SSH session. This parameter is optional. Supported algorithms include the following:

aes128-cbc

AES 128-bits

aes192-cbc

AES 192-bits

aes256-cbc

AES 256-bits

-l *username*

Login name for the remote server. This parameter is optional. If you specify a user name, you will be prompted for a password. If you do not specify a user name, the command assumes you are logging in as root and will prompt for the root password.

-m

Specifies the HMAC (Hash-based Message Authentication Code) message encryption algorithm. This parameter is optional; if no encryption algorithm is specified, the default (**hmac-md5**) is used. Supported algorithms include the following:

hmac-md5

MD5 128-bits. This is the default setting.

hmac-md5-96

MD5 96-bits

hmac-sha1

SHA1 160-bits

hmac-sha1-96

SHA1 96-bits

interface

Specifies an interface.
ethernet *slot/port*

Specifies an Ethernet interface slot and port number. The only supported value is 0.

management

Specifies the management interface.

ve *vlan-id*

Range is from 1 through 4090 if Virtual Fabrics is disabled, and from 1 through 8191 if Virtual Fabrics is enabled.

vrf *vrf-name*

Specifies a VRF instance. See the Usage Guidelines.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to establish an encrypted SSH connection from a switch to a remote networking device. This implementation is based on SSH v2.

To use the **ssh** command on the management VRF, use the vrf keyword and enter **mgmt-vrf** manually.

The following features are not supported:

- Displaying SSH sessions
- Deleting stale SSH keys

Examples

To connect to a remote device using an SSH connection with default settings:

```
device# ssh 10.70.212.152

The authenticity of host '10.70.212.152 (10.70.212.152)' can't be established.
RSA key fingerprint is f0:2a:7e:48:60:cd:06:3d:f4:44:30:2a:ce:68:fe:1d.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.70.212.152' (RSA) to the list of known hosts.
Password:
```

To connect to a remote device using an SSH connection with the management VRF:

```
device# ssh 10.70.212.152 vrf mgmt-vrf
```

To connect to a remote device using an SSH connection with a login name:

```
device# ssh -l admin 127.2.1.8

admin@127.2.1.8's password
```

ssh client cipher

Sets the SSH client's cipher list for the SSH client.

Syntax

ssh client cipher *string*

no ssh client cipher

Parameters

string

The string name of the cipher. Refer to the device for the available options.

Modes

Global configuration mode

Usage Guidelines

Use the **no ssh client cipher** command remove the cipher list from the ssh client.

Examples

Sets the SSH client's cipher list.

```
device# configure terminal
device(config)# ssh client cipher aes128-cbc
```

ssh client cipher non-cbc

Sets the SSH client's cipher list to non-cbc ciphers for the SSH client.

Syntax

ssh client cipher non-cbc

no ssh client ciphe non-cbc

Modes

Global configuration mode

Usage Guidelines

Use the **no ssh client cipher non-cbc** command remove the non-cbc cipher list from the ssh client.

Examples

Sets the SSH client's cipher list to non-cbc ciphers.

```
device# configure terminal
device(config)# ssh client cipher non-cbc
device(config)# do show running-config ssh
ssh server non-cbc
ssh client non-cbc
```

ssh client key-exchange

Specifies the method used for generating the one-time session keys for encryption and authentication with the Secure Shell (SSH) server and Diffie-Hellman group 14.

Syntax

ssh client key-exchange *string*

no ssh client key-exchange

Parameters

string

The string for the name of the algorithm diffie-hellman-group14-sha1, or a comma-separated list of supported Key-exchange algorithms, such as diffie-hellman-group14-sha1,diffie-hellman-group1-sha1. Refer to the device for a complete list of available options.

Command Default

This command is not configured by default.

Modes

Global configuration mode

Usage Guidelines

You can configure the SSH client key-exchange method to DH Group 14. When the ssh client key-exchange method is configured to DH Group 14, the SSH connection from a remote SSH client is allowed only if the key-exchange method at the client end is also configured to DH Group 14. Enter **no ssh client key-exchange** to restore ssh client key-exchange to the default value.

For information on DH Group 14, see RFC 3526.

For backward compatibility, the string "dh-group-14" is also acceptable in place of "diffie-hellman-group14-sha1"

Examples

To set ssh client key-exchange to DH Group 14:

```
device(config)#ssh client key-exchange diffie-hellman-group14-sha1
```

To restore the ssh client key-exchange to the default value:

```
device(config)# no ssh client key-exchange
```

ssh client mac

Supports MAC configurations for the SSH client.

Syntax

ssh client mac *string*

no ssh client mac

Command Default

SSH server is enabled by default.

Parameters

string

The string name of the default MAC required. Your choices are hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1,hmac-sha1-96, hmac-md5, hmac-md5-96, hmac-ripemd160, hmac-ripemd160@openssh.com, umac-64@openssh.com, umac-128@openssh.com, hmac-sha1-etm@openssh.com, hmac-sha1-96-etm@openssh.com, hmac-md5-etm@openssh.com, hmac-ripemd160-etm@openssh.com, umac-64-etm@openssh.com, umac-128-etm@openssh.com, and hmac-ripemd160-etm@openssh.com. The default MACs supported in FIPS mode are hmac-sha1, hmac-sha2-256, and hmac-sha2-512.

Modes

Global configuration mode

Usage Guidelines

The MAC hmac-md5 is not supported in FIPS mode.

Examples

Typical command example:

```
device# configure terminal
device(config)# ssh client mac hmac-sha1,hmac-sha2-256,hmac-sha2-512
device(config)# do show running-config ssh client
ssh client mac hmac-sha1,hmac-sha2-256,hmac-sha2-512
!
device(config)# do show ssh client status
SSH Client Mac: hmac-sha1,hmac-sha2-256,hmac-sha2-512
```

ssh server algorithm

Configures the SSH server host key algorithm to be used for X.509v3 certificate-based SSH authentication (server authentication).

Syntax

ssh server algorithm {**hostkey** {**x509v3-ssh-rsa** | **x509v3-rsa2048-sha256**}}

no ssh server algorithm hostkey

Command Default

The host key algorithm is not configured.

Parameters

hostkey {**x509v3-ssh-rsa** | **x509v3-rsa2048-sha256**}

Designates x509v3-SSH-RSA or x509v3-RSA2048-SHA256 as the host key algorithm.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of the command to remove the configured algorithm.

Examples

This example configures x509v3-SSH-RSA as the host key algorithm.

```
device# configure terminal
device(config)# ssh server algorithm hostkey x509v3-ssh-rsa
```

ssh server certificate

Configures the SSH server certificate profile and enters SSH server certificate profile configuration mode.

Syntax

ssh server certificate profile *name*

Command Default

By default, a profile name is not configured.

Parameters

profile *name*

Defines the certificate profile. Only "server" and "user" are valid strings.

Modes

Global configuration mode

Usage Guidelines

Examples

Example of entering server profile configuration mode.

```
device# configure terminal
device(config)# ssh server certificate profile server
device(ssh-server-cert-profile-server)#
```

ssh server cipher

Sets the SSH server's cipher list for the SSH server.

Syntax

ssh server cipher *string*

no ssh server cipher

Parameters

string

The string name of the cipher. Refer to the device for the available options.

Modes

Global configuration mode

Usage Guidelines

Use the **no ssh server cipher** command remove the cipher list from the ssh client.

Examples

Sets the SSH server's cipher list.

```
device# configure terminal
device(config)# ssh server cipher aes256-ctr
```

ssh server key

Generates or zeroizes SSH crypto keys on the device. All three keys can be active simultaneously.

Syntax

ssh server key { **dsa** | **rsa** [**1024** | **2048** | **4096**] | **ecdsa 256** }

no ssh server key { **dsa** | **rsa** | **ecdsa** }

Command Default

The default values of SSH keys are:

- DSA is active
- ECDSA value is 256
- RSA value is 2048

Parameters

dsa

Generates the DSA key.

rsa [**1024** | **2048** | **4096**]

Generates the RSA key, in either the 1024, 2048, or 4096 bit size.

ecdsa 256

Generates the ECDSA key at 256 bits.

Modes

Global configuration mode

Usage Guidelines

The **no ssh server key** command zeroizes the SSH keys on the device. Running the **no** form of the command requires you to save the configuration and reload the device. See the last example for more information.

If you generate and delete SSH crypto keys, you must restart the SSH server using the **no ssh server shutdown** command to enable the configuration.

Examples

Typical DSA command example:

```
device(config)# ssh server key dsa
```

Typical RSA command example:

```
device(config)# ssh server key rsa 4096
```

Typical ECDSA command example:

```
device(config)# ssh server key ecdsa 256
```

Typical zeroizing example. Note that running the **no** form of the command requires you to save the configuration and reload the device.

```
device(config)# no ssh server key dsa
                    % Info: Configuration is successful. For this config to take effect
immediately, restart SSH
                    server via exec command ssh-server restart or save the config and
reload.
```

ssh server key-exchange

Specifies the method used for generating the one-time session keys for encryption and authentication with the Secure Shell (SSH) server and Diffie-Hellman group 14.

Syntax

ssh server key-exchange *string*

no ssh server key-exchange

Parameters

string

The string for the name of the algorithm diffie-hellman-group14-sha1, or a comma-separated list of supported Key-exchange algorithms; such as diffie-hellman-group14-sha1,diffie-hellman-group1-sha1, and so on.

Command Default

This command is not configured by default.

Modes

Global configuration mode

Usage Guidelines

You can configure the SSH server key-exchange method to DH Group 14. When the SSH server key-exchange method is configured to DH Group 14, the SSH connection from a remote SSH client is allowed only if the key-exchange method at the client end is also configured to DH Group 14. Enter **no ssh server key-exchange** to restore SSH server key-exchange to the default value.

For information on DH Group 14, refer to RFC 3526.

For backward compatibility, the string "dh-group-14" is also acceptable in place of "diffie-hellman-group14-sha1"

Examples

To set SSH server key-exchange to DH Group 14:

```
device(config)# ssh server key-exchange diffie-hellman-group14-sha1
```

To restore the SSH server key-exchange to default value:

```
device(config)# no ssh server key-exchange
```

ssh server mac

Supports MAC configurations for the SSH server.

Syntax

ssh server mac *string*

no ssh server mac

Parameters

string

The string name of the required default MAC.
Your choices are hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1, hmac-sha1-96, hmac-md5, hmac-md5-96, hmac-ripemd160, hmac-ripemd160@openssh.com, umac-64@openssh.com, umac-128@openssh.com, hmac-sha1-etm@openssh.com hmac-sha1-96-etm@openssh.com, hmac-md5-etm@openssh.com, hmac-ripemd160-etm@openssh.com, umac-64-etm@openssh.com, umac-128-etm@openssh.com, and hmac-ripemd160-etm@openssh.com. The default MACs supported in FIPS mode are hmac-sha1, hmac-sha2-256, and hmac-sha2-512.

Modes

Global configuration mode

Usage Guidelines

The MAC hmac-md5 is not supported in FIPS mode.

Examples

Typical command example:

```
device# configure terminal
device(config)# ssh server mac hmac-sha1,hmac-sha2-256,hmac-sha2-512
device(config)# do show running-config ssh server
ssh server mac hmac-sha1,hmac-sha2-256,hmac-sha2-512
ssh server key rsa 2048
ssh server key ecdsa 256
ssh server key dsa
```

ssh server max-auth-tries

Configures the maximum number of times a user is allowed to try to authenticate to the SSH server.

Syntax

ssh server max-auth-tries { *num-tries* }

no ssh server max-auth-tries

Command Default

The default is 6 tries.

Parameters

num-tries

Maximum number of tries. Range of valid values is from 1 through 10.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of the command to reset the default.

This command configures the maximum number of times a user is allowed to try authenticate to the SSH server. When the number of attempts to log in to an SSH session is more than the defined value, the session is terminated.

Examples

This example changes the maximum number of tries to 2.

```
device# configure terminal
device(config)# ssh server max-auth-tries 2
```

ssh server max-idle-timeout

Configures the maximum number of seconds that the SSH session is allowed to idle before timing out.

Syntax

ssh server max-idle-timeout { *secs* }

no ssh server max-idle-timeout

Command Default

By default, there is no timeout.

Parameters

secs

Maximum idle time in seconds. Range of valid values is from 1 through 14400.

Modes

Global configuration mode

Usage Guidelines

Use the no form of the command to reset the default.

This command configures the maximum interval of time that the SSH session is allowed to idle. When an SSH session is idle for a time defined by the idle timeout, the session is terminated.

Examples

This example changes the timeout to 15 seconds.

```
device# configure terminal
device(config)# ssh server max-idle-timeout 15
```

ssh server max-login-timeout

Configures the maximum timeout interval for log in attempts in the SSH session.

Syntax

ssh server max-login-timeout { *secs* }

no ssh server max-login-timeout

Command Default

The default is 120 seconds.

Parameters

secs

Maximum timeout in seconds. Range of valid values is from 1 through 120.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of the command to reset the default.

This command configures the maximum timeout interval for the SSH session. When the loin prompt of an SSH session is idle for a time defined by the log in timeout, the session is terminated.

Examples

This example changes the timeout to 60 seconds.

```
device# configure terminal
device(config)# ssh server max-login-timeout 60
```

ssh server rekey-interval

Configures the Secure Shell (SSH) server rekey-interval.

Syntax

ssh server rekey-interval *interval*

no ssh server rekey-interval

Parameters

interval

The value for the rekey interval. Range is from 900 to 3600 seconds.

Modes

Global configuration mode

Usage Guidelines

Use the **no ssh server rekey-interval** command to remove the rekey-interval.

ssh server rekey-volume

Configures the Secure Shell (SSH) server rekey volume.

Syntax

ssh server { **rekey-volume** *value*}

no ssh server { **rekey-volume** *value*}

Command Default

The command default is 1024.

Parameters

rekey-volume *value*

The range of valid values is from 512 through 4095 megabytes. In FIPS mode, this value can not exceed 1024.

Modes

Global configuration mode

Usage Guidelines

The **no ssh server** command resets to no rekeying.

Examples

Example of setting the rekey value to 768 megabytes.

```
device# configure terminal
device(config)# ssh server rekey-volume 768
```

ssh server use-vrf shutdown

Disables the SSH service.

Syntax

ssh server use-vrf *vrf-name* **shutdown**

no ssh server use-vrf *vrf-name* **shutdown**

Parameters

use-vrf *vrf-name*

Specifies a user-defined VRF or built-in VRFs such as mgmt-vrf or default-vrf.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command enables the SSH service.

The use of the **use-vrf** keyword brings down the server only for the specified VRF. You can shut down any server in any VRF, including the management and default VRF.

Examples

This example shuts down the SSH service for a VRF.

```
device(config)# ssh server use-vrf myvrf shutdown
```

This example enables the SSH service on the VRF.

```
device(config)# no ssh server use-vrf myvrf shutdown
```

ssl-profile

Use the **ssl-profile** command to configure the lowest TLS version supported by the SLX software. SLX uses OpenSSL to provide transport layer security and the current version of OpenSSL supports TLS v 1.1 to TLS v 1.2. Since the SLX box can be considered as both a client as well as a server, you can apply different supported TLS versions for each of these types. This **ssl-profile** command enables you to select the SLX operation mode from either *Client* or *Server* and then set the lowest supported TLS version.

Syntax

ssl-profile { **client** | **server** }

Parameters

client

Specifies that the configuration is for when the SLX is a client to another device.

server

Specifies that the configuration is for when the SLX acts as a server to other devices.

Modes

Management Security mode

Usage Guidelines

Opens and navigates into the specific configuration modes.

Examples

This example show how to navigate into the *Client* configuration mode inside the *Management Security* mode.

```
SLX # conf term
Entering configuration mode terminal

SLX (config)#
SLX (config)# management-security
SLX (mgmt-security)# ?
SLX (mgmt-security)# ssl-profile ?
Possible completions:
   client    management security ssl profile client for tls configuration
   server    management security ssl profile server for tls configuration

SLX (mgmt-security)# ssl-profile client
SLX (mgmt-sec-ssl-profile-client)#
```

ssm-enable

Enables Source Specific Multicast (SSM) mode for IPv4 PIM.

Syntax

ssm-enable range *prefix-list*

no ssm-enable range *prefix-list*

Command Default

By default, PIM-SSM is not enabled.

Parameters

range

Specifies the range of the SSM map. By default, the range is 232.0.0.0/8 for IPv4.

prefix-list

Specifies the IPv4 prefix list that identifies the multicast group address range.

Modes

Router PIM configuration mode

Usage Guidelines

PIM-SSM is a subset of the PIM-SM protocol. In PIM-SSM mode, the Shortest Path Tree (SPT) is created at the source. The router closest to the receiver host is notified of the unicast IP address of the source for the multicast traffic. PIM-SSM goes directly to the source-based distribution tree without the need of the RP connection. In contrast to PIM-SM, PIM-SSM forms its own SPT, without forming a shared tree.

Examples

The following example enables SSM and applies the default IPv4 SSM range of 232.0.0.0/8.

```
device(config)# router pim
device(config-pim-router)# ssm-enable
```

The following example enables SSM and configures an SSM map at the global level.

```
device(config)# ip igmp ssm-map enable
device(config)# ip igmp ssm-map ssm-map-230-to-232 203.0.0.10
device(config)# ip igmp ssm-map ssm-map-233-to-234 204.0.0.10
```

The following example configures the SSM range at the router PIM configuration level.

```
device(config)# router pim
device(config-pim-router)# ssm-enable range PL_ssm_range-230-to-234
```

start (CFM)

Defines the start time for a delay measurement receiver session.

Syntax

start { **now** | **after** *HH:MM:SS* | *HH:MM:SS* **daily** }

no start

Command Default

The start time is not defined

Parameters

now

The session is initiated immediately.

after *HH:MM:SS*

Initiates the one-way delay measurement receiver session after a period of time has elapsed, in hours, minutes, and seconds.

HH:MM:SS **daily**

Initiates the one-way delay measurement receiver session at the specified time every day.

Modes

CFM protocol configuration mode

Usage Guidelines

The **no start** command deletes the start time.

Relative time is converted to absolute time. Otherwise, the system would not point to the expected time after a reboot.

Examples

Example of starting the session after one hour and thirty minutes.

```
device(config-cfm-oneway-dm-receiver-1)#  start after 01:30:00
```

Example of starting the session daily at 3:30 pm.

```
device(config-cfm-oneway-dm-receiver-1)#  start daily 15:30:00
```

start (Y1731)

Configure the start time.

Syntax

start at *hh:mm:ss* **daily**

start after *hh:mm:ss* **daily**

no start

Parameters:

at

Spcifies the time to start at.

hh:mm:ss

Specifies the time in hour, minute, and second format.

after

Specifies the measurement interval in minutes.

daily

Specifies time to start daily.

Command Default

The default value is start after 00:05:00 (After).

Modes

Y1731 configuration mode

Usage Guidelines

Use the **no** form of the command to delete the start configuration.

Examples

This example shows how to configure the start time.

```
device# configure terminal
device (config-cfm)# prtocol cfm
device (config-cfm)# y1731
device(config-cfm-y1731)# test-profile my_test_profile
device(config-cfm-y1731-test-profile-my_test_profile)# type delay-measurement
device(config-cfm-y1731-test-profile-my_test_profile)# tx-interval 60
device(config-cfm-y1731-test-profile-my_test_profile)# measurement-interval 30
device(config-cfm-y1731-test-profile-my_test_profile)# start at 00:00:00 daily
```

start-shell

Accesses the SLXVM Linux shell from the SLX-OS CLI.

Syntax

start-shell

Modes

Privileged EXEC mode

Usage Guidelines

This command is only available for users with admin-level permissions.

You can also run this command from Global configuration mode: `device(config)# do start-shell`.

Inside the SLXVM Linux shell, you can escalate your privileges to root access, by using the **su root** Linux command. Escalation to root access is password protected.

Inside the SLXVM Linux shell, execution of root privilege commands using **sudo** is not supported.

The idle timeout of Linux shell sessions is five minutes, after which you are automatically logged out of the Linux shell and returned to the SLX-OS CLI.

Examples

The following example accesses the SLXVM Linux shell from the SLX-OS CLI.

```
device# start-shell
Entering Linux shell for the user: admUser
[admUser@SLX]#
```

The following example escalates access from the default SLXVM Linux shell to root.

```
[admUser@SLX]# su root
Password:

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.
[root@SLX]#
```

In the following example, the Linux **ps -ef** command lists the process status.

```
[admUser@SLX]# ps -ef
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 Jul24 ?        00:00:04 /sbin/init
root         2     0  0 Jul24 ?        00:00:00 [kthreadd]
```

```
root         3     2  0 Jul24 ?        00:00:00 [migration/0]
root         4     2  0 Jul24 ?        00:00:03 [ksoftirqd/0]
root         5     2  0 Jul24 ?        00:00:00 [migration/1]
root         6     2  0 Jul24 ?        00:00:03 [ksoftirqd/1]
root         7     2  0 Jul24 ?        00:00:00 [migration/2]
root         8     2  0 Jul24 ?        00:00:02 [ksoftirqd/2]
root         9     2  0 Jul24 ?        00:00:00 [migration/3]
root        10     2  0 Jul24 ?        00:00:02 [ksoftirqd/3]
root        11     2  0 Jul24 ?        00:00:00 [migration/4]
root        12     2  0 Jul24 ?        00:00:02 [ksoftirqd/4]
root        13     2  0 Jul24 ?        00:00:00 [migration/5]
root        14     2  0 Jul24 ?        00:00:03 [ksoftirqd/5]
root        27     2  0 Jul24 ?        00:00:00 [cpuset]
root        28     2  0 Jul24 ?        00:00:01 [khelper]
root        31     2  0 Jul24 ?        00:00:00 [netns]
root        34     2  0 Jul24 ?        00:00:00 [async/mgr]
root       270     2  0 Jul24 ?        00:00:00 [sync_supers]
root       272     2  0 Jul24 ?        00:00:00 [bdi-default]

...

root      8kblockd/6]182     1  0 Jul24 ?        00:00:00 /usr/sbin/inetd
root      8237     1  0 Jul24 ?        00:00:00 /usr/sbin/sshd
admin    27536 27535  0 04:19 pts/4    00:00:00 ps -ef
```

The following example exits a root-level user to the SLXVM Linux shell.

```
[root@SLX]#  exit
exit
[admUser@SLX]#
```

The following example exits from the SLXVM Linux shell to the SLX-OS CLI.

```
[admUser@SLX]# exit
exit
Exited from Linux shell
device#
```

static-network

Configures a static BGP4 network, creating a stable network in the core.

Syntax

static-network *network/mask* [**distance** *num*]

no static-network *network/mask* [**distance** *num*]

Parameters

network/mask

Network and mask in CIDR notation.

distance *num*

Specifies an administrative distance value for this network. Valid values range from 1 through 255. The default is 200.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

Usage Guidelines

While a route configured with this command will never flap unless it is deleted manually, a static BGP4 network will not interrupt the normal BGP4 decision process on other learned routes that are installed in the Routing Table Manager (RTM). Consequently, when there is a route that can be resolved, it will be installed into the RTM.

Examples

The following example configures a static network and sets an administrative distance of 300.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# static-network 10.11.12.0/32 distance 300
```

statistics

Enables statistics on the tunnel interface.

Syntax

statistics

no statistics

Command Default

Statistics is disabled on a tunnel interface.

Modes

Interface tunnel configuration mode

Usage Guidelines

Use the **no** form of this command to disable statistics on the tunnel interface.

Note that traffic loss might occur when you enable or disable statistics on a tunnel interface.

Examples

This example enables statistics on the tunnel interface.

```
device# configure terminal
device (config)# interface tunnel 5
device(config-intf-tunnel-5)# statistics
```

statistics (bridge domain)

Enables ingress and egress statistics on a bridge domain.

Syntax

statistics

no statistics

Command Default

Statistics are disabled.

Modes

Bridge-domain configuration mode

Usage Guidelines

The **no** form of the command disables statistics on the bridge domain.

Examples

The following example shows how to enable ingress and egress statistics on bridge domain 2.

```
device# config terminal
device(config)# bridge-domain 2
device(config-bridge-domain-2)# statistics
```

statistics (VLAN)

Enables statistics on a VLAN.

Syntax

statistics

no statistics

Command Default

Statistics are disabled.

Modes

VLAN configuration mode

Usage Guidelines

The **no** form of the command disables statistics on a VLAN.

Examples

The following example shows how to enable statistics on VLAN 10.

```
device# config terminal
device(config)# vlan 10
device(config-Vlan-10)# statistics
```

stop (CFM)

Defines the stop time for a delay measurement receiver session.

Syntax

stop { **now** | **after** *HH:MM:SS* | *HH:MM:SS* **daily** }

no stop

Command Default

The stop time is not defined

Parameters

now

The session is halted immediately.

after *HH:MM:SS*

Halts the one-way delay measurement receiver session after a period of time has elapsed, in hours, minutes, and seconds.

HH:MM:SS **daily**

Halts the one-way delay measurement receiver session at the specified time every day.

Modes

CFM protocol configuration mode

Usage Guidelines

The **no stop** command deletes the stop time.

The one-way delay measurement receiver session should be started before starting the one-way delay measurement Initiator session. Also, the one-way delay measurement Initiator session should be stopped before stopping the one-way delay measurement Receiver session.

Relative time is converted to absolute time. Otherwise, the system would not point to the expected time after a reboot.

Examples

Example of stopping the session after one hour and thirty minutes.

```
device(config-cfm-oneway-dm-receiver-1)#  stop after 01:30:00
```

Example of stopping the session daily at 3:30 pm.

```
device(config-cfm-oneway-dm-receiver-1)#  stop daily 15:30:00
```

stop (Y1731)

Configure the stop time.

Syntax

stop [**at** *hh:mm:ss* | **after** *hh:mm:ss*]

no stop

Parameters:

at

Spcifies the time to stop at.

hh:mm:ss

Specifies the time in hour, minute, and second format.

after

Specifies the time to stop after.

Command Default

The default value is 01:05:00 (After).

Modes

Y1731 configuration mode

Usage Guidelines

Use the **no** form of the command to delete the stop configuration.

Examples

This example shows how to configure the stop time.

```
device# configure terminal
device (config-cfm)# protocol cfm
device (config-cfm)# y1731
device(config-cfm-y1731)# test-profile my_test_profile
device(config-cfm-y1731-test-profile-my_test_profile)# type delay-measurement
device(config-cfm-y1731-test-profile-my_test_profile)# tx-interval 60
device(config-cfm-y1731-test-profile-my_test_profile)# measurement-interval 30
device(config-cfm-y1731-test-profile-my_test_profile)# start at 00:00:00 daily
device(config-cfm-y1731-test-profile-my_test_profile)# stop at 23:59:00
```

storm-control ingress (global)

Limits ingress traffic globally on all device Ethernet interfaces.

Syntax

storm-control ingress { **broadcast** | **unknown-unicast** | **multicast** } **limit-bps** *rate*

no storm-control ingress { **broadcast** | **unknown-unicast** | **multicast** }

Parameters

broadcast

Specifies that the command operates on broadcast traffic only.

unknown-unicast

Specifies that the command operates on unknown-unicast traffic only.

multicast

Specifies that the command operates on multicast traffic only.

limit-bps *rate*

Specifies that the value given to the *rate* parameter is in bits per second. If the traffic on the interface reaches this rate, no more traffic (for the traffic type specified) is allowed on the interface. For the rate, enter an integer from 0 to 10000000000. Because each application-specific integrated circuit (ASIC) may support different bit granularity, bit rates are rounded up to the next achievable rate.

Modes

Global configuration mode

Usage Guidelines

This command limits the amount of broadcast, unknown unicast, and multicast (BUM) ingress traffic globally on all device interfaces when configured in global configuration mode.

If you want to modify an active BUM storm control configuration, you must first disable it, then issue the **storm-control ingress** command again with the new parameters.

Enter **no storm-control ingress** to disable BUM storm control for a particular traffic type on the interface.

Examples

The following example configures storm control on all Ethernet interfaces on the device with a rate limited to 1000000 bps.

```
device(config)# storm-control ingress broadcast 1000000
```

storm-control ingress (interface)

Limits ingress traffic on a specified interface.

Syntax

storm-control ingress { **broadcast** | **unknown-unicast** | **multicast** } **limit-bps** | *rate*

no storm-control ingress { **broadcast** | **unknown-unicast** | **multicast** }

Parameters

broadcast

Specifies that the command will operate on broadcast traffic only.

unknown-unicast

Specifies that the command will operate on unknown-unicast traffic only.

multicast

Specifies that the command will operate on multicast traffic only.

limit-bps

Specifies that the value given to the *rate* parameter is in bits per second. If the traffic on the interface reaches this rate, no more traffic (for the traffic type specified) is allowed on the interface.

rate

Specifies the amount of traffic allowed, either in bits per second or a percentage of the capacity of the interface, depending on which parameter was chosen with the rate.

If you are specifying rate in bps, enter an integer from 0 to 10000000000. Because each application-specific integrated circuit (ASIC) may support different bit granularity, bit rates are rounded up to the next achievable rate.

If you are specifying rate in percent of interface capacity, enter an integer from 0 to 100.

Modes

Interface configuration mode

Usage Guidelines

This command limits the amount of broadcast, unknown unicast, and multicast (BUM) ingress traffic on a specified interface.

If you want to modify an active BUM storm control configuration, you must first disable it, then issue the **storm-control ingress** command again with the new parameters.

Enter **no storm-control ingress** to disable BUM storm control for a particular traffic type on an interface.

Examples

This example configures storm control on an Ethernet interface, with a rate limited to 1000000 bps.

```
device(config)# interface ethernet 1/2
device(conf-if-eth-1/2)# storm-control ingress broadcast 1000000
```

subnet

Specifies the local IP address with the subnet mask of the routing device.

Syntax

subnet *subnet_addr*

no subnet *subnet_addr*

Command Default

The command is disabled by default.

Parameters

subnet_addr

Specifies the subnet mask of the IP address.

Modes

MPLS CSPF-group configuration mode

Usage Guidelines

When the command is configured, every link in the subnet is penalized.

The **no** form of the command disables the command.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures subnet *10.1.2.0* with a mask length of *24*.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# cspf-group group3
device(config-router-mpls-cspf-group-group3)# subnet 10.1.2.0/24
```

sub-ring

Configures a bridge as a sub-ring node for Ethernet Ring Protection (ERP) and specifies a parent ring ID.

Syntax

sub-ring parent-ring-id *id*

no sub-ring parent-ring-id *id*

Command Default

A bridge is not configured as a sub-ring node by default.

Parameters

parent-ring-id *id*

Specifies a parent ring ID.

Modes

ERP configuration mode

Usage Guidelines

This command sets the major-ring or sub-ring, and optionally the ERP ID, that are associated with this sub-ring. Both the parent and the sub-ring ERP instances can be configured with the same VLAN.

Use the **no** form of this command to revert to the previous configuration.

Examples

The following example sets the sub-ring and a parent-ring ID of 2.

```
device# configure terminal
device(config)# erp 1
device(config-erp-1)# sub-ring parent-ring-id 2
```

summary-address (IS-IS)

Configures route summarization to aggregate Intermediate System-to-Intermediate System (IS-IS) route information.

Syntax

summary-address *ip-address subnet-mask* **level-1** [**level-2**]

summary-address *ip-address subnet-mask* **level-2** [**level-1**]

no summary-address *ip-address subnet-mask* **level-1** [**level-2**]

no summary-address *ip-address subnet-mask* **level-2** [**level-1**]

Command Default

Disabled.

Parameters

ip-address

Specifies an IP address.

subnet-mask

Specifies a subnet mask.

level-1

Specifies that only routes redistributed into Level 1 are summarized with the configured address and mask value.

level-2

Specifies that only routes redistributed into Level 2 are summarized with the configured address and mask value.

Modes

IS-IS address-family IPv4 unicast configuration mode

Usage Guidelines

Route Summarization using this command is applicable only for redistributed routes.

The **no** form of the command disables route summarization.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures a summary address of 10.1.0.0 with a mask of 255.255.0.0 for Level 1 redistributed routes.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# summary-address 10.1.0.0 255.255.0.0 level-1
```

The following example configures a summary address of 10.1.0.0 with a mask of 255.255.0.0 for Level 2 redistributed routes.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# summary-address 10.1.0.0 255.255.0.0 level-2
```

The following example configures a summary address of 10.1.0.0 with a mask of 255.255.0.0 for Level 1 and Level 2 redistributed routes.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# summary-address 10.1.0.0 255.255.0.0 level-1 level-2
```

summary-address (OSPFv2)

Configures route summarization for redistributed routes for an Autonomous System Boundary Router (ASBR).

Syntax

summary-address *A.B.C.D E.F.G.H*

no summary-address

Command Default

Summary addresses are not configured.

Parameters

A.B.C.D E.F.G.H

IP address and mask for the summary route representing all the redistributed routes in dotted decimal format.

Modes

OSPF router configuration mode

OSPF VRF router configuration mode

Usage Guidelines

Use this command to configure an ASBR to advertise one external route as an aggregate for all redistributed routes that are covered by a specified address range. When you configure an address range, the range takes effect immediately. All the imported routes are summarized according to the configured address range. Imported routes that have already been advertised and that fall within the range are flushed out of the AS and a single route corresponding to the range is advertised.

If a route that falls within a configured address range is imported by the device, no action is taken if the device has already advertised the aggregate route; otherwise the device advertises the aggregate route. If an imported route that falls within a configured address range is removed by the device, no action is taken if there are other imported routes that fall within the same address range; otherwise the aggregate route is flushed.

The device sets the forwarding address of the aggregate route to 0 and sets the tag to 0. If you delete an address range, the advertised aggregate route is flushed and all imported routes that fall within the range are advertised individually. If an external link-state-database-overflow condition occurs, all aggregate routes and other external routes are flushed out of the AS. When the device exits the external LSDB overflow

condition, all the imported routes are summarized according to the configured address ranges.This parameter affects only imported, type 5 external routes.

The no form of the command disables route summarization.

Examples

The following example configures a summary address of 10.1.0.0 with a mask of 10.255.0.0. Summary address 10.1.0.0, includes addresses 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. For all of these networks, only the address 10.1.0.0 is advertised in external LSAs:

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# summary-address 10.1.0.0 10.255.0.0
```

summary-address (OSPFv3)

Configures route summarization for redistributed routes for an Autonomous System Boundary Router (ASBR).

Syntax

summary-address *IPv6-addr/mask*

no summary-address

Command Default

Summary addresses are not configured.

Parameters

A:B:C:D/LEN

IPv6 address and mask for the summary route representing all the redistributed routes in dotted decimal format.

Modes

OSPFv3 router configuration mode

OSPFv3 VRF router configuration mode

Usage Guidelines

Use this command to configure an ASBR to advertise one external route as an aggregate for all redistributed routes that are covered by a specified IPv6 address range. When you configure an address range, the range takes effect immediately. All the imported routes are summarized according to the configured address range. Imported routes that have already been advertised and that fall within the range are flushed out of the AS and a single route corresponding to the range is advertised.

If a route that falls within a configured address range is imported by the device, no action is taken if the device has already advertised the aggregate route; otherwise the device advertises the aggregate route. If an imported route that falls within a configured address range is removed by the device, no action is taken if there are other imported routes that fall within the same address range; otherwise the aggregate route is flushed.

The device sets the forwarding address of the aggregate route to 0 and sets the tag to 0. If you delete an address range, the advertised aggregate route is flushed and all imported routes that fall within the range are advertised individually. If an external link-state-database-overflow condition occurs, all aggregate routes and other external routes are flushed out of the AS. When the device exits the external LSDB overflow

condition, all the imported routes are summarized according to the configured address ranges.

Examples

The following example configures a summary address of 2001:db8::/24 for routes redistributed into OSPFv3. The summary prefix 2001:db8::/24 includes addresses 2001:db8::/1 through 2001:db8::/24. Only the address 2001:db8::/24 is advertised in an external link-state advertisement.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# summary-address 2001:db8::/24
```

summary-prefix

Configures summary prefixes to aggregate IPv6 Intermediate System-to-Intermediate System (IS-IS) route information.

Syntax

summary-prefix *ipv6-prefix prefix-length* { **level-1** | **level-2** }

no summary-prefix *ipv6-prefix prefix-length* { **level-1** | **level-2** }

Command Default

Disabled.

Parameters

ipv6-prefix prefix-length

Specifies the aggregate address. You must specify the *ipv6-prefix* parameter in hexadecimal using 16-bit values between colons as documented in RFC 2373. You must specify the *prefix-length* parameter as a decimal value. A slash mark (/) must follow the *ipv6-prefix* parameter and precede the *prefix-length* parameter.

level-1

Specifies that only routes redistributed into Level 1 are summarized

level-2

Specifies that only routes redistributed into Level 2 are summarized.

Modes

IS-IS address-family IPv6 unicast configuration mode

Usage Guidelines

IS-IS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Route Summarization using this command is applicable only for redistributed routes.

The **no** form of the command disables route summarization.

Examples

The following example configures a summary prefix of 2001:db8::/32 to be advertised to Level 1 redistributed routes only.

```
device# configure terminal
device(config)# router isis
```

```
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# summary-prefix 2001:db8::/32 level-1
```

The following example configures a summary prefix of 2001:db8::/32 to be advertised to Level 2 redistributed routes only.

```
device# configure terminal
device(config)# router isis
device(config-isis-router)# address-family ipv4 unicast
device(config-router-isis-ipv4u)# summary-prefix 2001:db8::/32 level-2
```

support autoupload-param

Defines autoupload parameters.

Syntax

support autoupload-param hostip *hostip* | **user** *user_acct* | **password** *password* [**protocol** [**ftp** | **scp** | **sftp**] **directory** *path*

Parameters

hostip *host-ip*

Specifies the IP address of the remote host.

user *user_acct*

Specifies the user name to access the remote host.

password *password*

Specifies the password to access the remote host.

protocol *FTP* | *SCP*| *SFTP*

Specifies the protocol used to access the remote server.

directory *path*

Specifies the path to the directory.

Modes

Global configuration mode

Examples

```
device(config)# support autoupload-param hostip 10.31.2.27 protocol [ftp|scp |
sftp]username hegdes directory /uers/home40/hegdes/autoupload password

(<string>): *****
```

suppress-arp

Enables Address Resolution Protocol (ARP) suppression on a current VLAN or bridge domain. ARP suppression can lessen ARP-related traffic within an IP Fabric.

Syntax

suppress-arp

no suppress-arp

Command Default

ARP suppression is disabled.

Modes

VLAN configuration mode

Bridge-domain configuration mode

Usage Guidelines

This feature is required, along with ND suppression, if static anycast gateway is supported in an IP Fabric.

To disable ARP suppression, use the **no** form of this command.

Examples

The following example enables ARP suppression on a VLAN.

```
device# configure terminal
device(config)# vlan 100
device(config-vlan-100)# suppress-arp
```

The following example enables ARP suppression on a bridge domain.

```
device# configure terminal
device(config)# bridge-domain 2
device(config-bridge-domain-2)# suppress-arp
```

suppress-nd

Enables Neighbor Discovery (ND) suppression on a VLAN or bridge domain. ND suppression can lessen the amount of ND control traffic within an IP Fabric.

Syntax

suppress-nd

no suppress-nd

Command Default

ND suppression is disabled.

Modes

VLAN configuration mode

Bridge-domain configuration mode

Usage Guidelines

This feature is required, along with ARP suppression, if static anycast gateway is supported in an IP Fabric.

To disable ND suppression, use the **no** form of this command.

Examples

The following example enables ND suppression on a specified VLAN.

```
device# configure terminal
device(config)# vlan 100
device(config-vlan-100)# suppress-nd
```

The following example enables ND suppression on bridge domain 2.

```
device# configure terminal
device(config)# bridge-domain 2
device(config-bridge-domain-2)# suppress-nd
```

switch-attributes

Configures the chassis or host name for the device.

Syntax

switch-attributes [**chassis-name** *chassis-name*] [**host-name** *host-name*]

switch-attributes [**chassis-name**][**host-name**]

Command Default

The default host name is SLX.

The default chassis name varies with the device.

Parameters

chassis-name *chassis-name*

Specifies the chassis name. A chassis name can be from 1 through 30 characters long, must begin with a letter, and can contain letters, numbers, and underscore characters.

host-name *host-name*

Specifies the host name and changes the CLI prompt. A host name can be from 1 through 30 characters long. It must begin with a letter, and can contain letters, numbers, and underscore characters.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of the command to reset the default settings.

We recommend that you customize the chassis name for each device. Some system logs identify the device by its chassis name; if you assign a meaningful chassis name, logs are more useful.

Examples

The following example configures the chassis and host names.

```
device# configure terminal
device(config)# switch-attributes chassis-name SLX-market1
device(config)# switch-attributes host-name SLX-mrkt
SLX-mrkt(config)#
```

switchport

Puts the interface in Layer 2 mode and sets the switching characteristics of the Layer 2 interface.

Syntax

switchport

no switchport

Command Default

All Layer 2 interfaces are mapped to default VLAN 1 and the interface is set to access mode.

Modes

Interface subtype configuration mode

Usage Guidelines

For changing the interface configuration mode to trunk or changing the default VLAN mapping, use additional **switchport** commands.

To redefine the switch from Layer 2 mode into Layer 3 mode, enter **no switchport**.

Examples

To put a specific Ethernet interface in Layer 2 mode:

```
device# configure terminal
switch(config)# interface ethernet 1/9
switch(conf-if-eth-1/9)# switchport
```

To remove a specific port-channel interface from Layer 2 mode:

```
device# configure terminal
switch(config)# interface port-channel 44
switch(config-Port-channel-44)# no switchport
```

switchport access

Sets the Layer 2 interface as access.

Syntax

switchport access { **vlan** *vlan_id*}

no switchport access { **vlan** *vlan_id*}

Command Default

All Layer 2 interfaces are in access mode and belong to the VLAN ID 1.

Parameters

vlan *vlan_id*

Sets the port VLAN (PVID) to the specified *vlan_id*. Range is below 4090 for 802.1Q VLANs.

Modes

Interface subtype configuration mode on edge ports

Usage Guidelines

In access mode, the interface only allows untagged and priority tagged packets.

Enter **no switchport access vlan** to set the PVID to the default VLAN 1.

Examples

To set the Layer 2 interface PVID to 100 on a specific Ethernet interface:

```
device# configure terminal
switch(config)# interface ethernet 1/9
switch(conf-if-eth-1/9)# switchport access vlan 100
```

To set the PVID to the default VLAN 1 on a specific port-channel interface:

```
device# configure terminal
switch(config)# interface port-channel 44
switch(config-Port-channel-44)# no switchport access vlan
```

switchport mode

Sets the mode of the Layer 2 interface.

Syntax

switchport mode { **access** | **trunk** }

Parameters

access

Sets the Layer 2 interface as access. Access mode assigns the port to a VLAN

trunk

Sets the Layer 2 interface as trunk. Trunk mode makes the port linkable to other switches and routers

Modes

Interface subtype configuration mode

Usage Guidelines

You must configure the same native VLAN on both ends of an 802.1 or classified VLAN trunk link. Failure to do so can cause bridging loops and VLAN leaks.

Examples

To set the mode of a specific Ethernet interface to access:

```
device# configure terminal
switch(config)# interface ethernet 1/9
switch(conf-if-eth-1/9)# switchport mode access
```

To set the mode of a specific port-channel interface to trunk:

```
device# configure terminal
switch(config)# interface port-channel 44
switch(config-Port-channel-44)# switchport mode trunk
```

switchport mode trunk-no-default-native

Configures a port to trunk mode without the native vlan.

Syntax

switchport mode trunk-no-default-native

Modes

Interface configuration mode

Usage Guidelines

By assigning this mode, you can configure an untagged logical interface on the specified port. The device discards any ingress tagged or untagged packet until a switchport classification or native VLAN classification is configured.

To disable this functionality, issue the **no switchport** command, or enter a different switchport mode by using the **switchport mode access** command or the **switchport mode trunk** command.

Before you change the switch port mode from **switchport mode access** with an explicit **switchport access vlan** to **switchport mode trunk-no-default-native**, you must enter the **no switchport** command on the interface level, and then enter the **switchport** command to set the interface as a switchport. Now you can configure the **switchport mode trunk-no-default-native** command.

Port mode change is not allowed when port security is enabled on the interface.

This is the fundamental difference between this command and the **switch mode trunk** command, which implicitly creates VLAN 1 on the port.

The global command **dot1q tag native-vlan** does not affect the ingress or egress tagging behavior of the native VLAN configured in this mode.

The following native VLAN commands that are supported in regular trunk mode are NOT supported in this mode:

- **switchport trunk tag native-vlan**
- **switchport trunk native-vlan**

Examples

The following example configures a trunk port without a default native VLAN, then explicitly configures the native VLAN.

```
device# configure terminal
device(config)# interface ethernet 0/1
```

```
device(config-if-eth-0/1)# switchport mode trunk-no-default-native
device(config-if-eth-0/1)# switchport trunk tagged
```

switchport port-security

Enables port security on an interface port.

Syntax

switchport port-security

no switchport port-security

Command Default

Port security is not enabled.

Modes

Interface configuration mode

Usage Guidelines

Port mode change is not allowed when port security is enabled on the interface.

The **no switchport port-security** command disables port security on the interface.

Examples

The following example enables port MAC security on an interface:

```
device(config)# interface Ethernet 3/2
device(conf-if-eth-3/2)# switchport
device(conf-if-eth-3/2)# switchport port-security
```

switchport port-security mac-address

Configures the MAC address option for port security on an interface port.

Syntax

switchport port-security mac-address *address* **vlan** *vlan_id*

Command Default

MAC address is not configured for port security.

Parameters

mac-address *address*

Specifies the MAC address-based VLAN classifier rule used to map to a specific VLAN.

vlan *vlan_id*

Specifies a VLAN.

Modes

Interface configuration mode

Usage Guidelines

Static MAC addresses cannot be configured on a secure port. They must be configured as secure MAC addresses on the secure port.

When static MAC address is configured on an access secure port, the MACs qualify for access VLANs, but on trunk port, VLAN must be specified.

The **no switchport port-security mac-adress** command removes the specified MAC address.

Examples

The following example configures static MAC address for port security on an interface:

```
device(config)# interface Ethernet 3/2
device(conf-if-eth-3/2)# switchport
device(conf-if-eth-3/2)# switchport port-security mac-address 0000.00eb.2d14 vlan 2
```

switchport port-security max

Configures the maximum number of MAC addresses used for port MAC security on an interface port.

Syntax

switchport port-security max *value*

no switchport port-security max

Parameters

value

The maximum number of secure MAC addresses. Range is from 1 through 8192.

Command Default

The default value is 8192 MAC addresses.

Modes

Interface configuration mode

Usage Guidelines

The maximum MAC address limit for sticky MAC address and static MAC address depends on the device limit. For dynamically learned MAC addresses, the maximum limit is 8192 per port.

The **no switchport port-security max** command restores the default value of maximum number of MAC addresses.

Examples

The following example configures the maximum number of MAC addresses used for port MAC security on an interface port as 10:

```
device(config)# interface Ethernet 3/2
device(conf-if-eth-3/2)# switchport
device(conf-if-eth-3/2)# switchport port-security max 10
```

switchport port-security shutdown-time

Configures the auto recovery time for ports that shuts down following a port security violation on an interface.

Syntax

switchport port-security shutdown-time *time*

Command Default

Auto recovery of ports is not enabled.

Parameters

time

The amount of time in minutes, the port waits before it recovers from forced port shutdown. Range is from 1 through 15.

Modes

Interface configuration mode

Usage Guidelines

The shutdown and no-shutdown processes initiated as part of the port violation action is independent of the shutdown process explicitly initiated by an administrator on the same port on which port MAC security is enabled.

If a port security-based change occurs when a port is shut down, the shutdown timer is not triggered. Consequently, the user must restore the full functionality of the port.

When port security violation causes a port to be shut down and the user manually changes the shutdown time, the shutdown timer is reset and the timer starts with the new shutdown time.

The **no switchport port-security shutdown-time** command disables the auto recovery functionality.

Examples

The following example configures the auto recovery time as 4 minutes for ports that shuts down following a port security violation on an interface.

```
device(config)# interface Ethernet 3/2
device(conf-if-eth-3/2)# switchport
device(conf-if-eth-3/2)# switchport port-security shutdown-time 4
```

switchport port-security sticky

Enables sticky MAC learning on the port to convert the dynamically learned MAC addresses to sticky secure MAC addresses.

Syntax

switchport port-security sticky [**mac-address** *address* **vlan** *vlan_id*]

no switchport port-security sticky [**mac-address** *address* **vlan** *vlan_id*]

Command Default

Sticky MAC learning on the port is not enabled.

Parameters

mac-address *address*

Specifies the MAC address-based VLAN classifier rule used to map to a specific VLAN.

vlan *vlan_id*

Specifies a VLAN.

Modes

Interface configuration mode

Usage Guidelines

When sticky MAC learning is enabled on a secured port, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses. All the subsequent sets of dynamically learned MAC addresses will also be converted to sticky secure MAC addresses.

The **no switchport port-security sticky** disables sticky MAC learning on a secure port, and all the sticky MAC addresses will be converted back to dynamically learned MAC addresses.

Sticky MAC addresses persist even if the port goes down or if the device reboots.

Examples

The following example enables sticky MAC learning on the port and configures port security with sticky MAC address:

```
device(config)# interface Ethernet 3/2
device(conf-if-eth-3/2)# switchport
```

```
device(conf-if-eth-3/2)# switchport port-security sticky
device(conf-if-eth-3/2)# switchport port-security sticky mac-address 0000.0018.747C vlan 5
```

switchport port-security violation

Configures the violation response action for port security on an interface.

Syntax

switchport port-security violation shutdown

Command Default

The port shuts downs if port security violation occurs.

Parameters

shutdown

Puts the interface into the error-disabled state.

Modes

Interface configuration mode

Usage Guidelines

If a MAC address already learned on a secured port ingresses on a non-secured port or through another secured port, it is not considered security violation. In this scenario, MAC movement happens if it is a dynamically learned MAC address. If it is a static MAC address or sticky MAC address, MAC movement does not happen, but the traffic is switched (flooded or forwarded) based on the destination MAC address.

If the port shuts down after security violation, an administrator can explicitly bring up the interface or a shutdown timer can be configured using the **switchport port-security shutdown-time** command. After the configured shutdown time, the interface automatically comes up and the port security configuration remains configured on the port.

When the device reboots after port shutdown due to security violation, the ports come up in the shutdown state.

Examples

The following example configures the violation response action as shutdown for port security on an interface:

```
device(config)# interface Ethernet 3/2
device(conf-if-eth-3/2)# switchport
device(conf-if-eth-3/2)# switchport port-security violation shutdown
```

switchport trunk allowed

Adds or removes VLANs on a Layer 2 interface in trunk mode.

Syntax

switchport trunk allowed { **vlan** } { **add** *vlan_id* | **all** | **except** *vlan_id* | **none** | **remove** *vlan_id* }

Parameters

add *vlan_id*

Adds a VLAN to transmit and receive through the Layer 2 interface. The VLAN can be an 802.1Q VLAN.

all

Allows only 802.1Q VLANs to transmit and receive through the Layer 2 interface. This keyword does not apply to classified or transport VLANs.

except *vlan_id*

Allows only 802.1Q VLANs except the specified VLAN ID to transmit and receive through the Layer 2 interface.

none

Allows only 802.1Q VLANs to transmit and receive through the Layer 2 interface. This keyword does not apply to service or transport VFs.

remove *vlan_id*

Removes a VLAN that transmits and receives through the Layer 2 interface.

Modes

Interface subtype configuration mode

Usage Guidelines

Examples

To add the tagged VLAN 100 to a specific Ethernet interface:

```
device# configure terminal
switch(config)# interface ethernet 0/9
switch(conf-if-eth-0/9)# switchport trunk allowed vlan add 100
```

To remove the tagged VLAN 100 from the interface:

```
device# configure terminal
switch(config)# interface ethernet 0/9
switch(conf-if-eth-0/9)# switchport trunk allowed vlan remove 100
```

switchport trunk native-vlan-untagged

Configures a port to accept only untagged packets, and specifies that those packets be egress untagged. The untagged packets may be classified to an 802.1Q VLAN, a service VF, or a transport VF.

Syntax

switchport trunk native-vlan-untagged *vlan_id*

no switchport trunk native-vlan-untagged

Parameters

vlan_id

Adds a classified VLAN (VLAN ID > 4095) to transmit and receive through the Layer 2 interface.

Modes

Interface subtype configuration mode on a trunk port

Usage Guidelines

This command is supported when the port is in no-default-vlan trunk mode, as enabled by means of the **switchport mode trunk-no-default-native** command.

Use the **no switchport trunk native-vlan-untagged** command to remove the configuration.

Port mode change is not allowed when port security is enabled on the interface.

Examples

Configure untagged native VLAN 5000, allow VLAN 6000, and make VLAN 7000 the default VLAN.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(config-if-eth-0/1)# switchport mode trunk-no-default-native
device(config-if-eth-0/1)# switchport trunk native-vlan untagged 5000
device(config-if-eth-0/1)# switchport trunk add vlan 6000 ctag 100-200
device(config-if-eth-0/1)# switchport trunk default-vlan 7000
```

Remove the native VLAN 5000.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(config-if-eth-0/1)# no switchport trunk native-vlan-untagged
```

switchport trunk native-vlan-xtagged

Configures a port to accept both tagged and untagged packets, and specifies the egress tagging behavior.

Syntax

switchport trunk native-vlan-xtagged *vlan_id* [**ctag** *cvid*] **egress** { **tagged** | **untagged** | **any** }

no switchport trunk native-vlan-xtagged

Parameters

vlan_id

Adds a classified VLAN (VLAN ID > 4095) to transmit and receive through the Layer 2 interface.

ctag *cvid*

Sets an optional C-TAG (802.1Q VLAN ID) for a service or transport VF (VLAN ID > 4095).

egress

Enables the selection of required tagging options.

tagged

Specifies packets as tagged.

untagged

Specifies packets as untagged.

any

Specifies that packets preserve their ingress encapsulation.

Modes

Interface subtype configuration mode on a trunk port

Usage Guidelines

This command is supported when the port is in no-default-vlan trunk mode, as enabled by means of the **switchport mode trunk-no-default-native** command.

Note the following:

- Ingress packets may be classified to an 802.1Q VLAN, a service VF, or a transport VF.
- The native VLAN must accept tagged frames for the **ctag** keyword to apply.
- If the specified VLAN is an 802.1Q VLAN, the **ctag** option is not required.

- If the specified VLAN is an 802.1Q VLAN or a service VF, the **egress** tagging options are **tagged** or **untagged**.
- If the specified VLAN is a transport VF, then the **egress** tagging option must be **any** to preserve the encapsulation of ingress frames.

Use the **no switchport trunk native-vlan-xtagged** command to remove the configuration.

Port mode change is not allowed when port security is enabled on the interface.

Examples

Configure transport VF 6000 that accepts C-TAG range 100 through 200 and a native VLAN that can be either tagged or untagged.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(config-if-eth-0/1)# switchport mode trunk-no-default-native
device(config-if-eth-0/1)# switchport trunk native-vlan-xtagged 6000 ctag 10 egress any
device(config-if-eth-0/1)# switchport trunk allow vlan 6000 ctag 100-200
```

Remove the native VLAN from the transport VF.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(config-if-eth-0/1)# no switchport trunk native-vlan-xtagged
```

switchport trunk tag native-vlan

Enables tagging on native VLAN traffic.

Syntax

switchport trunk tag native-vlan

no switchport trunk tag native

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no switchport trunk tag native** to untag native traffic for a specific interface.

Examples

To enable tagging for native traffic on a specific Ethernet interface:

```
device# configure terminal
switch(config)# interface ethernet 0/9
switch(conf-if-eth-0/9)# switchport trunk tag native-vlan
```

sync-interval

Configures the interval between Precision Time Protocol (PTP) synchronization (Sync) messages on an interface.

Syntax

sync-interval *seconds*

no sync-interval

Command Default

See Parameters.

Parameters

seconds

Interval between PTP Synch messages, in log seconds. Range is -4 through 2. The default is -1 (2 packets/second). See the Usage Guidelines. Range is -4 through 2. The default is -1 (2 packets/second).

Modes

PTP configuration mode

Interface subtype configuration mode

Usage Guidelines

The inputs for interval represent base 2 exponents, where the packet rate is $1/(2^{log\ seconds})$.

Configuring this interval on an edge port overrides the switch (global) default.

Important
Do not configure a rate slower than the default on links between SLX devices.

Use the no form of this command to revert to the default.

Examples

To configure a PTP Sync interval of 2 on an Ethernet interface:

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# protocol ptp
device(conf-if-eth-0/1-ptp)# sync-interval 2
```

To revert to the default PTP Sync interval of -1:

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# protocol ptp
device(conf-if-eth-0/1-ptp)# no sync-interval
```

sysmon fe-acces-check

Configures system error monitoring.

Syntax

sysmon fe-access-check [**action** | **disable** | **poll-interval** | **recovery-threshold** | **threshold**]

Parameters

action

Sets Fe-Access-Check action.

disable

Disables the Fe Access Check.

poll-interval

Sets the Fe-Access-Check poll-interval.

recovery-threshold

Sets the Fe-Access-Check recovery threshold.

threshold

sets the Fe-Access-Check threshold.

Modes

Global configuration mode

Usage Guidelines

By default, the Fe access check is disabled. The default recovery threshold is 1 and the default threshold is 3. The default action is log, which logs the FE acces errors.

Examples

```
device(config)# sysmon fe-access-check ?
Possible completions:
  action               Set Fe-Access-Check action
  disable              Disable Fe Access Check (Default: Enabled)
  poll-interval        Set Fe-Access-Check poll-interval
  recovery-threshold   Set Fe-Access-Check recovery threshold
  threshold            Set Fe-Access-Check threshold
device(config)# sysmon fe-access-check recovery-threshold ?
Possible completions:
  <1-3>   Default: 1
device(config)# sysmon fe-access-check recovery-threshold 2
device(config)# sysmon fe-access-check threshold?
Possible completions:
  threshold   Set Fe-Access-Check threshold
device(config)# sysmon fe-access-check threshold ?
Possible completions:
```

```
  <1-10>   Default: 3
device(config)# sysmon fe-access-check threshold 5
device(config)# sysmon fe-access-check action ?
Possible completions:
  log       Log FE access error (Default action)
  recover   Recover FE
device(config)# sysmon fe-access-check action log ?
Possible completions:
  <cr>
device(config)# sysmon fe-access-check action log?
Possible completions:
  log   Log FE access error (Default action)
device(config)# sysmon fe-access-check recover ?
Possible completions:
<1-3>  Default is 1
device(config)# sysmon fe-access-check recover 2
```

sysmon link-crc-monitoring

Enables link CRC monitoring.

Syntax

sysmon sfm-walk [**auto** | **disable-redundancy-check** | **poll-interval** | **threshold**]

Parameters

action

Sets Link CRC Monitoring actions.

disable

Disables link CRC Monitoring.

poll-interval

Sets link CRC monitoring poll-interval.

threshold

Sets link CRC Monitoring threshold.

Modes

Global configuration mode

Usage Guidelines

By default, link-crc monitoring is disabled. Default threshold is 5 and default poll-interval is 60 seconds.

Examples

```
device(config)# sysmon link-crc-monitoring ?
Possible completions:
  action          Set Link CRC Monitoring action
  disable         Disable Link CRC Monitoring (Default: Enabled)
  poll-interval   Set Link CRC Monitoring poll-interval
  threshold       Set Link CRC Monitoring threshold
device(config)# sysmon link-crc-monitoring threshold ?
Possible completions:
  <1-10>   Default: 5
device(config)# sysmon link-crc-monitoring threshold 9
device(config)# sysmon link-crc-monitoring poll-interval ?
Possible completions:
  <1-300>   Default: 60 Sec
device(config)# sysmon link-crc-monitoring poll-interval 500
```

sysmon sfm-walk

Enables SFM walk.

Syntax

sysmon sfm-walk [**auto** | **disable-redundancy-check** | **poll-interval** | **threshold**]

Parameters

auto

Enable auto SFM walk.

disable-redundancy-check

Disables SFM Walk redundancy check.

poll-interval

Sets SFM Walk poll-interval.

threshold

Sets SFM Walk reassembly error threshold.

Modes

Global configuration mode

Usage Guidelines

By default, SFM walk and redundancy check are disabled.

Examples

```
device(config)# sysmon sfm-walk ?
Possible completions:
  auto                       Enable Auto SFM Walk (Default: Disabled)
  disable-redundancy-check   Disable SFM Walk redundancy check (Default:
                             Enabled)
  poll-interval              Set SFM Walk poll-interval
  threshold                  Set SFM Walk reassembly error threshold
device(config)# sysmon sfm-walk auto?
Possible completions:
  auto   Enable Auto SFM Walk (Default: Disabled)
device(config)# sysmon sfm-walk auto ?
Possible completions:
  <cr>
device(config)# sysmon sfm-walk disable-redundancy-check?
Possible completions:
  disable-redundancy-check   Disable SFM Walk redundancy check (Default:
                             Enabled)
device(config)# sysmon sfm-walk disable-redundancy-check ?
Possible completions:
  <cr>
```

```
device(config)# sysmon sfm-walk poll-interval?
Possible completions:
  poll-interval   Set SFM Walk poll-interval
device(config)# sysmon sfm-walk poll-interval ?
Possible completions:
  <1-600>   Default: 30 Sec
SLX(config)# sysmon sfm-walk poll-interval 500
The Client sysmgr is not Known or Connected
```

system maintenance

Enters system maintenance mode.

Syntax

system maintenance

no system maintenance

Command Default

By default, system maintenance mode is not enabled.

Modes

Privileged EXEC mode

Usage Guidelines

Planned maintenance operations such as software upgrade, SFP replacement, cable replacement, and node replacement can require that the device be shutdown or restared. This can result in traffic disruption even if alternate paths are available. Maintenance mode provides graceful traffic diversion to alternate traffic paths, helping to minimize traffic loss during such planned operations.

When an alternate path is available, the BGP and MCT protocols redirect traffic away from the node that is going into maintenance mode. When maintenance mode is enabled, all protocols that are running on the maintenance mode node are notified and redirection of traffic (convergence) begins in stages.

The **no** form of the command disables maintenance mode. In `config-system-maintenance` sub-mode, the **no enable** command also disables maintenance mode.

The `enable-on-reboot` parameter allows the device to enter maintenance mode after a reboot, allowing any network errors and the device that gets added back to the network.

Maintenance mode is not supported for the following features: BGP address-family, Flowspec, Layer 3 VPN, VPLS, and VLL (virtual leased line).

Examples

The following example enables system maintenance mode and specifies a convergence time of 120 seconds.

```
SLX # configure terminal
SLX (config)# system maintenance
SLX (config-system-maintenance)# convergence-time 120
SLX (config-system-maintenance)# shutdown-time 360
SLX (config-system-maintenance)# enable
```

The following example disables maintenance mode.

```
SLX(config)# no system maintenance
```

The following example also disables maintenance mode.

```
device(config-system-maintenance)# no enable
```

The following example enables system reboot into maintenance mode

```
SLX # configure terminal
SLX (config)# system maintenance
SLX (config-system-maintenance)# enable-on-reboot
```

system maintenance turn-off

Brings device out of maintenance mode when **enable-on-reboot** is used.

Syntax

system maintenance turn-off

Parameters

system maintenance turn-off

Brings device out of maintenance mode when **enable-on-reboot** is used to reboot the device into maintenance mode.

Modes

Operational mode.

Examples

The following example brings the device out of maintenance mode.

```
SLX# system maintenance turn-off
SLX#
```

system-description

Sets the global system description specific to LLDP.

Syntax

system-description *line*

no system-description

Parameters

line

Specifies a description for the LLDP system. The string must be between 1 and 50 ASCII characters in length.

Modes

Protocol LLDP configuration mode

Usage Guidelines

Enter **no system-description** to clear the global LLDP system description.

Examples

To set the global system description specific to LLDP on the SLX-OS platform, enter the following:

```
device(conf-lldp)# system-description SLXR
```

system-monitor tm

Accesses system monitor traffic manager (sys-mon TM) configuration mode to configure the monitoring of the traffic manager (TM) device or Virtual Output Queue (VOQ) discarded packets.

Syntax

system-monitor tm

no system-monitor tm

Modes

Global configuration mode

Usage Guidelines

By default, the monitoring of the TM device and VOQ discarded packets is disabled until you configure their threshold.

Use the **no** form of this command to reset the monitoring of the TM device and VOQ discarded packets configurations to their default values and disable the monitoring of the packets.

Examples

The following example enables VOQ discarded packets monitoring and accesses sys-mon TM configuration mode.

```
device# configure terminal
device (config)# system-monitor tm
device (config-sys-mon-tm)#
```

system-monitor-mail

Configures various email settings as part of system monitoring.

Syntax

system-monitor-mail [**fru** | **interface** | **relay** | **security** |**sfp**]

Parameters

fru

Configure FRU mail settings.

interface

Configure interface mail settings.

relay

Configure relay ip mail settings.

security

Cconfigure security mail settings.

sfp

Configure sfp mail settings.

Modes

Global configuration mode

Examples

```
device(config)# system-monitor-mail ?
Possible completions:
  fru         Configure FRU mail settings
  interface   Configure interface mail settings
  relay       Configure relay ip mail settings
  security    Configure security mail settings
  sfp         Configure sfp mail settings
device(config)# system-monitor-mail fru ?
Possible completions:
  <email:string>  e-mail address for FRU alerts
  enable   Enable FRU email alerts
device(config)# system-monitor-mail fru enable ?
Possible completions:
  <cr>
device(config)# system-monitor-mail fru enable?
Possible completions:
  enable   Enable FRU email alerts
device(config)# system-monitor-mail fruemail ?
                                    ^
% Invalid input detected at '^' marker.
device(config)# system-monitor-mail fru email ?
Possible completions:
  <cr>
```

```
device(config)# system-monitor-mail fru ncp@extreme.com
device(config)#
```

system-monitoring power alert state removed action raslog

Monitors the power supply component and generates RASLog when the component changes from the configured state.

Syntax

system-monitoring power alert state removed action raslog

Parameters

Alert

Configures alerts for the POWER SUPPLY component.

State

Specifies the supported states for component (power supply) that may be monitored.

action

Specifies the action that may be taken when component (power supply) changes from the configured state.

Modes

Global configuration mode

Examples

```
device(config)# system-monitor power ?
Possible completions:
  alert       Configure alerts for component:POWER SUPPLY
  threshold   Configure threshold for component:POWER SUPPLY
device(config)# system-monitor power alert ?
Possible completions:
  action   Action that may be taken when component:POWER SUPPLY changes
           configured state
  state    Supported states for component: POWER-SUPPLY that may be monitored
device(config)# system-monitor power alert state ?
Possible completions:
  [removed]  all  faulty  inserted  none  on  removed
device(config)# system-monitor power alert state removed ?
Possible completions:
  action   Action that may be taken when component:POWER SUPPLY changes
           configured state
  <cr>
device(config)# system-monitor power alert state removed action ?
Possible completions:
  [raslog]  all  email  none  raslog
device(config)# system-monitor power alert state removed action raslog ?
Possible completions:
  <cr>
device(config)# system-monitor power alert state removed action raslog
```

system power-cycle-db-shutdown

Shuts down the chassis configuration database gracefully without restarting the device for a planned power-cycle.

Syntax

system power-cycle-db-shutdown

Command Default

The chassis configuration database is running normally.

Modes

Global configuration mode

Usage Guidelines

When devices encounter abrupt power cycles, there have been rare cases of device configuration database corruption. This database corruption causes the device to reboot and reverts the device to the startup configuration.

In the case of scheduled power-cycles, it is recommended to use the **system power-cycle-db-shutdown** command before actual restarting the device.

This command shuts down the chassis configuration database, without rebooting the device. All commands (except for the **reload** command) are blocked on this node until the node is restarted.

Note
Suppose the configuration database on a switch gets corrupted due to an abrupt power cycle, run the **firmware install** or the **write erase** commands to clean up the corrupted files and/or to reinstall the firmware.

The node is not fully functional until it restarts. This command should be run as part of any planned power outages.

Examples

```
device# configure terminal
device(config)# system power-cycle-db-shutdown
Are you sure you want to shutdown database for power-cycle? [y/n]: y
2017/02/09-13:02:42, [DCM-1015], 51,, INFO, SLX9140, Switch is prepared for power-cycle.
No clis will work henceforth. Need power-cycle or reload to make switch fully functional.
Operation Successful.
```

system-name

Sets the global system name specific to LLDP.

Syntax

system-name *name*

no system-name

Command Default

The host name from the device is used.

Parameters

name

Specifies a system name for the LLDP. The string must be between 1 and 32 ASCII characters in length.

Modes

Protocol LLDP configuration mode

Usage Guidelines

Enter **no system-name** to delete the name.

Examples

To specify a system name for the LLDP:

```
device(conf-lldp)# system-name System10
```

table-map

Maps external entry attributes into the BGP routing table, ensuring that those attributes are preserved after being redistributed into OSPF.

Syntax

table-map *string*

no table-map *string*

Command Default

This option is disabled.

Parameters

string

Specifies a route map to be whose attributes are to be preserved. Range is from 1 through 63 ASCII characters.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the no form of the command to remove the table map.

Use this command only to set the tag values. Normally, a route map is applied on routes (and therefore the routes are updated) before it is stored in the BGP routing table. Use the **table-map** command to begin the update before the routes are stored in the IP routing table.

Configurations made by this command apply to all peers.

Route maps that contain **set** statements change values in routes when the routes are accepted by the route map. For inbound route maps (route maps that filter routes received from neighbors), the routes are changed before they enter the BGP routing table. For tag values, if you do not want the value to change until a route enters the IP routing table, you can use a table map to change the value. A table map is a route map that you have associated with the IP routing table. The device applies the **set** statements for tag values in the table map to routes before adding them to the routing table. To configure a table map, you first configure the route map, then identify it as a

table map. The table map does not require separate configuration. You can have only one table map.

Note
Use table maps only for setting the tag value. Do not use table maps to set other attributes. To set other route attributes, use route maps or filters. To create a route map and identify it as a table map, enter commands such those shown in the first example below. These commands create a route map that uses an address filter. For routes that match the IP prefix list filter, the route map changes the tag value to 100 and is then considered as a table map. This route map is applied only to routes that the device places in the IP routing table. The route map is not applied to all routes. The first example below assumes that IP prefix list p11 has already been configured.

Examples

This example illustrates the execution of the **table-map** command.

```
device# configure terminal
device(config)# route-map tag_ip permit 1
device(config-route-map/tag_ip/permit/1)# match ip address prefix-list p11
device(config-route-map/tag_ip/permit/1)# set tag 100
device(config-route-map/tag_ip/permit/1)# exit
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# table-map tag_ip
```

This example removes the table map for the default VRF.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv4 unicast
device(config-bgp-ipv4u)# no table-map tag_ip
```

This example removes the table map for VRF “red”.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# no table-map tag_ip
```

tacacs-server

Configures a Terminal Access Controller Access-Control System plus (TACACS+) server.

Syntax

tacacs-server { **host** *hostname* }[**use-vrf** { **mgmt-vrf** | **default-vrf** |*vrf-name* }] [**port** *portnum*] [**protocol** { **chap** | **pap** }] [**key** *shared-secret*] [**encryption-level** *value_level*] [**timeout** *secs*] [**retries** *num*] [**source-interface** *ip-address*]

no tacacs-server { **host** *hostname* } [**use-vrf** { **mgmt-vrf** | **default-vrf** | *vrf-name* }] [**port** *portnum*] [**protocol** { **chap | pap**}] [**key** *shared-secret*] [**encryption-level** *value-level*] [**timeout** *secs*] [**retries** *num*] [**source-interface** *ip-address*]

Command Default

See the Parameters section for specific defaults.

Parameters

host hostname

Specifies the IP address or domain name of the TACACS+ server. IPv4 and IPv6 addresses are supported.

use-vrf

Specifies a VRF though which to communicate with the TACACS+ server. See the Usage Guidelines.

mgmt-vrf

Specifies the management VRF.

default-vrf

Specifies the default-vrf.

vrf-name

Specifies a VRF name.

source-interface *ip-address*

Specifies the source interface for the TACACS host.

port *portnum*

Specifies the TCP port for authentication. Valid values range from 0 through 65535. The default is 49.

protocol { **chap** | **pap**}

Specifies the authentication protocol. Options include CHAP and PAP. The default is CHAP.

key *shared-secret*

Specifies the text string that is used as the shared secret between the device and the TACACS+ server to make the message exchange secure. The key must be between 1 and 40 characters in length.

The default key is **sharedsecret**. The exclamation mark (!) is supported in RADIUS and TACACS+ servers. You can specify the password in either double quotes or the escape character (\), for example **"secret!key"** or **secret\!key**. The only other valid characters are alphanumeric characters (a-z and 0-9) and underscores. No other special characters are allowed.

encryption-level *value_level*

Designates the encryption level for the shared secret key operation. This operand supports JITC certification and compliance. The valid values are 0 and 7, with 0 being clear text and 7 being the most heavily encrypted. The default value is 7.

timeout *secs*

Specifies the time to wait for the TACACS+ server to respond. The default is 5 seconds.

retries *num*

Specifies the number of attempts allowed to connect to a TACACS+ server. The default is 5 attempts.

Modes

Global configuration mode

Usage Guidelines

If a TACACS+ server with the specified IP address or host name does not exist, it is added to the server list. If the TACACS+ server already exists, this command modifies the configuration. The **key** parameter does not support an empty string.

Use the no form of the command to reset the specified attributes to their default values.

Before downgrading to a software version that does not support the **encryption-level** keyword, set the value of this keyword to **0**. Otherwise, the firmware download will generate an error that requests this value be set to **0**.

Before downgrading to a version that doesn't support **tacacs-server source-interface**, you must remove the source-ip configuration using **no source-interface**. Otherwise, the firmware download process generates an error requesting to reset the cipher.

By default, all management services are enabled on the management VRF ("mgmt-vrf") and the default VRF ("default-vrf").

If the **encryption-level** is zero (0) but the key entered is encrypted then the following error message is displayed: `Error: Input key must be plain text when encryption-level selected is 0`.

Examples

This example configures an IPv4 TACACS+ server.

```
device# configure terminal
device(config)# tacacs-server host 10.24.65.6
device(config-host-10.24.65.6/mgmt-vrf)# tacacs-server source-ip chassis-ip
device(config-host-10.24.65.6/mgmt-vrf)# protocol chap retries 100
device(config-host-10.24.65.6/mgmt-vrf)#
```

This example modifies a TACACS+ server configuration.

```
device# configure terminal
device(config)# tacacs-server host 10.24.65.6
device(config-tacacs-server-10.24.65.6/mgmt-vrf))# key "changedsec"
```

This example deletes a TACACS+ server.

```
device# configure terminal
device(config)# no tacacs-server host 10.24.65.6
```

This example configures an IPv6 TACACS+ server

```
device# configure terminal
device(config)# tacacs-server host fec0:60:69bc:94:211:25ff:fec4:6010
device(config-tacacs-server-fec0:60:69bc:94:211:25ff:fec4:6010/mgmt-vrf)# protocol chap
key "mysecret"
device(config-tacacs-server-fec0:60:69bc:94:211:25ff:fec4:6010/mgmt-vrf)#  tacacs-server
source-ip chassis-ip
device(config-tacacs-server-fec0:60:69bc:94:211:25ff:fec4:6010/mgmt-vrf)#
```

tag-type

Configures Tag Protocol ID (TPID) for the specified interface.

Syntax

tag-type *tp-id*

no tag-type *tp-id*

Parameter:

tp-id

Specifies the TPID. TPID is a numerical value in hexadecimal format. Some of the TPIDs supported are `0x8100`, `0x9100`, `0x9200`, `0x88a8`.

Command Default

The default TPID value is 0x8100.

Modes

Interface configuration mode

Usage Guidelines

The interface can be a port or a port-channel (LAG).

Use the **no** form of the command to revert to the default TPID value.

The TPID feature has the following limitations:

- AVT profile limitation: Because of the limited number of AVT profiles (ingress and egress), the support for TPID configuration is available for the outer TPID of the packet without reducing the number of AVT profiles. When a packet is dual tagged, the inner TPID that is supported and recognized is TPID 0x8100.
- System maximum TPID: Hardware allows up to only four TPID configurations. The TPID can be any user-defined value. However, the inner TPID for a dual-tagged packet must be 0x8100, which means you can configure only three additional TPIDs in a system . TPID 0x8100 is the default value for all interfaces until you change it by means of the **tag-type** command.

  For the SLX 9740/Extreme 8820 series devices, only two (2) TPIDs are supported, which include the default TPID. Therefore, only one additional TPID is available for user configuration.
- LSP FRR limitation: Hardware support for LSP FRR is available only for TPID 0x8100. If you require a label switched path with fast reroute (LSP FRR) configuration, note that none of the routable interfaces (whether a router port or a LIF of a VE) can have

any nondefault TPID configuration, because FRR always assumes that the link layer has the default TPID of 0x8100.

Note
The LSP FRR limitation is for any tag-type configured in the device. You can configure either FRR or tag-type on any interface in the device, as in this example.

```
device(config-router-mpls-lsp-to-avalanche-1)# frr
%Error: Not allowed, when a non-default TPID (tag-type) is configured on any port-channel
or physical interfaces.
device(config-router-mpls-lsp-to-avalanche-1)#
```

Important
When the tag type is changed on interface, the interface is brought down first, causing all learned MAC addresses to be flushed.

Examples

This example shows how to configure a nondefault TPID on an Ethernet interface.

```
device# configure terminal
device(config)# inteface ethernet 1/1
device(conf-if-eth-1/1)# tag-type 0x9100
```

This example shows how to revert to the default TPID value.

```
device# configure terminal
device(config)# inteface ethernet 1/1
device(conf-if-eth-1/1)# no tag-type
```

This example shows how to configure a nondefault TPID on a port-channel interface.

```
device# configure terminal
device(config)# inteface port-channel 10
device(config-Port-channel-10)# tag-type 0x88a8
```

tdpa

Provisions the TPM chip on the SLX devices. This command cannot be executed and will always throw an error.

Syntax

tdpa { **provision** | **unit-test** | **dry-run** } **-i** < *ip-address* > **-p** < *port* > [**-v**]

Command Default

None.

Warning
This command cannot be executed once the TPM chip is provisioned. This command will always return an error message

Parameters

provision

Executing this command will display an error message

dry-run

Executing this command will display an error message

unit-test

Executing this command will display an error message

-i *ip-address*

Specifies the IPv4 address of the device being provisioned.

-p < *port* >

Specifies the port on the SLX device.

-v

Enables verbose logging

Modes

All modes

Usage Guidelines

This command will always throw an error when executed.

Examples

This example shows the error message that is displayed when this command is executed.

```
SLX#tdpa provision -i 10.1.1.1 -p 443
    TPM is already provisioned or TPM Ownership is locked
```

telemetry client-cert

Generates the SSL certificate used by Telemetry server and client for a secure connection.

Syntax

telemetry client-cert { **generate** | **delete** }

Command Default

There is no SSL certificate.

Parameters

generate

Generates the certificate

delete

Deletes the certificate.

Modes

Privileged EXEC mode

Usage Guidelines

Use the **telemetry client-cert delete** to delete the SSL certificate for Telemetry server and clients.

Examples

Typical command execution example.

```
device# telemetry client-cert generate
```

telemetry collector

Activates telemetry-collector configuration mode.

Syntax

telemetry collector *telemetry-collector*

Command Default

Telemetry collector configuration mode is deactivated.

Parameters

telemetry-collector

A unique name for a Telemetry collector. The name can be a string of up to 32 characters, consisting of letters, digits, and the underscore.

Modes

Global configuration mode

Usage Guidelines

Update operations are allowed only when telemetry collector is in deactivated (“no activate”) state.

Examples

Typical command example for activating Telemetry collector configuration mode.

```
device# configure terminal
device(config)# telemetry collector collector_1
device(config-telemetry-collector_collector_1)#
```

telemetry profile

Enters telemetry-profile configuration mode.

Syntax

telemetry profile enhanced-queue-discard-pkts
default_enhanced_queue_discard_pkts_statistics

telemetry profile enhanced-queue-max-queue-depth
default_enhanced_queue_max_queue_depth_statistics

telemetry profile interface default_interface_statistics

telemetry profile mpls-traffic-bypass
default_mpls_traffic_bypass_statistics

telemetry profile mpls-traffic-fec default_mpls_traffic_fec_statistics

telemetry profile mpls-traffic-lsp default_mpls_traffic_lsp_statistics

telemetry profile queue default_queue_statistics

telemetry profile system-utilization
default_system_utilization_statistics

Command Default

The Telemetry profile configuration mode is deactivated.

Parameters

enhanced-queue-discard-pkts
default_enhanced_queue_discard_pkts_statistics

(SLX 9540 and SLX 9640 devices) Accesses configuration mode for profile **default_enhanced_queue_discard_pkts_statistics** of the **enhanced-queue-discard-pkts** profile type. This profile tracks packets discarded in the 32 queues with the most discards.

enhanced-queue-max-queue-depth
default_enhanced_queue_max_queue_depth_statistics

(SLX 9540 and SLX 9640 devices) Accesses configuration mode for profile **default_enhanced_queue_max_queue_depth_statistics** of the **enhanced-queue-max-queue-depth** profile type. This profile tracks maximum queue size in the 32 queues with the largest queue size.

interface default_interface_statistics

Accesses configuration mode for profile **default_interface_statistics** of the **interface** profile type.

mpls-traffic-bypass default_mpls_traffic_bypass_statistics

(SLX 9540 and SLX 9640 devices) Accesses configuration mode for profile **default_mpls_traffic_bypass_statistics** of the **mpls-traffic-bypass** profile type.

mpls-traffic-fec default_mpls_traffic_fec_statistics

(SLX 9540 and SLX 9640 devices) Accesses configuration mode for profile **default_mpls_traffic_fec_statistics** of the **mpls-traffic-fec** profile type.

mpls-traffic-lsp default_mpls_traffic_lsp_statistics

(SLX 9540 and SLX 9640 devices) Accesses configuration mode for profile **default_mpls_traffic_lsp_statistics** of the **mpls-traffic-lsp** profile type.

queue default_queue_statistics

(SLX 9540 and SLX 9640 devices) Accesses configuration mode for profile **default_queue_statistics** of the **queue** profile type. This profile captures the overall queue statistics for the device.

system-utilization default_system_utilization_statistics

Accesses configuration mode for profile **default_system_utilization_statistics** of the **system-utilization** profile type.

Modes

Global configuration mode

Usage Guidelines

If a telemetry profile has no attributes, no information is streamed to the collector.

The **no** option is not supported for this command.

The interface statistics gathered by the default_interface_statistics profile are:

- In/Out packets
- In/Out unicast packets
- In/Out broadcast packets
- In/Out multicast packets
- In/Out packets per second
- In/Out octets
- In/Out errors
- In/Out CRC errors
- In/Out discards

The system utilization statistics gathered by the default_system_utilization_statistics profile are:

- Total system memory
- Total used memory
- Total free memory

- Cached memory
- Buffers
- User free memory
- Kernel free memory
- Total swap memory
- Total free swap memory
- Total used swap memory
- User process
- System process
- Niced process
- Io wait
- Hw interrupt
- Sw interrupt
- Idle state
- Steal time
- Uptime

The system utilization statistics gathered by the enhanced-queue-discard-pkts profile are:

- interval
- interface range
- discard pkts

The system utilization statistics gathered by the enhanced-queue-max-queue-depth profile are:

- interval
- interface range
- max-queue-depth

The statistics gathered by the queue profile are:

- interval
- enq-pkt-count
- enq-byte-count
- discard-pkt-count
- discard-byte-count
- current-queue-size
- max-queue-depth-size

Examples

Example of entering telemetry profile configuration mode.

```
device# configure terminal
device(config)# telemetry profile interface default_interface_statistics
device(config-interface-default_interface_statistics)#
```

telemetry profile (MPLS)

Enters Telemetry profile configuration mode for MPLS profile configurations.

Syntax

telemetry profile *profile-type telemetry-profile-name*

Command Default

The Telemetry profile configuration mode is not available until the **telemetry profile** command is entered.

Parameters

profile-type

The type of MPLS profile for the telemetry configuration. The available MPLS profile types are **mpls-traffic-lsp**, **mpls-traffic-bypass**, and **mpls-traffic-fec**.

telemetry-profile-name

The MPLS profile name. The available MPLS profile names are **default_mpls_traffic_lsp_statistics**, **default_mpls_traffic_bypass_statistics**, and **default_mpls_traffic_fec_statistics**.

Modes

Global configuration mode

Usage Guidelines

The MPLS profile types are supported only on SLX 9540 and SLX 9640 devices.

The "no" command is not supported for default telemetry profiles. Only the default telemetry profiles are supported. These profiles will contain all the streaming attributes supported. You can customize these profiles by adding or removing attributes using the **add** or **no add** sub command or by changing the interval using the **interval** sub command.

If a telemetry profile has no attributes, no information is streamed to the collector. The MPLS profile can be used for streaming after:

- Specifying the required MPLS LSP names for the mpls-traffic-lsp type profile using the **lsp** sub command.
- Specifying the required MPLS Bypass LSP names for the mpls-traffic-bypass type profile using the **bypass-lsp** sub command.

- Specifying the required MPLS LDP FEC addresses for the mpls-traffic-fec type profile using the **fec** sub command.

The statistics gathered by the MPLS profiles are:

- Out-packets
- Out-bytes

Examples

Example of entering telemetry profile configuration mode for an MPLS LSP configuration.

```
device(config)# telemetry profile mpls-traffic-lsp default_mpls_traffic_lsp_statistics
device(config-mpls-traffic-lsp-default_mpls_traffic_lsp_statistics)#
```

telemetry server

Enters telemetry-server configuration mode.

Syntax

telemetry server [**use-vrf** [*vrf-name*]]

Command Default

Telemetry-server configuration mode is deactivated.

Parameters

use-vrf *vrf-name*

Specifies a VRF, rather than the default mgmt-vrf.

Modes

Global configuration mode

Usage Guidelines

You use this command to configure gRPC-server telemetry streaming.

Update and No operations are available only when telemetry server is in deactivated (“no activate”) state.

Examples

The following example enters telemetry-server configuration mode and activates the internal gRPC telemetry-server on the default port 50051.

```
device# configure terminal
device(config)# telemetry server
device(config-server-mgmt-vrf)# activate
```

telnet

Establishes a Telnet session to a remote networking device.

Syntax

telnet *IP_address* [**port-number** *port_number*] [**vrf** *name*]

telnet *hostname* } [**port-number** *port_number*] [**interface** { **ethernet** *slot/port* } | **management** | {**ve** *number* }] [**vrf** *name*]

Command Default

The default port is 23.

Parameters

IP_address

The server IP address in either IPv4 or IPv6 format.

port-number *port*

Specifies the port number in the remote device to connect to. Range is from 0 through 65535. For the connection to succeed, a TCP server must be listening for client connections at the specified port.

vrf *vrf-name*

Specifies a VRF instance. See the Usage Guidelines.

hostname

Specifies the host name which is a string between 1 and 63 ASCII characters in length.

port-number *port*

Specifies the port number in the remote device to connect to. Range is from 0 through 65535. For the connection to succeed, a TCP server must be listening for client connections at the specified port.

interface

Specifies an interface.

ethernet *slot/port*

Specified the Ethernet interface slot and port number.

management

Specifies the management interface.

ve *VE-id*

Specifies the VE interface number.

Modes

Privileged EXEC mode

Usage Guidelines

You can override the default port. However, the device must be listening on this port for the connection to succeed.

The following features are not supported:

- Display Telnet sessions
- Ability to terminate hung Telnet sessions

Examples

The following example establishes a Telnet connection to a remote device.

```
device# telnet 10.20.51.68 vrf mgmt-vrf
```

telnet server

Configures the Telnet server on the device.

Syntax

telnet server use-vrf *name* [**shutdown**]

no telnet server use-vrf *name* [**shutdown**]

Command Default

The Telnet service is enabled by default.

Parameters

use-vrf *name*

Specifies a user-defined VRF.

shutdown

Disables the Telnet server.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of the command to re-enable the Telnet service on the device.

Shutting down the Telnet service forcibly disconnects all Telnet sessions running on a device.

Telnet services are associated and started on mgmt-vrf and default-vrf.

Telnet server can be enabled on a maximum number of 32 VRFs.

Examples

The following example shuts down the Telnet server on the default VRF.

```
device# configure terminal
device(config)# telnet server use-vrf default-vrf shutdown
```

terminal

Sets terminal parameters for the current session.

Syntax

terminal length *lines*

terminal monitor

terminal no length

terminal timeout *seconds*

no terminal { **monitor** | **timeout** }

Command Default

The terminal length is 24 lines.

The terminal timeout is 600 seconds (10 minutes).

Parameters

length *number_of_lines*

Specifies the number of lines to be displayed. Valid values range from 1 through 512. Specify 0 for infinite length.

monitor

Enables terminal monitoring.

timeout *seconds*

Specifies the timeout value in minutes. Enter an integer from 1 to 8192. Specify 0 to disable the timeout.

Modes

Privileged EXEC mode

Usage Guidelines

The **timeout** overrides the timeout configuration set by the **line vty exec-timeout** command, but only for the duration of the current session. When the current session ends, the configured values apply for any subsequent sessions.

Even if other keys are pressed during the timeout period, the only keystroke that prevents logout is **Enter**.

To reset the default timeout, use the **no terminal timeout** command.

To disable monitoring, use the **no terminal monitor** command.

To reset the default number of displayed lines, use the **terminal no length** command.

Examples

The following example sets the display length to 30 lines.

```
device# terminal length 30
```

The following example sets timeout length to 3600 seconds (60 minutes).

```
device# terminal timeout 3600
```

The following example restores the session timeout setting its default value of 600 seconds (10 minutes).

```
device# no terminal timeout
```

test-profile

Creates a test profile.

Syntax

test-profile *test-profile-name*

no test-profile

Parameters

test-profile-name

Specifies the test profile name. A test profile name can be can be a maximum of 32 characters .

Command Default

This feature is disabled.

Modes

Y.1731 configuration mode

Usage Guidelines

Use the **no** form of the command to delete the corresponding configured test profile and also its associations with Source and Target MEP pair.

Examples

This example shows how to create a test profile .

```
device# configure terminal
device(config)# protocol cfm
device((protocol-cfm)# test-profile my_test_profile
```

threshold

Specifies if the measurement exceeds the configured average or max threshold value.

Syntax

threshold { **forward** | **backward** } | { **average** *value* | **max** *value* }

no threshold

Parameters

forward

Defines the forward direction.

backward

Defines the backward direction.

average *value*

Defines the average value.

max *value*

Defines the maximum value.

Modes

Y.1731 configuration mode

Usage Guidelines

The **threshold** command specifies if the measurement exceeds the configured average or max threshold value in the backward or forward direction, then Syslogs or SNMP traps need to generated..

The **average-threshold** parameter specifies that when the average-threshold value in the applied profile is exceeded, take actions as configured in the action profile for this event.

The **max-threshold** parameter specifies that when the max-threshold value in the applied profile is exceeded, take actions as configured in the action profile for this event.

Examples

Example of setting the direction and average threshold.

```
device# configure terminal
device(config)# protocol cfm
device(protocol-cfm)# y1731
device(protocol-cfm-y1731)# test-profile my_test_profile
device(protocol-cfm-y1731-my_test_profile)# threshold backward
```

```
device(protocol-cfm-y1731-my_test_profile)# threshold average 25
device(protocol-cfm-y1731-my_test_profile)# exit
```

threshold (ETH-DM)

Configures the ETH-DM threshold.

Syntax

threshold [**average** *average-threshold* | **maximum** *maximum-threshold*]

no threshold [**average** *average-threshold* | **maximum** *maximum-threshold*]

Parameters:

average *average-threshold*

Specifies the average threshold. The valid value is from 1 to 4294967295.

maximum *maximum-thershold*

Specifies the maximum threshold. The valid value is from 1 to 4294967295.

Command Default

The default value for average threshold is 4294967295 uSec. The default value for maximum threshold is 4294967295 uSec.

Modes

Y1731 configuration mode

Usage Guidelines

Use the **no** form of the command to delete the threshold configuration.

Examples

This example shows how to configure the threshold value.

```
device# configure terminal
device (config-cfm)# protocol cfm
device (config-cfm)# y1731
device(config-cfm-y1731)# test-profile my_test_profile
device(config-cfm-y1731-test-profile-my_test_profile)# type delay-measurement
device(config-cfm-y1731-test-profile-my_test_profile)# tx-interval 60
device(config-cfm-y1731-test-profile-my_test_profile)# measurement-interval 30
device(config-cfm-y1731-test-profile-my_test_profile)# start at 00:00:00 daily
device(config-cfm-y1731-test-profile-my_test_profile)# stop at 23:59:00
device(config-cfm-y1731-test-profile-my_test_profile)# cos 7
device(config-cfm-y1731-test-profile-my_test_profile)# threshold maximum 3294967295
```

threshold (ETH-SLM)

Configures the ETH-SLM threshold.

Syntax

threshold { **backward** [**average** *average-value* | **maximum** *maximum-value*] | **forward** [**average** *average-value* | **maximum** *maximum-value*] }

no threshold { **backward** [**average** *average-value* | **maximum** *maximum-value*] | **forward** [**average** *average-value* | **maximum** *maximum-value*] }

Parameters:

backward

Specifies ETH-SLM backward threshold.

average *average-value*

Specifies the ETH-SLM backward average threshold value. The average value range is from 1 to 4294967295.

maximum *maximum value*

Specifies the ETH-SLM backward maximum threshold value. The average value range is from 1 to 4294967295.

forward

Specifies ETH-SLM forward threshold.

Command Default

The default value for average threshold is 4294967295 uSec. The default value for maximum threshold is 4294967295 uSec.

Modes

Y1731 configuration mode

Usage Guidelines

Use the **no** form of the command to delete the threshold configuration.

Examples

This example shows how to configure the threshold value.

```
device# configure terminal
device (config-cfm)# protocol cfm
device (config-cfm)# y1731
device(config-cfm-y1731)# test-profile my_test_profile
device(config-cfm-y1731-test-profile-my_test_profile)# type delay-measurement
device(config-cfm-y1731-test-profile-my_test_profile)# tx-interval 60
```

```
device(config-cfm-y1731-test-profile-my_test_profile)# measurement-interval 30
device(config-cfm-y1731-test-profile-my_test_profile)# start at 00:00:00 daily
device(config-cfm-y1731-test-profile-my_test_profile)# stop at 23:59:00
device(config-cfm-y1731-test-profile-my_test_profile)# cos 7
device(config-cfm-y1731-test-profile-my_test_profile)# threshold forward maximum
3294967295
```

threshold-monitor

Syntax

```
threshold-monitor [ acl | Cpu | Memory | bfd-session | ecmp | hardware-
   resources | host | lif | mac-table | nexthop | route | sfp | vxlan-
   tunnel ]
```

Parameters

acl

Configures the threshold monitor settings for the various ACL resources.

Cpu

Configures the threshold monitoring settings for the CPU.

Memory

Configures the threshold monitoring settings for the Memory.

bfd-session

Configures monitoring settings for monitoring BFD session scale.

ecmp

Configures monitoring settings for monitoring Layer 3 ECMP table utilization.

hardware-resources

Configures monitoring settings for monitoring hardware resources.

host

Configures monitoring settings for monitoring Layer 3 host table utilization.

lif

Configures monitoring settings for monitoring LIF scale.

mac-table

Configures monitoring settings for monitoring MAC table utilization.

nexthop

Configures monitoring settings for monitoring Layer 3 next hop table utilization.

route

Configures monitoring settings for monitoring Layer 3 Route table utilization.

sfp

Configures monitoring settings to monitor SFP class.

vxlan-tunnel

Configures monitoring settings for monitoring VXLAN Tunnel scale.

Modes

Privilege Execution Mode

Usage Guidelines

None

Examples

The following example lists all the available options for the **threshold-monitor** command.

```
SLX# configure terminal
SLX (config)# threshold-monitor ?

Possible completions:
  Cpu                  Configure settings for component:CPU
  Memory               Configure settings for component:MEMORY
  acl                  Settings for monitoring ACLs
  bfd-session          Configure settings to monitor BFD session scale
  ecmp                 Configure settings to monitor L3 ECMP table utilization
  hardware-resources   Common settings for monitoring hardware resources
  host                 Configure settings to monitor L3 Host table utilization
  lif                  Configure settings to monitor LIF scale
  mac-table            Configure settings to monitor MAC table utilization
  nexthop              Configure settings to monitor L3 Next Hop table
                       utilization
  route                Configure settings to monitor L3 Route table utilization
  sfp                  Monitor SFP class
  vxlan-tunnel         Configure settings to monitor VXLAN tunnel scale
```

threshold-monitor acl

Configures monitoring the utilization of finite user configurable ACL resources like MAC ACL, IP ACL, and IPv6 ACL. The current values of ternary content-addressable memory (TCAM) occupied by these ACLs are compared against the available hardware resources in a configured hardware profile. An alarm is raised every time the consumed resources crosses the configured high threshold level indicating a high utilization and also when, the utilization, subsequently, falls below the configured low threshold limit, indicating that the utilization has reached safer levels.
The alarm for low threshold is generated only in the case that an alarm for crossing the high threshold is already generated.

Syntax

threshold monitor acl [**mac-in** | **mac-out** | **ip-in** | **ip-out** | **ipv6-in** | **ipv6-out**]

threshold-monitor acl ip-in { [**high-limit** *value-in-percentage* | **low-limit** *value-in-percentage* | [**actions** [**all** | **none** | **raslog** | **snmp**]]] }

threshold-monitor acl ip-out { [**high-limit** *value-in-percentage* | **low-limit** *value-in-percentage* | [**actions** [**all** | **none** | **raslog** | **snmp**]]] }

threshold-monitor acl ipv6-in { [**high-limit** *value-in-percentage* | **low-limit** *value-in-percentage* | [**actions** [**all** | **none** | **raslog** | **snmp**]]] }

threshold-monitor acl ipv6-out { [**high-limit** *value-in-percentage* | **low-limit** *value-in-percentage* | [**actions** [**all** | **none** | **raslog** | **snmp**]]] }

threshold-monitor acl mac-in { [**high-limit** *value-in-percentage* | **low-limit** *value-in-percentage* | [**actions** [**all** | **none** | **raslog** | **snmp**]]] }

threshold-monitor acl mac-out { [**high-limit** *value-in-percentage* | **low-limit** *value-in-percentage* | [**actions** [**all** | **none** | **raslog** | **snmp**]]] }

no threshold-monitor acl ip-in { **high-limit** | **low-limit** | **actions** }

no threshold-monitor acl ip-out { **high-limit** | **low-limit** | **actions** }

no threshold-monitor acl ipv6-in { **high-limit** | **low-limit** | **actions** }

no threshold-monitor acl ipv6-out { **high-limit** | **low-limit** | **actions** }

no threshold-monitor acl mac-in { **high-limit** | **low-limit** | **actions** }

no threshold-monitor acl mac-out { **high-limit** | **low-limit** | **actions** }

Parameters

high-limit *value-in-percentage*

Specifies the high usage limit as a percentage (%) of available TCAM resources that will trigger the configured action. The range is 10%-100%. The default value is 90%.

low-limit *value-in-percentage*

Specifies the low usage limit as a percentage (%) of available TCAM resources that will trigger the configured action. The range is 10%-99%. The default value is 70%.

actions

Specifies the action to be taken when a threshold is crossed. The values supported are `all`, `none`, `raslog`, and `snmp`. Default action is `all`.

all

RASLOG and SNMP trap will be sent when the threshold is crossed. This is the default configuration.

none

No action will be taken when the threshold is crossed.

raslog

Only RASLOG will be sent when the threshold is crossed.

snmp

Only SNMP traps will be sent when the threshold is crossed.

Modes

Global Configuration Mode

Usage Guidelines

The **no** form of this command will reset the values to default.

The **low-limit** threshold value cannot be equal to or higher than the value configured for the **high-limit** threshold value.

Monitoring of IPv6 Egress ACL is only supported on SLX 9740 and Extreme 8820. It is supported through a new TCAM profile **ipv6-optimised**.

Examples

The following example configures the lower and higher threshold monitoring values for the IPv4 Ingress utilization.

```
SLX# configure terminal
SLX (config)# threshold-monitor acl ip-in high-limit 95 low-limit 50 action all
SLX (config)#
```

The following example resets the configured ACL IPv4 ingress utilization threshold monitoring values to their defaults.

```
 SLX# configure terminal
SLX (config)# no threshold-monitor acl ip-in high-limit
```

```
SLX (config)# no threshold-monitor acl ip-in low-limit
SLX (config)# no threshold-monitor acl ip-in action
```

threshold-monitor Cpu

Configures monitoring of CPU usage of the system and alerts the user when configured thresholds are exceeded.

Syntax

threshold-monitor Cpu { [**limit** *value-in-percentage* | **poll** *polling-interval* | **retry** *retry-interval* | [**actions** [**all** | **loginfo** | **none** | **raslog** | **snmp**]]] }

no threshold-monitor cpu

Parameters

actions

Specifies the action to be taken when a threshold is exceeded. The values supported are `all`, `loginfo`, `none`, `raslog`, and `snmp`. The default action is `all`.

all

RASLOG and SNMP trap will be sent when the threshold is exceeded.

loginfo

Additional diagnostics data will be collected along with RASLOG when the threshold is exceeded.

none

No action will be taken when the threshold is exceeded.

raslog

Only RASLOG will be sent when the threshold is exceeded.

snmp

Only SNMP traps will be sent when the threshold is exceeded.

limit *value-in-percentage*

Specifies the baseline CPU usage limit as a percentage (%) of available resources that will trigger the configured action. The range is 0%-95%. The default value is 50%.

poll *polling-interval*

Specifies the polling interval in seconds after which a sample will be taken. The range is 10-3600 seconds. The default interval is 120 seconds.

retry *retry-interval*

Specifies the number polling retries that will be attempted before desired action is taken. The range is 1-100. The default retries is 3.

Modes

Global configuration mode

Usage Guidelines

The default `action` is *all*. Prior to SLX-OS version 20.4.1, the default value was *none*.

Examples

```
SLX(config)# threshold-monitor Cpu ?
Possible completions:
  actions   Action to be taken when usage exceeds limit
  limit     PERCENT:0-95 Percent threshold usage for component:CPU
  poll      NUMBER:10-3600 Polling interval
  retry     NUMBER:1-100 Number of retries
SLX(config)#
```

This example details on threshold-monitor CPU actions.

```
SLX(config)# threshold-monitor Cpu actions ?
Possible completions:
  [none]
  all       RASLOG and SNMP trap will be sent
  loginfo   Diagnostic data collection along with RASLOG
  none      No action will be taken
  raslog    RASLOG will be sent
  snmp      SNMP trap will be sent
SLX(config)#
```

threshold-monitor memory

Configures monitoring of the memory usage of the system and alerts the user when configured thresholds are exceeded.

Syntax

threshold-monitor Memory { [**high-limit** *value-in-percentage* | **poll** *polling-interval* | **retry** *retry-interval* | [**actions** [**all** | **loginfo** | **none** | **raslog** | **snmp**]]] }

no threshold-monitor Memory

Parameters

actions

Specifies the action to be taken when a threshold is exceeded. The values supported are `all`, `loginfo`, `none`, `raslog`, and `snmp`. The default action is `all`.

all

RASLOG and SNMP trap will be sent when the threshold is exceeded.

loginfo

Additional diagnostics data will be collected along with RASLOG when the threshold is exceeded.

none

No action will be taken when the threshold is exceeded.

raslog

Only RASLOG will be sent when the threshold is exceeded.

snmp

Only SNMP traps will be sent when the threshold is exceeded.

high-limit *value-in-percentage*

Specifies the high usage limit as a percentage (%) of available memory that will trigger the configured action. The range is 0%-95%. The default value is 70%.

poll *polling-interval*

Specifies the polling interval in seconds after which a sample will be taken. The range is 10-3600 seconds. The default interval is 120 seconds.

retry *retry-interval*

Specifies the number polling retries that will be attempted before desired action is taken. The range is 1-100. The default retries is 3.

Modes

Global configuration mode

Usage Guidelines

None

Examples

```
SLX(config)# threshold-monitor Memory ?
Possible completions:
  actions      Action to be taken when usage exceeds limit
  high-limit   PERCENT:0-95: Percent high threshold usage for component:MEMORY
  poll         NUMBER:10-3600: Polling interval
  retry        NUMBER:0-100: Number of retries for component:MEMORY

SLX(config)#
```

This example displays threshold-monitor Memory actions

```
SLX(config)# threshold-monitor Memory actions
Possible completions:
  [none]
  all       RASLOG and SNMP trap will be sent
  none      No action will be taken
  raslog    RASLOG will be sent
  snmp      SNMP trap will be sent
SLX(config)#
```

threshold-monitor bfd-sessions

Configures monitoring of the number of BFD Session against the maximum number of supported BFD sessions and alerts the user when configured thresholds are exceeded.

Syntax

threshold-monitor bfd-sessions [**high-limit** *value-in-percent*] [**low-limit** *value-in-percent*] [**actions** [*none* | *raslog* | *snmp* | *all*]]

no threshold-monitor bfd-sessions

Parameters

actions [*none* | *raslog* | *snmp* | *all*]

Specifies the action to be taken when a threshold is exceeded. The values supported are `all`, `none`, `raslog`, and `snmp`. Default is `all`.

all

RASLOG and SNMP trap will be sent when the threshold is exceeded.

none

No action will be taken when the threshold is exceeded.

raslog

Only RASLOG will be sent when the threshold is exceeded.

snmp

Only SNMP traps will be sent when the threshold is exceeded.

high-limit *value-in-percentage*

Specifies the upper threshold limit of BFD sessions as a percentage (%) that will trigger the configured action. The range is 10%-100%. The default value is 90%.

low-limit *value-in-percentage*

Specifies the lower threshold limit of BFD sessions as a percentage (%) that will trigger the configured action. The range is 10%-99%. The default value is 70%.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command will reset the values to default.

The **low-limit** threshold value cannot be equal to or higher than the value configured for the **high-limit** threshold value.

Examples

The following example configures the lower and higher threshold monitoring values for the BFD sessions.

```
SLX# configure terminal
SLX (config)# threshold-monitor bfd high-limit 95 low-limit 50 action all
SLX (config)#
```

The following example resets the configured BFD session threshold monitoring values to their defaults.

```
SLX# configure terminal
SLX (config)# no threshold-monitor bfd high-limit
SLX (config)# no threshold-monitor bfd low-limit
SLX (config)# no threshold-monitor bfd action
```

threshold-monitor ecmp

Configures monitoring the utilization of the ECMP Table. The current values of number of ECMP Next Hop entries (in %) is compared with the configured profile limits and against the available hardware space. An alarm is raised when the number of entries falls below the configured low threshold or exceeds the configured high threshold.

Syntax

threshold-monitor ecmp { [**high-limit** *value-in-percentage* | **low-limit** *value-in-percentage* | [**actions** [**all** | **none** | **raslog** | **snmp**]]] }

no threshold-monitor ecmp { **high-limit** | **low-limit** | **actions** }

Parameters

high-limit *value-in-percentage*

Specifies the high usage limit as a percentage (%) of available ECMP table resources that will trigger the configured action. The range is 10%-100%. The default value is 90%.

low-limit *value-in-percentage*

Specifies the low usage limit as a percentage (%) of available ECMP table resources that will trigger the configured action. The range is 10%-99%. The default value is 70%.

actions

Specifies the action to be taken when a threshold is exceeded. The values supported are `all`, `none`, `raslog`, and `snmp`. The default action is `all`.

all

RASLOG and SNMP trap will be sent when the threshold is exceeded. This is the default configuration.

none

No action will be taken when the threshold is exceeded.

raslog

Only RASLOG will be sent when the threshold is exceeded.

snmp

Only SNMP traps will be sent when the threshold is exceeded.

Modes

Global Configuration Mode

Usage Guidelines

The **no** form of this command will reset the values to default.

The **low-limit** threshold value cannot be equal to or higher than the value configured for the **high-limit** threshold value.

For hardware tables that share space, it is possible to run out of free space even when the number of ECMP Next Hop entries has not reached its configured maximum. Once the hardware space runs out, addition of new entries will be affected.

Examples

The following example configures the lower and higher threshold monitoring values for ECMP Table.

```
SLX# configure terminal
SLX (config)# threshold-monitor ecmp high-limit 95 low-limit 50 action all
SLX (config)#
```

The following example resets the configured ECMP table threshold monitoring values to their defaults

```
 SLX# configure terminal
SLX (config)# no threshold-monitor ecmp high-limit
SLX (config)# no threshold-monitor ecmp low-limit
SLX (config)# no threshold-monitor ecmp action
```

threshold-monitor hardware-resources

Configures the maximum number of events to be generated in a configured time period for any hardware events on the device.

Syntax

threshold-monitor hardware-resources [**count** *max-number-of-generated-events* | **interval** *interval-in-seconds*]

no threshold-monitor hardware-resources [**count** | **interval**]

Parameters

count *max-number-of-generated-events*

Configures the maximum number of events that are generated for the configured time interval. The range is 1-60 events. The default is 4 events.

interval *interval-in-seconds*

Specifies the time interval during which events are generated. The range is 30-900 seconds. The default value is 30 seconds.

Modes

Global Configuration Mode

Usage Guidelines

The **no** form of this command will reset the values to default.

The default values of 4 and 30 indicate that up to 4 messages will be generated every 30 seconds.

Use this configuration to rate limit the generation of messages. Please note that RASLOGs are generated per resource and SNMP notifications are generated for the set of all hardware resources. This configuration controls the number of RASLOGs/SNMP Notifications generated within the specified time interval.

Examples

The following example configures the number of events that are generated for a particular time interval. This configures a rate limit of 30 events per 45 seconds.

```
SLX# configure terminal
SLX (config)# threshold-monitor hardware-resources count 30 interval 45
SLX (config)#
```

The following example resets the configured hardware-resource message generation rate limit values to their defaults.

```
 SLX# configure terminal
SLX (config)# no threshold-monitor hardware-resources count
SLX (config)# no threshold-monitor hardware-resources interval
```

threshold-monitor host

Configures monitoring of the utilization of the Host Table. The current values of number of host entries (in %) (both IPv4 ARP entries and IPv6 Neighbor entries) are compared with the configured profile limits and against the available hardware space. An alarm is raised when the number of entries falls below the configured low threshold or exceeds the configured high threshold.

Syntax

threshold-monitor host { [**high-limit** *value-in-percentage* | **low-limit** *value-in-percentage* | [**actions** [**all** | **none** | **raslog** | **snmp**]]] }

no threshold-monitor host { **high-limit** | **low-limit** | **actions** }

Parameters

high-limit *value-in-percentage*

Specifies the high usage limit as a percentage (%) of available Host table resources that will trigger the configured action. The range is 10%-100%. The default value is 90%.

low-limit *value-in-percentage*

Specifies the low usage limit as a percentage (%) of available Host table resources that will trigger the configured action. The range is 10%-99%. The default value is 70%.

actions

Specifies the action to be taken when a threshold is exceeded. The values supported are `all`, `none`, `raslog`, and `snmp`. The default action is `all`.

all

RASLOG and SNMP trap will be sent when the threshold is exceeded. This is the default configuration.

none

No action will be taken when the threshold is exceeded.

raslog

Only RASLOG will be sent when the threshold is exceeded.

snmp

Only SNMP traps will be sent when the threshold is exceeded.

Modes

Global Configuration Mode

Usage Guidelines

The **no** form of this command will reset the values to default.

The **low-limit** threshold value cannot be equal to or higher than the value configured for the **high-limit** threshold value.

For hardware tables that share space, it is possible to run out of free space even when the IPv4 or IPv6 routes have not individually reached their configured maximum. Once the shared hardware space runs out, addition of new hosts will be affected.

Supported In

Examples

The following example configures the lower and higher threshold monitoring values for the Host table.

```
SLX# configure terminal
SLX (config)# threshold-monitor host high-limit 95 low-limit 50 action all
SLX (config)#
```

The following example resets the configured Host table threshold monitoring values to their defaults

```
 SLX# configure terminal
SLX (config)# no threshold-monitor host high-limit
SLX (config)# no threshold-monitor host low-limit
SLX (config)# no threshold-monitor host action
```

threshold-monitor lif

Configures monitoring of the number of LIFs against the maximum number of supported LIFs and alerts the user when configured thresholds are exceeded.

Syntax

threshold-monitor lif [**high-limit** *value-in-percent*] [**low-limit** *value-in-percent*] [**action** [*none* | *raslog* | *snmp* | *all*]]

no threshold-monitor lif [**high-limit** | **low-limit** | **action**]

Parameters

high-limit *value-in-percentage*

Specifies the upper threshold limit for number of LIFs as a percentage (%) that will trigger the configured action. The range is 10%-100%. The default value is 90%.

low-limit *value-in-percentage*

Specifies the lower threshold limit for number of LIFs as a percentage (%) that will trigger the configured action. The range is 10%-99%. The default value is 70%.

action [*none* | *raslog* | *snmp* | *all*]

Specifies the action to be taken when a threshold is exceeded. The values supported are `all`, `none`, `raslog`, and `snmp`. Default is `all`.

all

RASLOG and SNMP trap will be sent when the threshold is exceeded.

none

No action will be taken when the threshold is exceeded.

raslog

Only RASLOG will be sent when the threshold is exceeded.

snmp

Only SNMP traps will be sent when the threshold is exceeded.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command will reset the values to default.

The **low-limit** threshold value cannot be equal to or higher than the value configured for the **high-limit** threshold value.

Examples

The following example configures the lower and higher threshold monitoring values for the number of LIFs.

```
SLX# configure terminal
SLX (config)# threshold-monitor lif high-limit 95 low-limit 50 action all
SLX (config)#
```

The following example resets the configured LIFs threshold monitoring values to their defaults.

```
SLX# configure terminal
SLX (config)# no threshold-monitor lif high-limit
SLX (config)# no threshold-monitor lif low-limit
SLX (config)# no threshold-monitor lif action
```

threshold-monitor mac-table

Configures monitoring of the utilization of available MAC Table resources and alerts the user when configured thresholds are exceeded.

Syntax

threshold-monitor mac-table [**high-limit** *value-in-percent*] [**low-limit** *value-in-percent*] [**actions** [*none* | *raslog* | *snmp* | *all*]]

no threshold-monitor mac-table [**high-limit** | **low-limit** | **action**]

Parameters

high-limit *value-in-percentage*

Specifies the upper threshold limit of MAC Table utilization as a percentage (%) that will trigger the configured action. The range is 10%-100%. The default value is 70%.

low-limit *value-in-percentage*

Specifies the lower threshold limit of MAC Table utilization as a percentage (%) that will trigger the configured action. The range is 10%-99%. The default value is 50%.

actions [*none* | *raslog* | *snmp* | *all*]

Specifies the action to be taken when a threshold is exceeded. The values supported are `all`, `none`, `raslog`, and `snmp`. Default "`action`" is "`all`".

all

RASLOG and SNMP trap will be sent when the threshold is exceeded.

none

No action will be taken when the threshold is exceeded.

raslog

Only RASLOG will be sent when the threshold is exceeded.

snmp

Only SNMP traps will be sent when the threshold is exceeded.

Modes

Global configuration mode

Usage Guidelines

The **no** form of this command will reset the values to default.

The **low-limit** threshold value cannot be equal to or higher than the value configured for the **high-limit** threshold value.

Examples

The following example configures the lower and higher threshold monitoring values for the entries in the MAC Table.

```
SLX# configure terminal
SLX (config)# threshold-monitor mac-table high-limit 95 low-limit 50 action all
SLX (config)#
```

The following example resets the configured MAC table entries threshold monitoring values to their defaults.

```
SLX# configure terminal
SLX (config)# no threshold-monitor mac-table high-limit
SLX (config)# no threshold-monitor mac-table low-limit
SLX (config)# no threshold-monitor mac-table action
```

threshold-monitor nexthop

Configures the monitoring the utilization of the Next Hop Table or the Encap Table depending on the platform. The current values of number of next hop entries (in %) is compared with the configured profile limits and against the available hardware space. An alarm is raised when the number of next hop entries falls below the configured low threshold or exceeds the configured high threshold.

Syntax

threshold-monitor nexthop { [**high-limit** *value-in-percentage* | **low-limit** *value-in-percentage* | [**actions** [**all** | **none** | **raslog** | **snmp**]]] }

no threshold-monitor nexthop { **high-limit** | **low-limit** | **actions** }

Parameters

high-limit *value-in-percentage*

Specifies the high usage limit as a percentage (%) of available Next Hop table resources that will trigger the configured action. The range is 10%-100%. The default value is 90%.

low-limit *value-in-percentage*

Specifies the low usage limit as a percentage (%) of available Next Hop table resources that will trigger the configured action. The range is 10%-99%. The default value is 70%.

actions

Specifies the action to be taken when a threshold is exceeded. The values supported are `all`, `none`, `raslog`, and `snmp`. The default action is `all`.

all

RASLOG and SNMP trap will be sent when the threshold is exceeded. This is the default configuration.

none

No action will be taken when the threshold is exceeded.

raslog

Only RASLOG will be sent when the threshold is exceeded.

snmp

Only SNMP traps will be sent when the threshold is exceeded.

Modes

Global Configuration Mode

Usage Guidelines

The **no** form of this command will reset the values to default.

The **low-limit** threshold value cannot be equal to or higher than the value configured for the **high-limit** threshold value.

For the hardware tables that share space, it is possible to run out of free space even when the number of next hop entires has not reached its configured maximum. Once the shared hardware space runs out, addition of new IPv4 Route/IPv6 Route/ARP/ Neighbor Discovery/Nexthop entries will be affected.

Examples

The following example configures the lower and higher threshold monitoring values for the Next Hop table.

```
SLX# configure terminal
SLX (config)# threshold-monitor nexthop high-limit 95 low-limit 50 action all
SLX (config)#
```

The following example resets the configured Next Hop table threshold monitoring values to their defaults

```
 SLX# configure terminal
SLX (config)# no threshold-monitor nexthop high-limit
SLX (config)# no threshold-monitor nexthop low-limit
SLX (config)# no threshold-monitor nexthop action
```

threshold-monitor route

Configures monitoring the utilization of the Route Table. The current values of number of routes (in %) (both IPv4 and IPv6 routes) are compared with the configured profile limits and against the available hardware space. An alarm is raised when the number of routes falls below the configured low threshold or exceeds the configured high threshold.

Syntax

threshold-monitor route { [**high-limit** *value-in-percentage* | **low-limit** *value-in-percentage* | [**actions** [**all** | **none** | **raslog** | **snmp**]]] }

no threshold-monitor route { **high-limit** | **low-limit** | **actions** }

Parameters

high-limit *value-in-percentage*

Specifies the high usage limit as a percentage (%) of available Route table resources that will trigger the configured action. The range is 10%-100%. The default value is 90%.

low-limit *value-in-percentage*

Specifies the low usage limit as a percentage (%) of available Route table resources that will trigger the configured action. The range is 10%-99%. The default value is 70%.

actions

Specifies the action to be taken when a threshold is exceeded. The values supported are `all`, `none`, `raslog`, and `snmp`. Default action is `all`.

all

RASLOG and SNMP trap will be sent when the threshold is exceeded. This is the default configuration.

none

No action will be taken when the threshold is exceeded.

raslog

Only RASLOG will be sent when the threshold is exceeded.

snmp

Only SNMP traps will be sent when the threshold is exceeded.

Modes

Global Configuration Mode

Usage Guidelines

The **no** form of this command will reset the values to default.

The **low-limit** threshold value cannot be equal to or higher than the value configured for the **high-limit** threshold value.

For hardware tables, it is possible to run out of free space even when the IPv4 or IPv6 routes have not reached their configured maximum. Once the hardware space runs out, addition of new routes will be affected.

Examples

The following example configures the lower and higher threshold monitoring values for the Route table utilization.

```
SLX# configure terminal
SLX (config)# threshold-monitor route high-limit 95 low-limit 50 action all
SLX (config)#
```

The following example resets the configured Route table utilization threshold monitoring values to their defaults.

```
 SLX# configure terminal
SLX (config)# no threshold-monitor route high-limit
SLX (config)# no threshold-monitor route low-limit
SLX (config)# no threshold-monitor route action
```

threshold-monitor sfp

Configures monitoring of SFP parameters.

Syntax

threshold-monitor sfp [**apply** | **pause** | **policy**]

threshold-monitor sfp apply *policy-name*

threshold-monitor sfp pause

threshold-monitor sfp policy *policy-name* **type** { **1GCOP** | **1GCWDM** | **1GLHA** | **1GLR** | **1GSR** | **10GDWDMT** | **10GER** | **10GLR** | **10GSR** | **10GUSR** | **10GZR** | **40GER** | **40GESR** | **40GLM** | **40GLR** | **40GSR** | **40GSRINT** | **100GAOC** | **100GCLR** | **100GCWDM** | **100GESR** | **100GLR** | **100GLRLT** | **100GPSM** | **100GSR** } **area** { **Current** | **RXP** | **TXP** | **Temperature** | **Voltage** } **threshold** { **buffer** *buffer-threshold-value* | **high-threshold** *high-threshold-value* | **low-threshold** *low-threshold-value* }

threshold-monitor sfp policy *policy-name* **type** { **1GCOP** | **1GCWDM** | **1GLHA** | **1GLR** | **1GSR** | **10GDWDMT** | **10GER** | **10GLR** | **10GSR** | **10GUSR** | **10GZR** | **40GER** | **40GESR** | **40GLM** | **40GLR** | **40GSR** | **40GSRINT** | **100GAOC** | **100GCLR** | **100GCWDM** | **100GESR** | **100GLR** | **100GLRLT** | **100GPSM** | **100GSR** } **area** { **Current** | **RXP** | **TXP** | **Temperature** | **Voltage** } **alert** { [**above** **highthreshold-action** [**all** | **email** | **none** | **raslog**]] | [**below** [**highthreshold-action** | **lowthreshold-action**] [**all** | **email** | **none** | **raslog**] }

no threshold-monitor sfp policy *policy-name*

Parameters

apply *policy-name*

Applies a SFP policy created by the **threshold-monitor sfp policy threshold** command. The policy-name is always *custom*.

pause

Pauses the enforcement of the currently applied SFP policy.

policy custom

Creates a custom SFP policy with the provided *policy-name* value. This policy can then be applied using the **threshold-monitor sfp apply** command. This policy-name should always be *custom*. You cannot assign an arbitrary name for the SFP policy.

type

Specifies the SFP type. Possible configurations are:

1GCOP

SFP type 1G SFP Copper

1GCWDM

SFP type 1G CWDM

1GLHA

1G SFP LHA

1GLR

1G SFP LR

1GSR

1G SFP SR

10GDWDMT

10G SFP+ DWDM Tunable

10GER

10G SFP+ ER

10GLR

10G SFP+ LR

10GSR

10G SFP+ SR

10GUSR

10G SFP+ USR

10GZR

10G SFP+ ZR

40GER

40G QSFP+ ER4

40GESR

40G QSFP+ eSR4

40GLM

40G QSFP+ LM4

40GLR

40G QSFP+ LR4

40GSR

40G QSFP+ SR4

40GSRINT

40G QSFP+ SR4 INT

100GAOC

100G QSFP28 AOC

100GCLR

100G QSFP28 CLR4

100GCWDM

100G QSFP28 CWDM4

100GESR

100G QSFP28 eSR4

100GLR

100G QSFP28 LR4

100GLRLT

100G QSFP28 LR4 Lite

100GPSM

100G QSFP28 PSM4

100GSR

100G QSFP28 SR4

area [**Current** | **RXP** | **TXP** | **Temperature** | **Voltage**]

Specifies the SFP parameter to be measured.

Current

Measures the current supplied to the SFP transceiver.

RXP

Measures the incoming laser power, in microWatts (µW).

TXP

Measures the outgoing laser power, in microWatts (µW).

Temperature

Measures the temperature of the SFP, in degrees Celsius.

Voltage

Measures the voltage supplied to the SFP.

threshold

Configures the threshold value for this SFP profile. Can be one or more of:

buffer *buffer-threshold-value*

Configures the Buffer threshold value.

high-threshold *high-threshold-value*

Configures the high threshold value.

low-threshold *low-threshold-value*

Configures the low threshold value.

highthreshold-action / lowthreshold-action

Specifies the action to be taken when a threshold is exceeded. The values supported are `all`, `none`, `raslog`, and `snmp`. The default action is `all`.

all

RASLOG and SNMP trap will be sent when the threshold is exceeded. This is the default configuration.

none

No action will be taken when the threshold is exceeded.

raslog

Only RASLOG will be sent when the threshold is exceeded.

snmp

Only SNMP traps will be sent when the threshold is exceeded.

Modes

Global Configuration Mode

Usage Guidelines

The **no** form of this command will remove the configured custom SFP policy.

The **low-threshold** threshold value cannot be higher than the value configured for the **high-threshold** threshold value.

Examples

The following example shows the creation and application of a custom SFP policy.

```
SLX# configure terminal
SLX (config)# threshold-monitor sfp policy custom type 100GLR area Voltage
    threshold high-threshold 95 low-threshold 50 buffer 75
SLX (config)# threshold-monitor sfp apply custom
```

The following example shows how to pause the applied SFP policy.

```
SLX# configure terminal
SLX (config)# threshold-monitor sfp pause
```

The following example removes the applied custom SFP policy.

```
SLX# configure terminal
SLX (config)# no threshold-monitor sfp custom
```

threshold-monitor vxlan-tunnel

Configures monitoring of the number of VXLAN Tunnels against the maximum number of supported VXLAN tunnels and alerts the user when configured thresholds are exceeded.

Syntax

threshold-monitor vxlan-tunnel [**high-limit** *value-in-percent*] [**low-limit** *value-in-percent*] [**actions** [*none* | *raslog* | *snmp* | *all*]]

no threshold-monitor vxlan-tunnel

Parameters

high-limit *value-in-percentage*

Specifies the upper threshold limit for the number of open VXLAN Tunnels that will trigger the configured action. The range is 10%-100%. The default value is 90%.

low-limit *value-in-percentage*

Specifies the lower threshold limit for the number of open VXLAN Tunnels that will trigger the configured action. The range is 10%-99%. The default value is 70%.

actions [*none* | *raslog* | *snmp* | *all*]

Specifies the action to be taken when a threshold is exceeded. The values supported are `all`, `none`, `raslog`, and `snmp`. Default is `all`.

all

RASLOG and SNMP trap will be sent when the threshold is exceeded.

none

No action will be taken when the threshold is exceeded.

raslog

Only RASLOG will be sent when the threshold is exceeded.

snmp

Only SNMP traps will be sent when the threshold is exceeded.

Modes

Global configuration mode

Usage Guidelines

The default `action` is *all*.

The `high-limit` value must always be higher than the `low-limit` value. If not, an error will be generated.

Examples

This example configures the various thresholds for monitoring open VXLAN Tunnels.

```
SLX# configure terminal
SLX (config)#
SLX (config)# threshold-monitor vxlan-tunnel interval 180
SLX (config)# threshold-monitor vxlan-tunnel count 30
SLX (config)# threshold-monitor vxlan-tunnel high-limit 85
SLX (config)# threshold-monitor vxlan-tunnel low-limit 55
SLX (config)# threshold-monitor vxlan-tunnel action raslog
SLX (config)#
SLX (config)# do show running-config threshold-monitor vxlan-tunnel
threshold-monitor vxlan-tunnel high-limit 85 low-limit 55 actions raslog count 30
interval 180
SLX (config)#
```

threshold-timer (management-heartbeat)

Configures the threshold value for listening to heartbeat message from EFA. Used within the *management-heartbeat* context.

Syntax

threshold-timer *time*

no threshold-timer

Command Default

By default, threshold value is set at five (5) minutes.

Parameters

time

The time duration in minutes for which this device will listen for a heartbeat message from EFA. Once this time exceeds, the device proceeds to perform the action configured through the `action` command. A value in the range of 1-30 minutes can be configured.

Modes

Management Heartbeat mode

Examples

The following example sets the threshold value to 30 minutes. This is the maximum value that can be configure for this parameter.

```
SLX(config-management-heartbeat-manage) # threshold-timer 30
```

tie-breaking

Configures the device to choose the path with the highest available bandwidth or the lowest available bandwidth.

Syntax

tie-breaking { [**least-fill** | **most-fill** | **random**] }

no tie-breaking { [**least-fill** | **most-fill** | **random**] }

Command Default

The default is the tie-breaking random mode.

Parameters

least-fill

Causes CSPF to choose the path with the highest available bandwidth (that is, the path with the least utilized links).

most-fill

Causes CSPF to choose the path with the lowest available bandwidth (that is, the path with the most utilized links).

random

Causes CSPF to choose the path randomly from the equal-cost paths.

Modes

MPLS LSP configuration mode (config-router-mpls-lsp-*lsp_name*)

MPLS router bypass LSP configuration mode (config-router-mpls-bypass-lsp-*bypass_name*)

MPLS router MPLS interface dynamic bypass configuration mode (config-router-mpls-if-ethernet-*slot/port* -dynamic-bypass)

Usage Guidelines

The **no** form of the command removes the tie-breaking configuration and reverts to the default mode.

The user can configure an interface level tie-breaking option for the CSPF calculation of dynamic bypass LSPs to be created for the protected MPLS interface. The set value is used for dynamic bypass LSP path computation tie-breaking procedure.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

In the following example, the configuration causes the CSPF to select the path with the highest available bandwidth when choosing among equal cost paths calculated for LSP *tunnel1*.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp tunnel1
device(config-router-mpls-lsp-tunnel1)# tie-breaking least-fill
```

The following example configures the tie-breaking path bandwidth to the least-fill option for dynamic bypass MPLS Ethernet interface *2/8* .

```
device# configure
device(config)# router mpls
device(config-router-mpls)# mpls-interface ethernet 2/8
device(config-router-mpls-if-ethernet-2/8)# dynamic-bypass
device(config-router-mpls-if-ethernet-2/8-dynamic-bypass)# tie-breaking least-fill
```

timeout (link-oam)

Allows you to configure timeout value, which corresponds to hold time before the Discovery process restarts.

Syntax

timeout *sec*

no timeout

Command Default

The default wait time is 5 seconds.

Parameters

sec

Specifies the hold time (in seconds) before the discovery process restarts. The range is from 1 through 10. The default value is 5.

Modes

Link OAM configuration mode

Usage Guidelines

The **no** form of the command restores the command default value.

Examples

The following example shows how to configure a wait time of 10 seconds.

```
device(config-link-oam)# timeout 4
```

timeout (RADIUS)

Species the wait time allowed for a Remote Authentication Dial-In User Service (RADIUS) server response.

Syntax

timeout *sec*

no timeout

Command Default

The default wait time is 5 seconds.

Parameters

sec

Specifies the wait time (in seconds) allowed for a RADIUS server response. The range is from 1 through 60. The default value is 5.

Modes

RADIUS server host VRF configuration mode

Usage Guidelines

The **no** form of the command restores the command default value.

Examples

The following example shows how to configure a wait time of 10 seconds.

```
device# configure terminal
device(config)# radius-server host 10.37.73.180 use-vrf green-vrf
device(config-host-10.37.73.180/green-vrf)# timeout 10
```

timeout (Y1731)

Configures timeout in seconds.

Syntax

timeout *timeout-value*

no timeout *timeout-value*

Parameters:

timeout-value

Spcifies the timeout value. The range is from 1 to 4 seconds.

Command Default

The default value for timeout is 1 second.

Modes

Y1731 configuration mode

Usage Guidelines

Use the **no** form of the command to delete the timeout configuration.

Examples

This example shows how to configure the timeout value.

```
device# configure terminal
device (config-cfm)# prtocol cfm
device (config-cfm)# y1731
device(config-cfm-y1731)# test-profile my_test_profile
device(config-cfm-y1731-test-profile-my_test_profile)# type delay-measurement
device(config-cfm-y1731-test-profile-my_test_profile)# tx-interval 60
device(config-cfm-y1731-test-profile-my_test_profile)# measurement-interval 30
device(config-cfm-y1731-test-profile-my_test_profile)# start at 00:00:00 daily
device(config-cfm-y1731-test-profile-my_test_profile)# stop at 23:59:00
device(config-cfm-y1731-test-profile-my_test_profile)# cos 7
device(config-cfm-y1731-test-profile-my_test_profile)# threshold maximum 3294967295
device(config-cfm-y1731-test-profile-my_test_profile)# timeout 1
```

timer

Sets the global MVRP join, leave and leave-all timers values on all MVRP-enabled interfaces except the interfaces configured with the **mvrp timer** command in interface configuration mode.

Syntax

timer join *cs* **leave** *cs* **leave-all** *cs*

no timer join *cs* **leave** *cs* **leave-all** *cs*

Command Default

The join timer default setting is 20 centiseconds (cs).

The leave timer default setting is 100 cs.

The leave-all timer default setting is 1000 cs.

Parameters

join *cs*

Specifies the join timer in centiseconds. Enter an integer from 20 to 10000000.

leave *cs*

Specifies the leave timer in centiseconds. Enter an integer from 100 to 10000000. The leave timer setting must be greater than or equal to twice the join timer setting plus 30 centiseconds.

leave-all *cs*

Specifies the leave-all timer in centiseconds. Enter an integer from 1000 to 10000000. The leave-all timer setting must be a minimum of three times the value of the leave timer setting.

Modes

MVRP configuration mode

Usage Guidelines

MVRP is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

The **no** form of the command resets the default settings globally and on interfaces that are not configured with the **mvrp timer** command in interface configuration mode.

This command requires that you configure the timer values in the specified order and you must configure all values.

When the network radius is large or the expected system load is higher normally, since the default timer values are aggressive, Extreme recommends that you change the timer values to higher numbers to reduce the MVRP message exchanges and the load of the system.

The configured timer settings on the individual interfaces override the global timer configuration.

The join timer is not run periodically but is triggered by the MVRP events or state changes. However, the leave-all timer is periodic; required for garbage collection purposes.

Examples

The following example configures the global MVRP timer settings.

```
device# configure terminal
device(config)# protocol mvrp
device(config-mvrp)# timer join 40 leave 200 leave-all 2000
device(config-mvrp)#
```

timers (BGP)

Adjusts the interval at which BGP KEEPALIVE and HOLDTIME messages are sent.

Syntax

timers { **keep-alive** *keepalive_interval* **hold-time** *holdtime_interval* }

no timers

Parameters

keep-alive *keepalive_interval*

Frequency in seconds with which a device sends keepalive messages to a peer. Range is from 0 through 65535 seconds. The default is 60.

hold-time *holdtime_interval*

Interval in seconds that a device waits to receive a keepalive message from a peer before declaring that peer dead. Range is from 0 through 65535 seconds. The default is 180.

Modes

BGP configuration mode

Usage Guidelines

The KEEPALIVE and HOLDTIME message interval is overwritten when the **fast-external-failover** command takes effect on a down link to a peer.

You must enter a value for keep-alive before you can enter a value for **hold-time**. Both values must be entered. If you only want to adjust the value of one parameter, enter the default value of the parameter that you do not want to adjust.

The **no** form of the command clears the timers.

Examples

The following example sets the keepalive timer for a device to 120 seconds and the hold-timer to 360 seconds.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# timers keep-alive 120 hold-time 360
```

The following example sets the keepalive timer for a device to 0 seconds and the hold-timer to 0 seconds so that the device waits indefinitely for messages from a neighbor without tearing down the session.

```
device# configure terminal
```

```
device(config)# router bgp
device(config-bgp-router)# timers keep-alive 0 hold-time 0
```

timers (OSPFv2)

Configures Link State Advertisement (LSA) pacing and Shortest Path First (SPF) throttle timers.

Syntax

timers { **lsa-group-pacing** *interval* | **throttle spf** *start hold max* }

Command Default

See the parameters section for specific defaults.

Parameters

lsa-group-pacing *interval*

Specifies the interval at which OSPF LSAs are collected into a group and refreshed, check-summed, or aged by the OSPF process. Valid values range from 10 to 1800 seconds. The default is 240 seconds.

throttle spf

Specifies start, hold and maximum wait intervals for throttling SPF calculations for performance. The values you enter are in milliseconds.

start

Initial SPF calculation delay. Valid values range from 0 to 60000 milliseconds. The default is 0.

hold

Minimum hold time between two consecutive SPF calculations. Valid values range from 0 to 60000 milliseconds. The default is 0.

max

Maximum wait time between two consecutive SPF calculations. Valid values range from 0 to 60000 milliseconds. The default is 0.

Modes

OSPF router configuration mode

OSPF VRF router configuration mode

Usage Guidelines

The device paces LSA refreshes by delaying the refreshes for a specified time interval instead of performing a refresh each time an individual LSA refresh timer expires. The accumulated LSAs constitute a group, which the device refreshes and sends out together in one or more packets.

The LSA pacing interval is inversely proportional to the number of LSAs the device is refreshing and aging. For example, if you have a large database of 10,000 LSAs, decreasing the pacing interval enhances performance. If you have a small database of about 100 LSAs, increasing the pacing interval to 10 to 20 minutes may enhance performance.

The **no timers lsa-group-pacing** command restores the pacing interval to its default value.

The **no timers throttle spf** command sets the SPF timers back to their defaults.

Examples

The following example sets the LSA group pacing interval to 30 seconds.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# timers lsa-group-pacing 30
```

The following example sets the SPF delay to 10000 milliseconds, the hold time to 15000 milliseconds, and the maximum wait time to 30000 milliseconds.

```
device# configure terminal
device(config)# router ospf
device(config-router-ospf-vrf-default-vrf)# timers throttle spf 10000 15000 30000
```

timers (OSPFv3)

Configures Link State Advertisement (LSA) pacing and Shortest Path First (SPF) timers.

Syntax

timers { **lsa-group-pacing** *interval* | **spf** *start hold* }

Command Default

Enabled.

Parameters

lsa-group-pacing *interval*

Specifies the interval at which OSPFv3 LSAs are collected into a group and refreshed, check-summed, or aged by the OSPFv3 process. Valid values range from 10 to 1800 seconds. The default is 240 seconds.

spf

Specifies start and hold intervals for SPF calculations for performance. The values you enter are in milliseconds.

start

Initial SPF calculation delay. Valid values range from 0 to 65535 seconds.

hold

Minimum hold time between two consecutive SPF calculations. Valid values range from 0 to 65535 seconds.

Modes

OSPFv3 router configuration mode

OSPFv3 router VRF configuration mode

Usage Guidelines

The device paces LSA refreshes by delaying the refreshes for a specified time interval instead of performing a refresh each time an individual LSA refresh timer expires. The accumulated LSAs constitute a group, which the device refreshes and sends out together in one or more packets.

The LSA pacing interval is inversely proportional to the number of LSAs the device is refreshing and aging. For example, if you have a large database of 10,000 LSAs, decreasing the pacing interval enhances performance. If you have a small database of about 100 LSAs, increasing the pacing interval to 10 to 20 minutes may enhance performance.

The **no timers lsa-group-pacing** command restores the pacing interval to its default value.

The **no timers spf** command sets the SPF timers back to their defaults.

Examples

The following example sets the LSA group pacing interval to 30 seconds.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# timers lsa-group-pacing 30
```

The following example sets the SPF delay time to 10 and the hold time to 20.

```
device# configure terminal
device(config)# ipv6 router ospf
device(config-ipv6-router-ospf-vrf-default-vrf)# timers spf 10 20
```

tls min-version

The command enables configuring the lowest TLS version supported by SLX OS for the *Client* and *Server* modes of operation of the SLX device. This command is available under the respective modes under the *Management Security SSL Profile* mode. SLX uses OpenSSL to provide transport layer security and the current version of OpenSSL supports TLS v 1.1 to TLS v 1.3. Since the SLX box can be considered as both a client as well as a server, you can apply different supported TLS versions for each of these types. The default TLS version supported is v 1.2.

Syntax

tls min-version { *1.1* | *1.2* | *1.3* }

no tls min-version

Command Default

The default supported TLS version is version 1.2.

Parameters

min-version { *1.1* | *1.2* | *1.3* }

Indicates that the minimum version of TLS support is being configured. Select from one of the available choices.

Modes

Client Profile mode and Server Profile mode in SSL Profile mode. SSL Profile mode is available under Management Security mode.

Usage Guidelines

The **no** format of this command resets the manual configuration of TLS support to the defaults. The default support is for TLS v 1.2 and TLS v 1.3.

Note
TLS v 1.1 will be deprecated in an upcoming release.

Examples

This example shows how to navigate into the Client Profile mode and configure the minimum supported TLS version to 1.3.

```
SLX # conf term
Entering configuration mode terminal
SLX # conf term
Entering configurationSLX (config)#
SLX (config)# management-security
```

```
SLX (mgmt-security)#
SLX(mgmt-security)# ssl-profile ?
Possible completions:
client management security ssl profile client for tls configuration
server management security ssl profile server for tls configuration
SLX (mgmt-security)# ssl-profile client
SLX (mgmt-sec-ssl-profile-client)#
SLX (mgmt-sec-ssl-profile-client)# tls ?
Possible completions:
min-version minimum version to be supported by client
SLX(mgmt-sec-ssl-profile-client)# tls min-version ?
Possible completions:
<1.1|1.2|1.3> specify TLS version
SLX(mgmt-sec-ssl-profile-client)# tls min-version 1.3
```

This example shows how to disable the manual configuration for TLS version support.

```
SLX # conf term
Entering configuration mode terminal

SLX (config)#
SLX (config)# management-security
SLX (mgmt-security)#
SLX (mgmt-security)# ssl-profile client
SLX (mgmt-sec-ssl-profile-client)#
SLX(mgmt-sec-ssl-profile-client)# no tls min-version
```

This example shows how by running the **`show running-config management-security`** command a TLS version is configured and the configured value can be seen.

```
SLX# conf
Entering configuration mode terminal
SLX(config)# management-security
Possible completions:
  <cr>
SLX(config)# management-security
SLX(mgmt-security)# ssl-profile client
SLX(mgmt-sec-ssl-profile-client)# tls min-version
Possible completions:
  <1.1|1.2|1.3> specify TLS version[1.2]
SLX(mgmt-sec-ssl-profile-client)# tls min-version
SLX(mgmt-sec-ssl-profile-client)# ex
SLX(mgmt-security)# ex
SLX(config)# exi
SLX# show running-config management-security
management-security
 ssl-profile server
  tls min-version 1.2
 !
 ssl-profile client
  tls min-version 1.2
 !
!
```

tlv-type

Enables the Port Status type-length-value (TLV) metric for the specified Maintenance End Points (MEP).

Syntax

tlv-type port-status-tlv

no tlv-type port-status-tlv

Command Default

The Port Status TLV is not enabled.

Parameters

port-status-tlv

Enables the Port Status TLV metric.

Modes

CFM protocol configuration mode .

Usage Guidelines

The **no tlv-type port-status-tlv** command disables the Port Status TLV metric for the specified MEP.

Examples

Command example to enable the Port Status TLV metric.

```
device# configure terminal
device(config-cfm)# domain name md1 level 4
device(config-cfm-md-md1)# ma-name ma1 id 1 vlan-id 30 priority 3
device(config-cfm-md-ma-ma1)# mep 1 down ethernet 1/2
device(config-cfm-md-ma-mep-1)# tlv-type port-status-tlv
```

to

Configures a destination address for the bypass LSP.

Syntax

to *ip_addr*

no to *ip_addr*

Parameters

ip_addr

Specifies the destination or egress IPv4 address of the bypass LSP.

Modes

MPLS router bypass LSP configuration mode

Usage Guidelines

The destination address is mandatory to enable a bypass LSP.

The **no** form of the command removes the destination address of the bypass LSP.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures the destination address to 33.33.33.33 for bypass LSP my-bypass-lsp.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# bypass-lsp my-bypass-lsp
device(config-router-mpls-bypass-lsp-my-bypass-lsp)# to 33.33.33.33
```

topology-group

Configures the topology group.

Syntax

topology-group *group-id*

no topology-group *group-id*

Command Default

A topology group is not configured.

Parameters

group-id

Specifies the topology group ID. The ID ranges from 1 through 256.

Modes

Global configuration mode

Usage Guidelines

Each topology group contains a master VLAN and can contain one or more member VLANs and VLAN groups. You must configure the master VLAN and member VLANs or member VLAN groups before you configure the topology group.

You can configure up to 30 topology groups. Each group can control up to 4096 VLANs. A VLAN cannot be controlled by more than one topology group. The topology group must contain a master VLAN and can also contain individual member VLANs, VLAN groups, or a combination of individual member VLANs and VLAN groups.

The **no** form of the command removes the topology group.

Examples

The following example configures the topology group with ID 2 and adds master VLAN and member VLANs.

```
device# configure terminal
device(config)# topology-group 2
device(config-topo-group-2)# master-vlan 2
device(config-topo-group-2)# member-vlan 3
device(config-topo-group-2)# member-vlan 4
device(config-topo-group-2)# member-vlan 5
```

tpvm

Provides administrative support, for users without root privileges, for Third-Party Virtual Machine (TPVM) applications.

Syntax

tpvm [**install** | **uninstall** [**force**]]

tpvm [**start** | **stop**]

tpvm auto-boot [**disable** | **enable**]

tpvm disk { **add name** { *disk_name* | **auto** *disk_size* } | **remove name** { *disk_name* | **auto** } }

tpvm password

tpvm console

Command Default

This feature is not enabled.

Parameters

install

Installs TPVM.

uninstall

Uninstalls TPVM.

force

Clears installation or uninstallation errors, then tries to force an uninstallation.

start

Starts TPVM.

stop

Stops TPVM.

auto-boot disable

Prevents TPVM from starting at the next reboot of SLX-OS.

auto-boot enable

Starts TPVM at the next reboot of SLX-OS (without the need for the start keyword).

disk add name

Adds a new disk to TPVM.

disk_name

Name of the disk to be added if the auto keyword is not specified.

auto

Assigns a disk name automatically. See the Usage Guidelines.

disk_size

Size of the disk (any positive integer). See the Usage Guidelines.

disk remove name

Removes an additional disk from TPVM.

disk_name

Name of the additional disk to be removed. See the Usage Guidelines.

password

Changes the password on the TPVM for the user account named 'extreme'.

console

Connects to the TPVM console from SLX-OS Telnet or console sessions only on SLX 9640, SLX 9150, and SLX 9250 devices. See the Usage Guidelines.

Modes

Privileged EXEC mode

Usage Guidelines

When the **tpvm console** command is used, use **ctrl+** to return to the session from where the TPVM console was started.

The **tpvm uninstall force** command asks for confirmation before proceeding. This command removes the TPVM and all its disks, including data.

The **tpvm password** command sets the password for the user account named 'extreme.' This password uses SHA-512 hash.

Use the **show tpvm** command for display options.

If the auto keyword is not used with the **tpvm disk** command, the name of the disk must be that of the next disk. For example, if the last disk added to the system is *vdb*, the name of the next disk must be *vdc*.

You can add one of the following suffixes to specify disk size:

- b or B (bytes)
- k or K (kilobytes)
- m or M (megabytes)
- g or G (gigabytes)

If no suffix is used, the default is gigabytes.

The maximum number of disks supported is currently 3 and if the number of allocated disks exceeds this number, the add_disk keyword fails. Also, the total disk capacity for TPVM is limited to 117 gigabytes on the SLX 9540 and SLX 9640, and limited to 68.7 gigabytes on the SLX 9150 and SLX 9250.

If the auto keyword is not used with the **remove_disk** command, the name of the disk must be that of the last disk added to the system.

Important
If the disk is mounted, it must be unmounted before it is removed from the system. Otherwise, the next added disk will be labeled incorrectly. If this happens, TPVM must be rebooted to recover.

Examples

To install TPVM:

```
device# tpvm install
```

To uninstall TPVM:

```
device# tpvm uninstall
```

To force the clearing of installation or uninstallation errors by means of the force keyword:

```
device# tpvm uninstall force
```

To start TPVM if it is not running:

```
device# tpvm start
```

To stop TPVM if it is running:

```
device# tpvm stop
```

To start TPVM at the next reboot of SLX-OS (without the need for the start keyword):

```
device# tpvm auto-boot enable
```

To prevent TPVM from starting at the next reboot of SLX-OS:

```
device# tpvm auto-boot disable
```

Note
In this case, the **tpvm start** command is required to enable TPVM.

To add a new disk to TPVM, by either using the auto keyword or specifying a disk name:

```
device# tpvm disk add name auto 10g
disk add succeeds
```

```
device# tpvm disk add name vdd
disk add succeeds
```

Note
The maximum number of disks supported is 3. If the number of allocated disks exceeds this number, the disk add name keywords fail. Also, the total disk capacity for TPVM is limited to 117 gigabytes on the SLX 9540 and SLX 9640, and limited to 68.7 gigabytes on the SLX 9150 and SLX 9250. If you exceed this limit when you create a disk, the disk add name keywords fail.

To remove an additional disk from TPVM:

```
device# tpvm disk remove name  auto
'umount' is needed before this disk is removed. Continue? [y/n]: y
disk remove succeeds

device# tpvm disk remove name vdc
'umount' is needed before this disk is removed. Continue? [y/n]: y
disk remove succeeds
```

Important
If the disk is mounted, it must be unmounted before it is removed from the system. Otherwise, the next added disk will be labeled incorrectly. If this happens, TPVM must be rebooted to recover.

To clear errors by means of the clear *<error>* keywords, where the error in this example is "disk add":

```
device# tpvm disk add name auto 10g
disk add failed

device# show tpvm status
TPVM had runtime error(s) -- these error(s) seem not fatal, and the operation(s) could be
retryable
disk add: virsh vol-create-as failed. error detail: error: Failed to create vol vde
error: operation failed: the number of volumes goes beyond the maximum

TPVM is running, and AutoStart is disabled on this host.

device# show tpvm ststus clear disk add
TPVM is running, and AutoStart is disabled on this host.
```

Note
The runtime error can be also removed automatically when the same subcommand succeeds.

To connect to the TPVM console on an SLX 9150:

```
device# tpvm console
Connected to domain TPVM
Escape character is ^\
Ubuntu 16.04.4 LTS TPVM ttyS0
TPVM login:
```

tpvm config dns

Configures a DNS server in a Third-Party VM (TPVM).

Syntax

tpvm config dns add dns-server *ipv4-addr* [*ipv4-addr*]**domain-name** *domain-name*

tpvm config dns remove

Command Default

By default, a DNS server is not configured in TPVM.

Parameters

add

Adds a DNS server.
dns-server *ipv4-addr* [*ipv4-addr*]

Specifies a list of up to 2 IP addresses. One address (primary) is mandatory. The second address (secondary) is optional.

domain-name *domain-name*

Specifies the domain name for the DNS server. You can configure only one domain name.

remove

Removes a DNS server.

Modes

Privileged EXEC mode

Usage Guidelines

There is not a **no** form of this command.

Examples

This example adds two DNS servers and updates the domain name.

```
device# tpvm config dns add dns-server 1.2.3.4 1.1.1.1 domain-name example.com
```

This example removes all DNS configuration from the TPVM.

```
device# tpvm config dns remove
```

tpvm config hostname

Configures the Hostname for a Third-Party VM (TPVM).

Syntax

tpvm config hostname *hostname*

Command Default

None

Parameters

hostname

TPVM Hostname.

Modes

Privileged EXEC mode

Usage Guidelines

no form of this command is not available. To reset hostname to its default value of *tpvm*, use the **hostname** command from within the TPVM context. For more information, see hostname (tpvm mode) on page 2697.

The length of the Hostname should be between 1 to 64 characters. The starting letter should be an alphabet.

The allowed characters are alphabets (a-z), numbers(0-9), “.”(dot), and “-“(hyphen).

Note
Configuring TPVM hostname from the SLX device is not recommended when EFA is deployed. Doing so will cause unknown state for the EFA and could lead to EFA downtime. To change the TPVM Hostname, use the procedures provided in EFA documentation. Refer EFA documents for hostname restrictions and format.

Examples

Example to update the hostname in TPVM

```
device# tpvm config hostname tpvm
```

tpvm config ldap

Configures an LDAP server in a Third-Party VM (TPVM).

Syntax

tpvm config ldap add host *hostname* **port** *portnum* [**secure**]

tpvm config ldap add basedn *domain-name* **rootdn** *root-domain-name* **rootdnpw** *root-password*

tpvm config ldap remove host *hostname* **port** *portnum*

tpvm config ldap remove basedn *domain-name* **rootdn** *root-domain-name* **rootdnpw** *root-password*

Command Default

By default, an LDAP server is not configured in TPVM.

Parameters

add

Adds LDAP configuration.

remove

Removes LDAP configuration.

host *hostname*

Specifies the IPv4 or IPv6 address or the FQDN of the LDAP server.

port *portnum*

Specifies the port on the LDAP server. The default secure port is 636. The default non-secure port is 389.

secure

Enables LDAP over TLS.

basedn *domain-name*

Specifies the base Domain Name.

rootdn *root-domain-name*

Specifies the root Domain Name.

rootdnpw *root-password*

Specifies the password for the root Domain Name.

Modes

Privileged EXEC mode

Usage Guidelines

There is not a **no** form of this command.

When LDAP replication is in use, no more than 2 LDAP servers can be configured. The base Domain Name and root Domain Name must be common to both servers.

Configuring a secure LDAP server without importing certificates results in an error. Use the **tpvm config ldap ca-cert** command to import certificates.

Examples

This example adds an LDAP host.

```
device# tpvm config ldap add host 10.24.15.200
```

This example adds a secure LDAP host with the default port.

```
device# tpvm config ldap add host 10.24.15.200 secure
```

This example adds an LDAP host with a custom port.

```
device# tpvm config ldap add host 1.1.1.1 port 234
```

This example adds a secure LDAP host with a custom port.

```
device# tpvm config ldap add host 1.1.1.1 port 234 secure
```

This example configures the base Domain Name.

```
device# tpvm config ldap add basedn dc=ldap,dc=hc-fusion,dc=in
```

This example configures the root Domain Name.

```
device# tpvm config ldap add rootdn cn=admin,dc=ldap,dc=hc-fusion,dc=in
```

This example configures the root Domain Name password.

```
device# tpvm config ldap add rootdnpw pass123
```

This example configures the base Domain Name, the root Domain Name, and the root Domain Name password.

```
device# tpvm config ldap add basedn dc=ldap,dc=hc-fusion,dc=in
rootdn cn=admin,dc=ldap,dc=hc-fusion,dc=in rootdnpw pass123
```

This example removes the configured LDAP server.

```
device# tpvm config ldap remove host 10.24.15.200
```

This example resets the configured port to the default (389 if the port was non-secure, 636 if the port was secure).

```
device# tpvm config ldap remove host 1.1.1.1 port
```

This example disables the secure option for the LDAP server. The configured port remains the same and is not reset to the default. Use the **tpvm config ldap remove host <ip-addr> port** command to reset the port.

```
device# tpvm config ldap remove host 1.1.1.1 secure
```

This example removes the base Domain Name.

```
device# tpvm config ldap remove basedn
```

This example removes the root Domain Name.

```
device# tpvm config ldap remove rootdn
```

This example removes the root Domain Name password.

```
device# tpvm config ldap remove rootdnpw
```

This example removes the base Domain Name, the root Domain Name, and the root Domain Name password.

```
device# tpvm config ldap remove basedn rootdn rootdnpw
```

tpvm config ldap ca-cert

Imports or removes certificates for LDAP over TLS in a Third-Party VM (TPVM).

Syntax

tpvm config ldap ca-cert import protocol *SCP* **user** *username* **password** *password* **directory** *dirname* **file** *filename*

tpvm config ldap ca-cert remove

Command Default

By default, certificates are not imported.

Parameters

import

Imports certificates for LDAP over TLS.

protocol *SCP*

Specifies the SCP protocol.

host *hostname*

Specifies the host name or IP address of the remove server from which the CA certificate is imported.

user *username*

Specifies the login name for the remote server.

password *password*

Specifies the password associated with the user name.

directory *dirname*

Specifies the name of the remote directory that contains the certificate.

file *filename*

Specifies the file name of the certificate.

remove

Removes certificates for LDAP over TLS.

Modes

Privileged EXEC mode

Usage Guidelines

There is not a **no** form of this command.

You cannot remove certificates from configured secure LDAP servers. Use the **tpvm config ldap** command to disable the **secure** option and then remove the certificates.

Examples

This example imports certificates needed for the secure LDAP server configuration.

```
device# tpvm config ldap ca-cert import protocol SCP host 10.6.46.51
user fvt password pray4green directory /home/cert filename cacert.pem
```

This example removes a certificate.

```
device# tpvm config ldap ca-cert remove
```

tpvm config ntp

Configures the Network Time Protocol (NTP) for a Third-Party VM (TPVM) and now gets/display IPv6 configurations with IPv4 configurations.

Syntax

tpvm config ntp add server {*ipv4-address* | *fqdn* }

tpvm config ntp default

tpvm config ntp remove server {*ipv4-address* | *fqdn* }

Parameters

add

Adds NTP configuration.

default

Resets NTP configuration to the default.

remove

Removes NTP configuration.

server {*ipv4-address* | *fqdn*}

Identifies the NTP server by IPv4 address or fully qualified Domain Name.

Modes

Privileged EXEC mode

Usage Guidelines

There is not a **no** form of this command.

There is no limit to the number of NTP servers that you can configure.

Examples

This example adds a server to the list of NTP servers in the `/etc/systemd/timesyncd.conf` file in TPVM.

```
device# tpvm config ntp add server time.google.com
```

This example removes a server from the list of NTP servers in the `/etc/systemd/timesyncd.conf` file in TPVM.

```
device# tpvm config ntp remove server time.google.com
```

This example resets NTP configuration in TPVM to the default.

```
device# tpvm config ntp default
```

tpvm config timezone

Configures the Timezone for a Third-Party VM (TPVM).

Syntax

tpvm config timezone <timezone name>

Command Default

None.

Parameters

timezone

Timezone.

Modes

Privileged EXEC mode

Usage Guidelines

There is not a **no** form of this command.

Examples

Example to update the timezone in TPVM.

```
device# tpvm config timezone Etc/GMT
```

tpvm config trusted-peer

Adds and removes bi-directional password-less SSH connection between the root user accounts of both the TPVM and Peer TPVM instances.

Syntax

tpvm config trusted-peer add *ipv4-address* **sudo-user** *username* **password** *sudo-user-password*

tpvm config trusted-peer add *ipv4-address* **password** *sudo-user-password*

tpvm config trusted-peer remove *ipv4-address* **sudo-user** *username* **password** *sudo-user-password*

tpvm config trusted-peer remove *ipv4-address* **password** *sudo-user-password*

Command Default

None.

Parameters

add

Adds Trusted-Peer configuration.

remove

Removes Trusted-Peer configuration.

ipv4-address

Specifies the IPv4 address of the Peer TPVM.

sudo-user *username*

Specifies the Sudo User in the Peer TPVM. The default sudo-user is "extreme". User-name length varies from 1-32 characters.

password *sudo-user-password*

Password for sudo-user in Peer TPVM. Password length varies from 1-512 characters. Special characters are not supported as part of the password are: double quote (“), single quote (‘), back slash (\), question mark (?), exclamation mark (!) and pipe (|).

Modes

Privileged EXEC mode

Usage Guidelines

The **no** form of this command is not available.

The IPv4 address of the Peer TPVM and the password are mandatory parameters.

Examples

This example shows how to add a trusted peer

```
SLX# tpvm config trusted-peer add 10.23.31.67 password password
```

This example shows how to add a trusted peer without providing the user ID of the sudo user.

```
SLX# tpvm config trusted-peer add 10.23.31.67 password password
```

This example shows how to add a trusted peer and providing the user ID of the sudo user.

```
SLX# tpvm config trusted-peer add 10.23.31.67 sudo-user extreme password password
```

When trying to run two sessions in parallel.

```
SLX# tpvm config trusted-peer add 10.23.31.67 password password
    Another trusted-peer configuration is in progress. Please try again later.
```

Note
This behaviour is common when you try to perform add-add, add-remove, or remove-remove commands running in parallel.

When the TPVM Peer IP address is not reachable and the user tries to add a trusted peer.

```
SLX# tpvm config trusted-peer add 10.23.31.68 sudo-user extreme password password
   Failed to connect to 10.23.31.68
```

When the user provides an invalid credential when adding a trusted peer.

```
SLX# tpvm config trusted-peer add 10.23.31.67 sudo-user test password password
   Check input credentials.
```

Note
This message is displayed when invalid username or invalid password is supplied while creating a trusted peer.

When the user account used to access the remote trusted peer is not in the sudo user's list or the account is not configured properly.

```
SLX# tpvm config trusted-peer add 10.23.31.67 sudo-user testuser password password
   Check sudouser configuration for testuser user.
```

This example shows how to remove a configured trusted peer without providing the remote peer's sudo user account user name:

```
SLX# tpvm config trusted-peer remove 10.23.31.67 password password
```

This example shows how to remove a configured trusted peer by providing the remote peer's sudo user account user name:

```
SLX# tpvm config trusted-peer add 10.23.31.67 sudo-user extreme password password
```

When trying to remove a trusted peer but the peer is not reachable.

```
SLX# tpvm config trusted-peer remove 10.23.31.68 sudo-user extreme password password
   Failed to connect to 10.23.31.68
```

when trying to remove a trusted peer, but the user credentials are incorrect.

```
SLX# tpvm config trusted-peer add 10.23.31.67 sudo-user extreme password wrognpass
   Check input credentials.
```

Note
This message is displayed when invalid username or invalid password is supplied while removing the trusted peer.

When the user account used to access the remote trusted peer is not in the sudo user's list or the account is not configured properly.

```
SLX# tpvm config trusted-peer remove 10.23.31.67 sudo-user testuser password password
   Check sudouser configuration for testuser user.
```

tpvm deploy

Performs TPVM and Insight Interface set up and configuration.

Syntax

tpvm deploy insight *admin-pwd* **allow-pwdless** *confirm-pwd* **gw ipaddr**

tpvm deploy mgmt *admin-pwd* **allow-pwdless** *confirm-pwd* [**dhcp**]**gw ipaddr**

Command Default

This feature is not enabled.

Parameters

insight

Configures the insight (Eth1) interface.

mgmt

Configures the management (Eth0) interface.

admin-pwd

(Optional) Sets the password on the TPVM for the user account named "extreme". Requires password to be entered twice.

allow-pwdless

(Optional) Enables passwordless configuration for ssh and sudo access.

confirm-pwd

Confirms the password on the TPVM for the user account named "extreme".

dhcp

(Optional under mgmt) Default is static. If selected, dhcp fetches an ip-address and gateway. If dhcp is not selected, the static IP configuration must be supplied.

With a static IP configuration, a gateway IP is optional.

gw

(Optional) Sets the IP address of the default gateway.

ipaddr

(Optional) Configures the static interface IPv4 address and network mask.

Modes

Privileged EXEC mode

Usage Guidelines

This command performs the following operations:

- Installs TPVM
- Sets up TPVM networking
- Enables passwordless ssh from root@slx to extreme@TPVM
- Enable passwordless “sudo” inside TPVM
- Sets the TPVM password for the user account named "extreme".

This command begins with the standard TPVM installation.

By default the TPVM management interface eth0 is configured to acquire an IP Address via DHCP, whereas the eth1 address is manually configured by adding a static entry in `/etc/network/interfaces`.

The passwordless parameter in `tpvm deploy` allows you to configure ssh access from the root user account on the SLX-OS to TPVM without a password.

The TPVM default user is extreme with `sudo` privileges. The `tpvm deploy` command configures TPVM so `sudo` for this user does not ask for a password. Setting this parameter once will persist for the lifetime of the TPVM.

TPVM ships with `admin/password` as the default login credential. To automate the TPVM setup and achieve one touch provisioning of TPVM, this optional parameter sets the password for the TPVM `extreme` user account. Setting this parameter once will persist for the lifetime of the TPVM.

Auto-boot may be specified to restart the TPVM image automatically in subsequent reboots, such as an SLX-OS start on a Baremetal platform, or a HOST start on a VM-based platform.

After configuring the TPVM, `tpvm deploy` will start the TPVM. On a Baremetal platform, a reboot of SLX will reboot TPVM. On a VM-based platform, an SLX-OS reboot does not affect TPVM. However if the HOST reboots for any reason, TPVM also reboots.

Examples

The following example configures TPVM on Eth0 with a static IP and an administrative password of "mypassword".

```
device# tpvm deploy mgmt ipaddr 10.25.101.121/22 gw 10.25.100.1 admin-pwd mypassword
confirm mypassword
Starting TPVM deploy CLI, please DO NOT hit CTRL+C
Tpvm install started
..Tpvm is installed
Tpvm set_ip succeeds
Tpvm password succeeds
auto-boot enable succeeds
Tpvm is started
```

The following example configures Eth0 with static IP, default gateway and passwordless login.

```
device# tpvm deploy mgmt ipaddr 192.168.1.1/24 gw 192.168.1.100 allow-pwdless
```

The following example configures Eth1 with a static IP address, a default gateway, but no passwordless login, and new TPVM password setup.

```
device# tpvm deploy insight ipaddr 10.10.10.1/24 gw 10.10.10.100 admin-pwd admin123
      confirm-pwd admin123
```

The following example configures Eth1 with a static IP address and default gateway.

```
device# tpvm deploy insight ipaddr 10.10.10.1/24 gw 10.10.10.100
```

tpvm download

Downloads the TPVM image from the remote location, and then optionally, verifies if the file size and the version of the downloaded TPVM image is correct.

Syntax

tpvm download { **block** } **directory** *remote-directory-name* **filename** *image-file-name* **host** [*hostname* | *ip-address*] **password** *password* **protocol** {**FTP** | **SCP** | **SFTP** } { **sanity** [*yes* | *no*] } **use-vrf** *vrf-name* **user** *user-name*

Parameters

block

Optional Parameter. When passed, it enables NetCONF/RPC requests to operate in the blocking mode. When not passed, NetCONF/RPC operation is always non-blocking. This parameter does not affect CLI commands as CLI is always considered blocking in nature.

directory *remote-directory-name*

Specifies the remote directory that contains the TPVM image.

filename *image-file-name*

Specifies the TPVM Debian image file name.

host [*hostname* | *ip-address*]

Specifies the remote server. Remote server information can be provided either as a *hostname* or *ip-address*. Both IPv4 and IPv6 addresses are supported.

password *password*

Password for the username provide in the *user* parameter.

protocol {**FTP** | **SCP**| **SFTP**}

Specifies the use of either FTP, SCP or SFTP protocol for exporting the certification file.

sanity [*yes* | *no*]

Optional parameter. When set to *yes*, the TPVM image file is verified for size and version number after being downloaded. When set to *no*, the TPVM image is downloaded but not verified.

use-vrf *vrf-name*

Defines the VRF to use to access the remote host.

user *user-name*

The account that will be used to access the remote host. The password of this account is passed in the *password* parameter.

Modes

Privileged EXEC mode

Usage Guidelines

Use the optional **sanity** key to ensure that the downloaded TPVM image is verified for version and length after it has been downloaded from the remote server.

Use the optional **block** key to indicate that NetCONF/RPC calls are considered *blocking* in nature. By default, NetCONF/RPC calls are *non-blocking*. Also, CLI commands are always *blocking* by nature. This key does not affect this action when performed through SLX-OS CLI.

Examples

The following example shows the usage of the **tpvm download** command. This example shows the interactive mode for this command.

```
SLX # tpvm download ?
Possible completions:
    block         optional wait mode for netconf
    directory     Remote directory
    filename      TPVM debian filename
    host          Hostname or IPv4/IPv6 address
    password      Password for the user
    protocol      Protocol
    sanity        Perform sanity check
    use-vrf       Vrf to use for downloading TPVM package (Default =mgmt-vrf)
    user          Login name in the host
SLX# tpvm download sanity ?
Possible completions:
      <yes|no>     Sanity check
SLX# tpvm download sanity
```

tpvm fileinfo

Displays information for the TPVM image file stored in the /tftpboot/SWD2900 directory of the SLX-OS. TPVM is installed from this image file.

Syntax

tpvm fileinfo

Modes

Privileged EXEC mode

Usage Guidelines

Debian image file must exist under the */tftpboot/SWBD2900* directory on the SLX-OS device.

If no TPVM image file is found in the above directory, or more than one TPVM images are found, **tpvm fileinfo** command will display appropriate error messages.

Examples

The following example shows the use of the **tpvm fileinfo** command.

```
SLX# tpvm fileinfo
File Name tpvm-4.2.5-1.amd64.deb
File length 1952933946
File Version 4.2.5
Success
```

tpvm (mode)

Enters into the TPVM persistence configuration mode. Only one TPVM instance can be configured at present. Currently, the *tpvm-id* only allowed value is **TPVM**, and its optional and default also.

Syntax

tpvm [*tpvm-id*]

no tpvm [*tpvm-id*]

Modes

Global Configuration Mode

Usage Guidelines

The value for the *tpvm-id* must always be **TPVM**.

Examples

This example navigates into the *TPVM Configuration* mode.

```
SLX# configure terminal
SLX (config)# tpvm TPVM
SLX (config-tvpm-TPVM)#
```

This example purges a configured TPVM instance completely.

```
SLX (config)# no tpvm TPVM
```

ldap host

Configures an LDAP server in the TPVM instance.

Syntax

ldap host [*hostname* | *ip-address*] [**port** *portnum*] [**secure**]

ldap [**basedn** *domain-name*] [**rootdn** *root-domain-name* [**rootdnpw** *root-password*]]

no ldap host [*hostname* | *ip-address*] [**port** *portnum*]

no ldap [**basedn** *domain-name*] [**rootdn** *root-domain-name* [[**rootdnpw** *root-password*]

Command Default

By default, an LDAP server is not configured in TPVM.

Parameters

host [*hostname* | *ip-address*]

Specifies the host name or *IPv4* or *IPv6* address or the FQDN of the LDAP server.

port *portnum*

Specifies the port on the LDAP server. The default secure port is 636. The default non-secure port is 389.

secure

Enables LDAP over TLS.

basedn *domain-name*

Specifies the base Domain Name.

rootdn *root-domain-name*

Specifies the root Domain Name.

rootdnpw *root-password*

Specifies the password for the root Domain Name.

Modes

TPVM Configuration mode

Usage Guidelines

When LDAP replication is in use, no more than 2 LDAP servers can be configured. The base Domain Name and root Domain Name must be common to both servers.

Configuring a secure LDAP server without importing certificates results in an error. Use the **tpvm config ldap ca-cert** command to import certificates.

Examples

This example adds an LDAP host.

```
SLX (config)# tpvm TPVM
SLX (config-tpvm-TPVM)# ldap host 10.24.15.200
```

This example adds an LDAP host with IPv6 address.

```
SLX (config)# tpvm TPVM
SLX (config-tpvm-TPVM)# ldap host 2001:db8::172:1f
```

This example adds a secure LDAP host with the default port.

```
device# tpvm config ldap add host 10.24.15.200 secure
```

This example adds an LDAP host with a custom port.

```
SLX (config)# tpvm TPVM
SLX (config-tpvm-TPVM)# ldap host 10.24.15.200 port 234
```

This example adds a secure LDAP host with a custom port.

```
SLX (config)# tpvm TPVM
SLX (config-tpvm-TPVM)# ldap host 10.24.15.200 port 234 secure
```

This example configures the base Domain Name.

```
SLX (config-tpvm-TPVM)# ldap basedn dc=ldap,dc=hc-fusion,dc=in
```

This example configures the root Domain Name.

```
SLX (config-tpvm-TPVM)# ldap rootdn cn=admin,dc=ldap,dc=hc-fusion,dc=in
```

This example configures the root Domain Name password.

```
SLX (config-tpvm-TPVM)# ldap rootdnpw pass123
```

This example configures the base Domain Name, the root Domain Name, and the root Domain Name password.

```
SLX (config-tpvm-TPVM)# ldap basedn dc=ldap,dc=hc-fusion,dc=in
rootdn cn=admin,dc=ldap,dc=hc-fusion,dc=in rootdnpw pass123
```

This example removes the configured LDAP server.

```
SLX (config-tpvm-TPVM)# no ldap host 10.24.15.200
```

This example resets the configured port to the default (389 if the port was non-secure, 636 if the port was secure).

```
SLX (config-tpvm-TPVM)# no ldap host 1.1.1.1 port
```

This example disables the secure option for the LDAP server. The configured port remains the same and is not reset to the default. Use the **no ldap host <ip-addr> port** command to reset the port.

```
SLX (config-tpvm-TPVM)# no ldap host 1.1.1.1 secure
```

This example removes the base Domain Name.

```
SLX (config-tpvm-TPVM)# no ldap basedn
```

This example removes the root Domain Name.

```
SLX (config-tpvm-TPVM)# no ldap rootdn
```

This example removes the root Domain Name password.

```
SLX (config-tpvm-TPVM)# no ldap rootdnpw
```

This example removes the base Domain Name, the root Domain Name, and the root Domain Name password.

```
SLX (config-tpvm-TPVM)# no ldap basedn rootdn rootdnpw
```

ldap ca-cert

Imports or removes certificates for LDAP over TLS in the TPVM instance.

Syntax

ldap ca-cert import protocol *SCP* **host** [*hostname* | *ip-address*] **user** *username* **password** *password* **directory** *dirname* **file** *filename*

no ldap ca-cert

Command Default

By default, certificates are not imported.

Parameters

import

Imports certificates for LDAP over TLS.

protocol *SCP*

Always use the SCP protocol.

host [*hostname* | *ip-address*]

Specifies the host name or *IPv4* or *IPv6* address of the remote server from where the CA certificate is to be imported.

user *username*

Specifies the login name for the remote server.

password *password*

Specifies the password associated with the above user name.

directory *dirname*

Specifies the name of the remote directory that contains the certificate.

file *filename*

Specifies the file name of the certificate on the remote server.

Modes

TPVM Configuration mode

Usage Guidelines

You cannot remove certificates from configured secure LDAP servers without disabling the secure mode. Use the **ldap** command to disable the **secure** option and then remove the certificates. Also `secure` and `non-secure` LDAP configuration cannot be issued at a time for IPv6 `ldap` configuration.

Examples

This example imports the certificates needed for secure LDAP server configuration.

```
SLX (config-tpvm-TPVM)#  ldap ca-cert import protocol SCP host 10.6.46.51
user fvt password pray4green directory /home/cert filename cacert.pem
```

This example removes a certificate.

```
SLX (config-tpvm-TPVM)# no ldap ca-cert
```

This example imports certificates for LDAP SCP user from a host with an IPv6 address.

```
SLX(config-tpvm-TPVM)# ldap ca-cert import protocol SCP user extreme password pass host ?
Possible completions:
    <Hostname or IP address>
SLX(config-tpvm-TPVM)# ldap ca-cert import protocol SCP user extreme password pass
    host 2001:db8::172:1f directory/home/cert filename cacert.pem
```

ntp (tpvm mode)

Configures the Network Time Protocol (NTP) server for TPVM instance. Supports IPv4 and IPv6 addresses.

Syntax

ntp { *ipv4-address* | *ipv6-address* }

Parameters

{ *ipv4-address* | *ipv6-address* }

Configures the NTP server by their IPv4 and / or IPv6 address.

Modes

TPVM Configuration mode

Usage Guidelines

Up to five (5) NTP servers can be configured for TPVM using their IPv4 and / or IPv6 addresses.

Examples

This example displays possible completion of NTP configuration for TPVM.

```
SLX(config-tpvm-1)# ntp ?
    Possible completions:
        <A.B.C.D IP address in dotted decimal>
        <string, min: 1 char, max: 253 chars>
    NTP server IPV4 address or FQDN
        <A:B::C:D IPV6 address>
SLX(config-tpvm-1)# ntp 100:23::45:55 ?
    Possible completions:
    <cr>
```

tpvm dns

Configures the DNS server details for the TPVM instance. DNS configuration CLI already supports IPv4 address. It is enhanced to support IPv6 address.

Syntax

dns primary-server [*ipv4-addr* | *ipv6-addr*] **secondary-server** [*ipv4-addr* | *ipv6-addr*] { **domain** *domain-name* }

no dns [**primary-server**] [**secondary-server**] [**domain**]

Command Default

By default, a DNS server is not configured in TPVM.

Parameters

primary-server [*ipv4-addr* | *ipv6-addr*]

Adds a DNS server. Specifies the mandatory (primary) DNS server IP. DNS server IP can be in IPv4 or IPv6 format.

secondary-server [*ipv4-addr* | *ipv6-addr*]

Adds a secondary DNS server. This server will be used to resolve addresses in case the primary DNS server fails for any reason. Secondary DNS server IP can be in IPv4 or IPv6 format.

domain-name *domain-name*

Specifies the domain name for the DNS server. You can configure only one domain name.

Modes

TPVM Configuration mode

Usage Guidelines

- When configuring DNS servers, both the primary and secondary servers should have the same IP address format.
- When changing the DNS server IP of the primary server from one IP format to another, the secondary DNS server configuration will not be retained and must be reconfigured.
- The secondary DNS server IP cannot be changed from one IP format to another without making the same change to the primary DNS server. You cannot modify only the secondary DNS server.
- While re-configuring the primary IPv4 address to IPv6 address, then implicitly of secondary IPv4 address is removed.

- You cannot change the secondary address alone from IPv4 to IPv6, till both primary and secondary address is provide.
- If you re-configure primary IPv6 address to IPv4 address, then implicitly of secondary IPv6 address is removed.

Examples

This example shows the configuration of DNS server.

```
SLX(config-tpvm-TPVM)# dns primary-server ?
Possible completions:
    <A.B.C.D> IPv4 address of primary DNS
    <A:B::C:D> IPv6 address of primary DNS
```

This example shows the configuration of a IPv6 primary DNS server and configures its domain.

```
SLX(config-tpvm-TPVM)# dns primary-server 100:23::45:55 ?
Possible completions:
    domain             Domain name
    secondary-server   Secondary name server
<cr>
SLX(config-tpvm-TPVM)# dns primary-server 100:23::45:55
    secondary-server 110:13::15:51 domain ?
 Possible completions:
    <string>
SLX(config-tpvm-TPVM)# dns primary-server 100:23::45:55
    secondary-server 110:13::15:51 domain extreme
```

This example removes the secondary DNS server configuration from the TPVM.

```
SLX (config-tpvm-TPVM)# no dns secondary-server
```

hostname (tpvm mode)

Configures the *Hostname* for the TPVM instance.

Syntax

hostname *hostname*

no hostname

Command Default

The default Hostname is *tpvm*.

Parameters

hostname

The TPVM *Hostname*.

Modes

TPVM Configuration mode

Usage Guidelines

The **no** form of this command resets the hostname to its default value of *tpvm*.

The length of the Hostname should be between 1 to 64 characters. The starting letter should be an alphabet.

The allowed characters are alphabets (a-z), numbers(0-9), “.”(dot), and “-“(hyphen).

Note
Configuring TPVM hostname from the SLX device is not recommended when EFA is deployed. Doing so will cause unknown state for the EFA and could lead to EFA downtime. To change the TPVM Hostname, use the procedures provided in EFA documentation. Refer EFA documents for hostname restrictions and format.

Examples

Example to update the hostname in TPVM

```
SLX (config-tpvm-TPVM)# hostname mytpvm
```

This example resets hostname configuration in TPVM to the default.

```
SLX (config-tpvm-TPVM)# no hostname
```

timezone (tpvm mode)

Configures the Timezone for the TPVM instance.

Syntax

timezone <timezone name>

no timezone

Command Default

The default timezone is *Etc/GMT*.

Parameters

timezone name

Timezone to assign.

Modes

TPVM Configuration mode

Examples

Example to update the timezone in TPVM.

```
SLX (config-tpvm-TPVM)# timezone Etc/GMT
```

trusted-peer (tpvm mode)

Adds and removes bi-directional password-less SSH connection between the root user accounts of both the TPVM and Peer TPVM instances.

Syntax

trusted-peer ip *ipv4-address* **password** *sudo-user-password* [**sudo-user** *username*]

trusted-peer ipv6 *ipv6-address* **password** *sudo-user-password* [**sudo-user** *username*]

no trusted-peer [**ip** *ipv4-address* | **ipv6** *ipv6-address*]

Command Default

None.

Parameters

ip *ipv4-address*

Specifies the IPv4 address of the Peer TPVM.

ipv6 *ipv6-address*

Specifies the IPv6 address of the peer TPVM.

sudo-user *username*

Specifies the SUDO User in the Peer TPVM. The default sudo-user is *extreme*. User-name length varies from 1-32 characters.

password *sudo-user-password*

Password for sudo-user in Peer TPVM. Password length varies from 1-512 characters. Special characters are not supported as part of the password are: double quote (“), single quote (‘), back slash (\), question mark (?), exclamation mark (!) and pipe (|).

Modes

TPVM Configuration mode

Usage Guidelines

The IPv4 address of the Peer TPVM and the password are mandatory parameters.

Examples

This example shows how to add a trusted peer without providing the user ID of the sudo user.

```
SLX (config-tpvm-TPVM)# trusted-peer ip 10.23.31.67 password password
```

This example shows how to add a trusted peer (with IPv6 address) without providing the user ID of the sudo user.

```
SLX (config-tpvm-TPVM)# trusted-peer ipv6 2002:2002::2001:2001 password password
```

This example shows how to add a trusted peer and providing the user ID of the sudo user.

```
SLX (config-tpvm-TPVM)# trusted-peer ip 10.23.31.67 sudo-user extreme password password
```

When trying to run two sessions in parallel.

```
SLX (config-tpvm-TPVM)# trusted-peer ip 10.23.31.67 password password
Another trusted-peer configuration is in progress. Please try again later.
```

Note
This behaviour is common when you try to perform add-add, add-remove, or remove-remove commands running in parallel.

When the TPVM Peer IP address is not reachable and the user tries to add a trusted peer.

```
SLX (config-tpvm-TPVM)# trusted-peer ip 10.23.31.68 sudo-user extreme password password
Failed to connect to 10.23.31.68
```

When the user provides an invalid credential when adding a trusted peer.

```
SLX (config-tpvm-TPVM)# trusted-peer ip 10.23.31.67 sudo-user test password password
Check input credentials.
```

Note
This message is displayed when invalid username or invalid password is supplied while creating a trusted peer.

When the user account used to access the remote trusted peer is not in the sudo user's list or the account is not configured properly.

```
SLX (config-tpvm-TPVM)# trusted-peer ip 10.23.31.67 sudo-user testuser password password
Check sudouser configuration for testuser user.
```

This example shows how to remove a configured trusted peer without providing the remote peer's sudo user account user name:

```
SLX (config-tpvm-TPVM)# no trusted-peer ip 10.23.31.67 password password
```

This example shows how to remove a configured trusted peer by providing the remote peer's sudo user account user name:

```
SLX (config-tpvm-TPVM)# no trusted-peer ip 10.23.31.67 sudo-user extreme password password
```

When trying to remove a trusted peer but the peer is not reachable.

```
SLX (config-tpvm-TPVM)# no trusted-peer 10.23.31.68 sudo-user extreme password password
Failed to connect to 10.23.31.68
```

when trying to remove a trusted peer, but the user credentials are incorrect.

```
SLX (config-tpvm-TPVM)# no trusted-peer ip 10.23.31.67 sudo-user extreme password
wrognpass
Check input credentials.
```

Note
This message is displayed when invalid username or invalid password is supplied while removing the trusted peer.

When the user account used to access the remote trusted peer is not in the sudo user's list or the account is not configured properly.

```
SLX (config-tpvm-TPVM)# no trusted-peer ip 10.23.31.67 sudo-user testuser password
password
Check sudouser configuration for testuser user.
```

auto-boot (tpvm mode)

Enables auto-start of TPVM on next boot of SLX-OS.

Syntax

auto-boot

no auto-boot

Modes

TPVM Configuration mode

Examples

To start TPVM at the next reboot of SLX-OS :

```
SLX (config-tpvm-TPVM)#  auto-boot
```

To prevent TPVM from starting at next reboot of SLX-OS :

```
SLX (config-tpvm-TPVM)# no auto-reboot
```

disk (tpvm mode)

Adds disks to TPVM. Up to three (3) disks can be added. These disks can be added only in the order *vdb*, *vdc*, and *vdd*. When removing disks, they must be removed in the order *vdd*, *vdc*, and *vdb* (in the reverse order in which they were added). When the *auto* parameter is used, the name of the next disk in the order will be selected and added to the TPVM configuration.

Syntax

disk { **name** { *disk_name* | **auto** } { **size** *disk_size* }

disk { **name** { *disk_name* | **auto** } { **size** *disk_size* }

Parameters

name

disk_name

Adds a new disk to TPVM. Name of the disk to be added if the auto keyword is not specified.

auto

Assigns a disk name automatically. See the Usage Guidelines.

size *disk_size*

Size of the disk (any positive integer). See the Usage Guidelines.

no disk name

Removes a disk from TPVM.
disk_name

Name of the disk to be removed. See the Usage Guidelines.

Modes

TPVM Configuration mode

Usage Guidelines

If the auto keyword is not used with the **tpvm disk** command, the name of the disk must be that of the next disk. For example, if the last disk added to the system is *vdb*, the name of the next disk must be *vdc*.

You can add one of the following suffixes to specify disk size:

- b or B (bytes)
- k or K (kilobytes)
- m or M (megabytes)
- g or G (gigabytes)

If no suffix is used, the default is gigabytes.

The maximum number of disks supported is currently 3 and if the number of allocated disks exceeds this number, the add_disk keyword fails. Also, the total disk capacity for TPVM is limited to 117 gigabytes on the SLX 9540 and SLX 9640, and limited to 68.7 gigabytes on the SLX 9150 and SLX 9250.

If the auto keyword is not used with the **remove_disk** command, the name of the disk must be that of the last disk added to the system.

Important
If the disk is mounted, it must be unmounted before it is removed from the system. Otherwise, the next added disk will be labeled incorrectly. If this happens, TPVM must be rebooted to recover.

Examples

To add a new disk to TPVM, by either using the auto keyword or specifying a disk name:

```
SLX (config-tpvm-1)# disk name auto 10g
disk add succeeds

dSLX (config-tpvm-1)# disk name vdd
disk add succeeds
```

Note
The maximum number of disks supported is 3. If the number of allocated disks exceeds this number, the disk add name keywords fail. Also, the total disk capacity for TPVM is limited to 117 gigabytes on the SLX 9540 and SLX 9640, and limited to 68.7 gigabytes on the SLX 9150 and SLX 9250. If you exceed this limit when you create a disk, the disk add name keywords fail.

To remove a disk from TPVM:

```
SLX (config-tpvm-1)# no disk name auto
'umount' is needed before this disk is removed. Continue? [y/n]: y
                    disk remove succeeds

SLX (config-tpvm-1)# no disk name vdc
'umount' is needed before this disk is removed. Continue? [y/n]: y
disk remove succeeds
```

Important
If the disk is mounted, it must be unmounted before it is removed from the system. Otherwise, the next added disk will be labeled incorrectly. If this happens, TPVM must be rebooted to recover.

password (tpvm mode)

Updates the password for the default TPVM user account *extreme*. The password can be normal text string or encrypted string.

Syntax

password *password*

no password

Parameters

password

The password to be assigned to the default user account *extreme*.

Modes

TPVM Configuration mode

Examples

The following example shows how to set the password for the default *extreme* account.

```
SLX (config-tpvm-TPVM)# password 2#eXtreme%4
```

allow-pwless (tpvm mode)

Enables password less login for SSH and SUDO accounts in TPVM.

Syntax

allow-pwless

no allow-pwless

Parameters

none

Modes

TPVM Configuration mode

Examples

The following example shows how to enable password less login for SSH and SUDO accounts.

```
SLX (config-tpvm-1)# allow-pwless
```

interface management (tpvm mode)

Configures the static IPv4/IPv6 address and gateway on the TPVM's management interface (eth0).

Syntax

interface management ip { **dhcp** | *ipv4-address/net-mask* [**gw** *gw-ip-address*] }

interface management ipv6 { **dhcpv6** | *ipv6-address/length* [**gw** *gw-ipv6-address*] }

no interface management ip { **dhcp** | *ip-address* [**gw** *gw-ip-address*] }

no interface management ipv6 { **dhcpv6** | *ipv6-address/length* [**gw** *gw-ipv6-address*] }

Parameters

dhcp

Indicates that the IPv4 address of the management interface is assigned by DHCP.

ip-address/net-mask

Configures the static *IPv4* address of the management interface and its net-mask.

gw *gw-ip-address*

The interface gateway *IPv4* address.

dhcpv6

Indicates the that IPv6 address of the interface is assigned by IPv6 DHCP.

ipv6-address/length

Configures the static *IPv6* address of the management interface along with the prefix length.

gw *gw-ipv6-address*

The interface gateway *IPv6* address. The IPv6 interface gateway address can also be dynamiacally configured when tpvm is running.

Modes

TPVM Configuration mode

Examples

The following example shows how to configure a static *IPv4* address and default gateway for the TPVM management interface *eth0*.

```
SLX (config-tpvm-TPVM)# interface management ip ?
Possible completions:
  <A.B.C.D/Y>   IPv4 address/netmask
```

```
  dhcp          Enable dhcp to configure ip
SLX(config-tpvm-TPVM)# interface management ip 10.9.9.24/24 ?
Possible completions:
  gw                      Interface gateway address
  <cr>
SLX (config-tpvm-TPVM)# interface management IP 10.9.9.24/24 gw ?
Possible completions:
  <A.B.C.D/Y>   IPv4 address/netmask
SLX (config-tpvm-TPVM)# interface management IP 10.9.9.24/24 gw 10.9.9.2
SLX (config-tpvm-TPVM)#
```

The following example shows how to configure DHCP on the TPVM management interface *eth0* .

```
SLX (config-tpvm-TPVM)# interface management ip
Possible completions:
  <A.B.C.D/Y>   IPv4 address/netmask
  dhcp          Enable dhcp to configure ip
SLX(config-tpvm-TPVM)# interface management ip dhcp
SLX (config-tpvm-TPVM)#
```

The following example shows how to configure the static *IPv6* address and default gateway for the TPVM management interface *eth0*.

```
SLX(config-tpvm-TPVM)# interface management ipv6 ?
Possible completions:
  <A:B::C:D/length>     The IPv6 Address/Prefix length
  dhcp                        Enable dhcp to configure IP
SLX (config-tpvm-TPVM)# interface management ipv6 2002:2002::2002:2002 gw
1001:1001::1000:0001
SLX (config-tpvm-TPVM)#
```

The following example shows how to configure DHCPv6 on the TPVM management interface *eth0*.

```
SLX(config-tpvm-TPVM)# interface management ipv6 ?
Possible completions:
  <A:B::C:D/length>     The IPv6 Address/Prefix length
  dhcpv6                        Enable dhcp to configure IP
SLX(config-tpvm-TPVM)# interface management ipv6 dhcpv6
SLX(config-tpvm-TPVM)#
```

interface insight (tpvm mode)

Configures the IP and gateway address on the insight interface of TPVM (eth1).

Syntax

interface insight ip { **dhcp** | *ip-address* [**gw** *gw-ip-address*] }

no interface insight ip { **dhcp** | *ip-address* [**gw** *gw-ip-address*] }

Parameters

dhcp

Indicates that the IP address of the insight interface is assigned by DHCP.

ip-address

Configures the IP address of the insight interface

gw *gw-ip-address*

The interface gateway IP address.

Modes

TPVM Configuration mode

Examples

The following example shows how to configure the IP address and default gateway for the TPVM insight interface (eth0)

```
SLX (config-tpvm-1)# interface insight ip 10.2.4.3/23 gw 10.2.3.1
```

deploy (tpvm mode)

This configuration will deploy the TPVM instance. It performs multiple steps of installing and starting the TPVM, as well applying all TPVM instance related configuration, which is currently set in the SLX configuration database. The *no deploy* configuration will purge the TPVM instance, which implies *stop*, *uninstall* and *delete*, as well as applying all TPVM instance related configurations in the SLX config database. This is similar to *no tpvm TPVM*.

Syntax

tpvm deploy

no deploy

Parameters

no parameters

Modes

Privileged EXEC mode

Usage Guidelines

As described above, this configuration will deploy the TPVM instance -

It expects the following:

Usage Guidelines

- There is no installing or running TPVM instance.
- The TPVM Debian image file is available at */tftpboot/SWBD2900* folder.
- All intermediate installation steps will succeed, but if it fails, it cleans up the partial installation if any.

It will perform the following steps:

Usage Guidelines

- It installs the TPVM Debian file.
- It starts the *TPVM (Guest OS)* instance.
- It applies the TPVM instance related configuration, to the *TPVM/Guest-OS*, if found persisted in the SLX configuration database.

Usage Guidelines

Note

Configurations like *password* and *interface management* are applied before starting the TPVM, means they will always fail, if attempted after deploy.
So they should be set in the SLX configuration database before *deploy*.
Alternatively, TPVM stops through the command *tpvm stop*, and then these two configurations will be set in the *tpvm config* mode, followed by the *tpvm start*. However, re-issuing the *config deploy* command, will be an idempotent operation with a void affect.

Logs:

It is time consuming operation, which may take few minutes. It publishes following logs.

```
[DCM-1451], 818,, INFO, SLX, Tpvm-id:TPVM operation:deploy mode:sync started.
[DCM-1452], 819,, INFO, SLX, Tpvm-id:TPVM operation:deploy mode:sync completed.
```

Examples

The following example configures the default installation of TPVM.

```
SLX(config-tpvm-TPVM)# deploy
2021/06/15-17:06:17, [DCM-1451], 818,, INFO, SLX, Tpvm-id:TPVM operation:deploy mode:sync
started.
2021/06/15-17:09:10, [DCM-1452], 819,, INFO, SLX, Tpvm-id:TPVM operation:deploy mode:sync
completed.
```

The following example performs the installation of the TPVM with few already persisted configurations. Use the *show tpvm config ...* commands to display the output of various configurations, or use the "*get-tpvm-detail*RPC for all operational data.

```
SLX# conf
Entering configuration mode terminal
SLX(config)# tpvm
SLX(config-tpvm-TPVM)# hostname myTpvm
SLX(config-tpvm-TPVM)# interface management ip dhcp
SLX(config-tpvm-TPVM)# password newpassword
SLX(config-tpvm-TPVM)# ntp time.google.com
SLX(config-tpvm-TPVM)# ntp ntp.ubuntu.com

SLX# show running-config tpvm
tpvm TPVM
 password encryted-string
 ntp ntp.ubuntu.com
 ntp time.google.com
 hostname myTpvm
 interface management ip dhcp
!

SLX# conf
Entering configuration mode terminal
SLX(config)# tpvm
SLX(config-tpvm-TPVM)# deploy
2021/06/15-17:22:42, [DCM-1451], 820,, INFO, SLX, Tpvm-id:TPVM operation:deploy mode:sync
started.
2021/06/15-17:26:20, [DCM-1452], 821,, INFO, SLX, Tpvm-id:TPVM operation:deploy mode:sync
completed.
```

```
SLX# show tpvm config hostname
myTpvm
```

tpvm upgrade

Upgrades the TPVM image. This command downloads the TPVM Debian image file using *SCP* or *SFTP* or *FTP* servers. Any previously installed TPVM instance is upgraded, and TPVM configuration from the SLX configuration database is applied, if available. Upgrades can be full or incremental. By default, full upgrades are performed.

Syntax

```
tpvm upgrade directory directory-name filename image-file-name host
   { hostname | ip-address } user username password password protocol
   { SCP | SFTP | FTP } uselocalfile tpvmid incremental snapshot use-vrf
   vrf-name force-default-password-change
```

Parameters

directory *directory-name*

Specifies the remote directory that contains the TPVM image.

filename *image-file-name*

The Debian TPVM image file name.

host [*hostname* | *ip-address*]

Specifies the remote server. Remote server information can be provided either as a *hostname* or *ip-address*. Both IPv4 and IPv6 addresses are supported.

user *username*

Specifies the login name for the remote server.

password *password*

Specifies the password associated with the user name.

protocol [*SCP* | *SFTP* | *FTP*]

Specifies the protocol to be used to download the TPVM image.

uselocalfile

Indicates that the TPVM upgrade process must use the TPVM Debian file located in the directory */tftpboot/SWBD2900*.

tpvmid

The ID of the TPVM instance. This value is always *TPVM*.

incremental

Indicates that *incremental* update must be performed.

snapshot

Indicates that when performing updates, both *incremental* as well as *full*, a snapshot of the TPVM instance before upgrade must be taken. This snapshot is then available for use if the upgrade fails for any reason.

use-vrf *vrf-name*

Defines the VRF to use to access the remote host.

force-default-password-change

Enforces changing the password if the default password is detected at the time of upgrade of TPVM.

Modes

EXEC mode

Usage Guidelines

The new TPVM Debian image file is downloaded to the */tftpboot/SWBD2900* directory. If any previous image file is present, it is moved to the */support/OldTpvm* directory, provided enough space is available.

Note
The *snapshot* feature may delete this subfolder, */support/OldTpvm*, to free space disk space when required.

During download of the TPVM image file, if TPVM is running, it is not stopped till the download is complete. On completion, the running TPVM instance (if any) is stopped and then uninstalled. If the *snapshot* parameter is used while upgrading, then a snapshot of the running TPVM is created.

The download may fail due to networking issues or not having enough free space on the device.

If SLX OS configuration database has TPVM configurations set, specially *config deploy*, then the upgrade process shall further install the new TPVM Debian image file, start the instance, and also apply other TPVM related persisted configurations from the SLX configuration database.

The default behavior of the **tpvm upgrade** command is to perform a full upgrade of the TPVM instance. To perform an incremental upgrade, you must use the *incremental* keyword explicitly. While performing the incremental upgrade, the Ubuntu Packages, TPVM script files, and XML files will be upgraded.

Incremental upgrade fails under the following conditions:

- The current installed instance of TPVM is not running.
- The installed TPVM version is lesser than version 4.5.0. In this case, you must perform a full TPVM install.
- At least 1Gb of space is not available on the TPVM.

Note
When you downgrade the existing TPVM version to a version that is **lower than** SLXOS version 20.4.1, then you will have to remove the IPv6 configurations before downgrading. Appropriate warning will be displayed.

The *force-default-password-change* parameter enforces changing the password if the default password is detected at the time of upgrade of TPVM.

- When this parameter is passed, and the password for the TPVM user is the default password, RAS LOG DCM-1458 is generated and upgrade is aborted. Change the password and restart the TPVM upgrade process.
- When this parameter is not passed, and the password for TPVM is the default password, then RAS LOG DCM-1457 is generated and the upgrade continues.

In the case that there is an existing instance of TPVM with the default password, and SLX-OS is reloaded or upgraded, RAS LOG DCM-1457 is generated and the upgrade continues.

For a fresh deployment of TPVM, when a password is not explicitly configured, the default password is applied for the TPVM user. In this case, during TPVM deployment, the RAS LOG DCM-1457 is generated and the deployment continues.

Examples

This example shows the command to perform a full upgrade of TPVM and forces change of default password.

```
SLX# tpvm upgrade directory /proj/tpvm_upgrade/ filename tpvm-4.5.0-0.amd64.deb host
10.10.10.1 user fav password testpassword protocol scp use-vrf mgmt-vrf force-default-
password-change
```

This example shows the command to perform an incremental installation of TPVM.

```
SLX# tpvm upgrade incremental directory /proj/tpvm_upgrade/ filename
tpvm_inc_upg-4.5.0-0.amd64.deb host 10.10.10.1 user fav password testpassword protocol
scp use-vrf mgmt-vrf
```

tpvm snapshot

Manually creates and manages TPVM snapshots. These snapshots can then be used to restore a TPVM to its previous state post any TPVM crash.

Syntax

tpvm snapshot [**create** | **delete** | **revert**] *tpvm-id*

Parameters

create

Creates a snapshot of the current TPVM and stores it to the SLX device.

delete

Deletes an existing snapshot.

restore

Restores the stored TPVM snapshot.

Modes

Privilege Execution mode

Usage Guidelines

Only one snapshot can be created and stored on the SLX device at any point of time.

Examples

The following example creates a snapshot

```
SLX (config)# tpvm snapshot create
```

The following example restores a snapshot

```
SLX (config)# tpvm snapshot restore
```

The following example deletes a snapshot

```
SLX (config)# tpvm snapshot delete
```

traceroute

Traces the network path of packets as they are forwarded to a destination address.

Syntax

```
traceroute { ip-address | host-name | ipv6 [ ipv6-address| host-name ] }
   [ interface ] [ maxttl value ] [ minttl value ] [ src-addr src-addr ]
   [ timeout seconds ] [ vrf { mgmt-vrf | default-vrf |vrf-name } ]
```

Parameters

ip-address

Specifies the IP address of the destination device.

host-name

Specifies the hostname of the destination device.

ipv6 *ipv6-address*

Specifies the IPv6 address of the destination device.

interface

Selects the output interface.

maxttl *value*

Maximum Time To Live value in a number of hops.

minttl *value*

Minimum Time To Live value in a number of hops.

src-addr *address*

Specifies the IPv4 or IPv6 address of the source device.

timeout *seconds*

The traceroute timeout value.

vrf

Specifies a VRF on which to run a traceroute.

mgmt-vrf

Specifies the management VRF.

default-vrf

Specifies the default-vrf.

vrf-name

Specifies a VRF name.

Modes

Privileged EXEC mode

Examples

This example executes an IPv6 traceroute, with minimum and maximum TTL values.

```
device# traceroute ipv6 fec0:60:69bc:92:218:8bff:fe40:1470
maxttl 128 minttl 30 src-addr fec0:60:69bc:92:205:33ff:fe9e:3f20 timeout 3

traceroute to fec0:60:69bc:92:218:8bff:fe40:1470 (fec0:60:69bc:92:218:8bff:fe40:1470),
128 hops max, 80 byte packets 30  fec0:60:69bc:92:218:8bff:fe40:1470
(fec0:60:69bc:92:218:8bff:fe40:1470)  2.145 ms  2.118 ms  2.085 ms
```

track (VRRP)

Enables VRRP tracking for a specified interface. VRRP Extended (VRRP-E) sessions can track a specified interface or a network.

Syntax

track { **ethernet** *slot*/*port*| **port-channel** *number* } [**priority** *value*]

track network { *ip-addressmask* | *ipv6-address*/*mask* } [**priority** *value*]

no track { **ethernet** *slot*/*port*| **port-channel** *number* } [**priority** *value*]

no track network { *ip-address*/*mask* | *ipv6-address*/*mask* } [**priority** *value*]

Command Default

The default priority value is 2.

Parameters

ethernet *slot port*

Specifies a valid, physical Ethernet subtype with appropriate slot and port number.

port-channel *number*

Specifies the port-channel number.

priority *value*

The track priority is a number from 1 through 254, and is used when a tracked interface or network up or down event is detected. For VRRP, if the tracked interface goes offline, the specified priority value is subtracted from the priority of the current device. For VRRP-E, if the tracked interface or network goes offline, the current device priority is reduced by the configured priority value. If the tracked interface or network comes online, the specified priority value is added to the priority of the current device.

network

Enables tracking of a specified network. Network tracking is supported only on VRRP-E sessions.

ip-address

Specifies an IPv4 network address.

ipv6-address

Specifies an IPv6 network address.

mask

Specifies a mask for the associated IP or IPv6 subnet.

Modes

Virtual-router-group configuration mode

Usage Guidelines

This command can be used to track interfaces for VRRP or VRRP-E. Only VRRP-E sessions support network tracking.

For VRRP, the tracked interface can be any Ethernet or port-channel interface other than the one on which this command is issued.

The networks to be tracked can be either present or absent from the Routing Information Base (RIB).

The maximum number of interfaces or networks you can track per virtual router is 16.

Enter **no track** with the specified interface or network to remove the tracked port or tracked network configuration.

Examples

To set the track port to 2/4 and the track priority to 60:

```
device# configure terminal
device(config)# protocol vrrp
device(config)# interface ethernet 1/6
device(conf-if-eth-1/6)# vrrp-group 1
device(config-vrrp-group-1)# track ethernet 2/4 priority 60
```

The following example shows how to configure network 10.1.1.0/24 to be tracked, and if the network goes down, the VRRP-E device priority is lowered by a value of 20. The lower priority may trigger a switchover and a backup device with a higher priority becomes the new master for VRRP-E group 1.

```
device# configure terminal
device(config)# protocol vrrp-extended
device(config)# interface ve 100
device(conf-if-Ve-100)# vrrp-extended-group 1
device(config-vrrp-extended-group-1)# track network 10.1.1.0/24 priority 20
```

traffic-engineering (LSP)

Allocating bandwidth to an LSP lets the LSRs determine how much bandwidth the LSP can consume and how much of the available bandwidth resources can be advertised.

Syntax

traffic-engineering { [[**max-burst** *kbps*] | [**max-rate** *kbps*] | [**mean-rate** *kbps*]] }

no traffic-engineering { [[**max-burst** *kbps*] | [**max-rate** *kbps*] | [**mean-rate** *kbps*]] }

Command Default

There are no allocated bandwidth allocations in the default mode.

Parameters

max-burst *kbps*

Specifies the maximum burst rate in bytes. The range is from 0-2147483647.

max-rate *kbps*

Specifies the maximum rate in kbps. The range is from 0-2147483647.

mean-rate *kbps*

Specifies the average rate in kbps. The range is from 0-2147483647.

Modes

MPLS LSP configuration mode (config-router-mpls-lsp-*lsp_name*)

MPLS router MPLS interface dynamic bypass configuration mode (config-router-mpls-if-ethernet-*slot/port*-dynamic-bypass)

Usage Guidelines

The user can specify an average mean-rate kbps for the data on the LSP. When necessary, data can travel at max-rate Kbps, as long as the burst sent at the maximum rate contains no more than max-burst bytes.

Use the **traffic-engineering** command to configure bandwidth parameters for the dynamic bypass LSPs to be created for the MPLS protected interface.

When the interface mode mean-rate value not configured at all then all dynamic bypass LSPs are created with the bandwidth the same as the backup path requested bandwidth. This means that system tries to create a dynamic bypass LSP with the backup path requested bandwidth and the dynamic bypass LSP bandwidths can vary based on the backup riding on it.

When the interface mode configured mean-rate value is 0 kbps, then the system creates dynamic bypasses for backup bandwidth requests of only 0 kbps. When the backup path bandwidth is more than zero, then this request does not create a new dynamic bypass LSP. This option provides a way to the user to limit the dynamic bypass creations to only non-bandwidth protected backups.

When the interface mode configured mean-rate value is a non-zero value, then the system does not create dynamic bypasses for the backups which request backup bandwidth that is more than the interface mode configured value. When the backup bandwidth is less than, or equal to the configured value, then the request is used to ride an existing dynamic bypass or to create a new dynamic bypass. With this configuration, all the newly created dynamic bypasses have a fixed bandwidth, meaning the value is same as the interface mode user configured non-zero mean-rate value.

A mean-rate value that is more than the current interface reservable bandwidth is not desired. Configuration succeeds with the new value even when it is more than the interface reservable bandwidth.

The **no** form of the command removes the traffic-engineering options.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures the maximum rate of packets that can go through LSP *tunnel1* (in Kbps).

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp tunnel1
device(config-router-mpls-lsp-tunnel1)# traffic-eng max-rate 20
```

The following example configures the average rate of packets that can go through LSP *tunnel1* (in Kbps).

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp tunnel1
device(config-router-mpls-lsp-tunnel1)# traffic-eng mean-rate 10
```

The following example configures the maximum size (in bytes) of the largest burst LSP *tunnel1* can send at the maximum rate.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# lsp tunnel1
device(config-router-mpls-lsp-tunnel1)# traffic-eng max-burst 10
```

The following example configures the traffic-engineering maximum rate to 1000000 kbps. for dynamic bypass MPLS Ethernet interface *2/8*.

```
device# configure
device(config)# router mpls
```

```
device(config-router-mpls)# mpls-interface ethernet 2/8
device(config-router-mpls-if-ethernet-2/8)# dynamic-bypass
device(config-router-mpls-if-ethernet-2/8-dynamic-bypass)# traffic-eng max-rate  1000000
```

traffic-engineering (MPLS)

When an MPLS-enabled device receives an IS-IS TE LSP, it stores the traffic engineering information in its Traffic Engineering database (TED). The device uses information in the TED when performing calculations to determine a path for an LSP. The user can configure the device to send out IS-IS TE LSPs for all of its MPLS-enabled interfaces.

Syntax

traffic-engineering { [**isis** [**level-1**| **level-2**]] | [**ospf** [**area** [*area_id* | **all**]]] }

no traffic-engineering { [**isis** [**level-1**| **level-2**]] | [**ospf** [**area** [*area_id* | **all**]]] }

Command Default

By default, the device does not send out IS-IS LSPs with TE extensions for its MPLS-enabled interfaces.

Parameters

isis

Advertise by way of ISIS.

level-1

Traffic-engineering for level-1.

level-2

Traffic-engineering for level-2.

ospf

Advertise by way of OSPF.

area

designate OSPF area.

area_id

Specifies OSPF area ID in IP address format.

all

Advertise in all OSPF areas.

Modes

MPLS policy mode

Usage Guidelines

The no for of the command disables the configuration.

The user must enable the device to send out IS-IS LSPs with TE extensions when the user wants CSPF to perform constraint-based path selection because information in the TED is used to make path selections using CSPF, and information in the TED comes from IS-IS LSPs with TE extensions.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures the device to send out IS-IS TE LSPs to the level-1 MPLS-enabled interface.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy)# traffic-engineering isis level-1
```

transit-session-accounting

Enables traffic statistics for transit sessions.

Syntax

transit-session-accounting

no transit-session-accounting

Command Default

By default, the command is disabled.

Modes

MPLS policy mode.

Usage Guidelines

Use the **no** form of the command disables the traffic statistics for transit sessions.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example enables transit session accounting.

```
device# configure
device(config)# router mpls
device(config-router-mpls)# policy
device(config-router-mpls-policy) transit-session-accounting
```

transport

Specifies the transport protocol for network-elements telemetry streaming.

Syntax

transport { **tcp** | **ssl** }

no transport

Command Default

TCP is specified.

Parameters

tcp

Specifies TCP as the telemetry transport protocol.

ssl

Specifies SSL as the as the telemetry transport protocol.

Modes

Telemetry-server configuration mode

Usage Guidelines

This command (and the SSL option) are available only for the gRPC-server implementation. They are not supported for the external-collector telemetry implementation.

To revert to the default TCP protocol, use the **no** form of this command.

Examples

The following example enables SSL as the telemetry transport protocol.

```
device# configure terminal
device(config)# telemetry server
device(config-server-mgmt-vrf)# do telemetry client-cert generate
device(config-server-mgmt-vrf)# transport ssl
device(config-server-mgmt-vrf)# activate
```

trigger

Defines event-handler triggers. When the trigger-condition occurs, a Python script is run.

Syntax

trigger *trigger-id* **raslog** *raslog-id* [**pattern** *posix-ext-regex*]

trigger *trigger-id* **raslog** *raslog-id* [**pattern** *trigger-pattern*]

no trigger [*trigger-id*]

Command Default

No trigger is defined.

Parameters

trigger-id

Specifies an ID number for the trigger. Valid values are 1 through 100, and must be unique per event-handler profile.

raslog *raslog-id*

Specifies a RASlog message ID as the trigger. String can be 1 through 32 characters long.

pattern *posix-ext-regex*

Specifies a POSIX extended regular expression to search within the specified RASlog message ID.

pattern *trigger-pattern*

Specifies a sequence of strings with included regular expressions to search within the specified RASlog message ID. Contains alphabets, digits and all characters supported in regex. String can be 1 through 128 characters long.

Modes

Event-handler configuration mode

Usage Guidelines

You can create from 1 through 100 triggers per profile.

You can also define one trigger as part of the **event-handler** command.

To delete one or all triggers, use the **no** form of this command, as follows:

- To delete all triggers, enter **no trigger**.

- To delete a specific trigger, enter **no trigger** *trigger-id*

Note
You cannot delete the last remaining trigger from an activated event-handler profile.

You can modify an existing trigger without deleting it and then re-creating it.

If the event-handler for which you are modifying triggers is active on the device, the changes take effect with no need to de-activate and re-activate the event-handler.

A Python event-handler script runs only if all of the following occur:

- Using the **copy** command, copy the Python file to the `flash://` location on the device.
- Using the **event-handler** command, create an event-handler profile.
- In configuration mode for that profile:
  - Using the **trigger** command, create one or more triggers.
  - Using the **action** command, specify the Python script that will be triggered.
- Using the **event-handler activate** command, activate an instance of the event handler.
- The trigger event occurs.

Examples

The following example defines triggers in two event handlers.

```
device# configure terminal
device(config)# event-handler eventHandler2
device(config-event-handler-eventHandler2)# trigger 1 raslog NSM-1001
device(config-event-handler-eventHandler2)# trigger 2 raslog NSM-1003
```

The following example defines a trigger that uses POSIX extended REGEX to search for a match within a specified RASlog message ID.

```
device# configure terminal
device(config-event-handler-eventHandler1)# event-handler eventHandler2
device(config-event-handler-eventHandler2)# trigger 1 raslog NSM-1003 pattern Interface
Ethernet 1/[1-9] is link down
```

RASlog message NSM-1003 includes "**interface** *interface-name* is link down", indicating that an interface is offline because the link is down. The REGEX searches within such a message for an interface from 1/1 through 1/9.

trigger-function

Specifies whether the action runs only if all of the triggers occur or if one is sufficient, for an implementation of an event-handler profile when multiple triggers are defined for an event-handler action.

Syntax

trigger-function { **OR** | **AND time-window** *seconds* }

no trigger-function

Command Default

The event-handler action runs if any of the triggers occur.

Parameters

OR

The event-handler action runs if any of the triggers occur.

AND

The event-handler action runs only if all of the triggers occur.

time-window *seconds*

In seconds, specify the time window within which all of the triggers must occur in order that the event-handler action runs.

Following an initial triggering of an event-handler action, any subsequent trigger launches the action an additional time if the following conditions are true:

- The **trigger-mode** parameter is set to the default **each-instance**.
- The subsequent trigger occurs within the specified **time-window**.

Modes

Event-handler activation mode

Usage Guidelines

The **no** form of this command sets the **trigger-function** setting to the default **OR** option.

Examples

The following example determines that the event-handler action runs only if all of the triggers occur within 120 seconds.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# trigger-function AND time-window 120
```

The following example resets **trigger-function** to the default **OR** option.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# no trigger-function
```

trigger-mode

For an implementation of an event-handler profile, specifies if recurring trigger conditions can launch an event-handler action more than once.

Syntax

trigger-mode *mode*

no trigger-mode

Command Default

Each time the trigger condition occurs, the event-handler action is launched.

Parameters

mode

Specifies if an event-handler action can be triggered only once or more than once.

each-instance

The event-handler action is launched on each trigger instance received.

on-first-instance

As long as the device is running, the event-handler action is launched only once. Following a device restart, the event-handler action can be triggered again.

only-once

For the duration of a device configuration, the event-handler action is launched only once.

Modes

Event-handler activation mode

Usage Guidelines

The **no** form of this command resets the **trigger-mode** setting to the default **each-instance** option.

Examples

The following example sets the trigger mode to **on-first-instance**.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# trigger-mode on-first-instance
```

The following example resets **trigger-mode** to the default value of **each-instance**.

```
device# configure terminal
device(config)# event-handler activate eventHandler1
device(config-activate-eventHandler1)# no trigger-mode
```

trustpoint sign

Configures the trustpoint to the server certificate profile that is used to sign the server certificate.

Syntax

trustpoint sign { *trustpoint-name* }

no trustpoint sign

Command Default

By default, the trustpoint is not configured.

Parameters

trustpoint-name

Defines the name of the trustpoint you are configuring. This name needs to be the same as that of the trustpoint created by the **crypto ca trustpoint** command. The string for the name cannot be left blank. The length of the string can range from 1 through 64 characters.

Modes

SSH server profile server configuration mode

Usage Guidelines

Use the **no** form of the command to remove the trustpoint configured on the device.

The trustpoint must be configured before you run this command. The same trustpoint must be used to sign and import the server certificate using the following commands: **crypto ca authenticate**, **crypto ca enroll**, **crypto ca import**, and **crypto ca trustpoint**.

Examples

The following example configures a trustpoint named myca.

```
device# configure terminal
device(config)# ssh server certificate profile server
device(ssh-server-cert-profile-server)# trustpoint sign myca
```

ttl

Configures the time to live (TTL) value for a tunnel interface.

Syntax

ttl *ttl-value*

no ttl

Parameters

ttl-value

Specifies the TTL value. The range is from 1 to 255.

Command Default

The default TTL value is 255.

Modes

Interface tunnel configuration mode

Usage Guidelines

Use the **no** form of this command to revert to the default value.

Examples

This example configures the TTL value for the tunnel interface.

```
device# configure terminal
device (config)# interface tunnel 5
device(config-intf-tunnel-5)# mode gre ip
device(config-intf-tunnel-5)# source 10.1.1.10
device(config-intf-tunnel-5)# source ve 4
device(config-intf-tunnel-5)# destination 10.1.1.11
device(config-intf-tunnel-5)# router-interface ve 3
device(config-intf-tunnel-5)# dscp-ttl-mode pipe
device(config-intf-tunnel-5)# ttl 64
```

tunable-optics

This command assigns channels to tunable optic interfaces (T-SFP+) for specific wavelengths.

Syntax

tunable-optics sfpp channel *channel_number*

Command Default

The T-SFP+ optic defaults to a "no wavelength" state before being activated.

Modes

Interface configuration mode

Usage Guidelines

Tunable SFP+ optics are optional hardware that can be installed with optical SFPs.

If you are installing a T-SFP+ in a 144S port, the T-SFP+ optic needs to be installed in both ends of the cable. The T-SFP+ at each end of the cable link must be configured at the same wavelength by setting them to the same channel on each device.

Failure to duplicate the channel setting may allow the link to come online, but the link behavior may be erratic.

If the firmware determines an error is exceeding a specified limit, a RASLOG message event occurs and the port is taken offline.

The T-SFP+ interface defaults to a "no wavelength" state. When a supported Extreme Networks device boots, the firmware sets the desired wavelength of the T-SFP+ optic.

When a T-SFP+ interface is installed it is very important that the interface is configured to the same channel (wavelength) at both ends. Use the **show media tunable-optic-sfpp** command to determine the currently configured channel.

T-SFP+ interfaces are tuned to specific wavelengths and frequencies using pre-defined channels.

Refer to the *Extreme SLX-OS Monitoring Configuration Guide* for complete information on tunable optics.

The following tables lists the frequency and wavelength assigned to channels for tunable SFP+ optic interfaces.

Table 22: Supported wavelengths and channel numbers

Channel	Frequency (THz)	Wavelength (nm)
1	191.10	1568.77
2	191.15	1568.36
3	191.20	1567.95
4	191.25	1567.54
5	191.30	1567.13
6	191.35	1566.72
7	191.40	1566.31
8	191.45	1565.90
9	191.50	1565.50
10	191.55	1565.09
11	191.60	1564.68
12	191.65	1564.27
13	191.70	1563.86
14	191.75	1563.45
15	191.80	1563.05
16	191.85	1562.64
17	191.90	1562.23
18	191.95	1561.83
19	192.00	1561.42
20	192.05	1561.01
21	192.10	1560.61
22	192.15	1560.20
23	192.20	1559.79
24	192.25	1559.39
25	192.30	1558.98
26	192.35	1558.58
27	192.40	1558.17
28	192.45	1557.77
29	192.50	1557.36
30	192.55	1556.96
31	192.60	1556.55
32	192.65	1556.15

Table 22: Supported wavelengths and channel numbers (continued)

Channel	Frequency (THz)	Wavelength (nm)
33	192.70	1555.75
34	192.75	1555.34
35	192.80	1554.94
36	192.85	1554.54
37	192.90	1554.13
38	192.95	1553.73
39	193.00	1553.33
40	193.05	1552.93
41	193.10	1552.52
42	193.15	1552.12
43	193.20	1551.71
44	193.25	1551.32
45	193.30	1550.92
46	193.35	1550.52
47	193.40	1550.12
48	193.45	1549.72
49	193.50	1549.32
50	193.55	1548.91
51	193.60	1548.51
52	193.65	1548.11
53	193.70	1547.72
54	193.75	1547.32
55	193.80	1546.92
56	193.85	1546.52
57	193.90	1546.12
58	193.95	1545.72
59	194.00	1545.32
60	194.05	1544.92
61	194.10	1544.53
62	194.15	1544.13
63	194.20	1543.73
64	194.25	1543.33
65	194.30	1542.94
66	194.35	1542.54

Table 22: Supported wavelengths and channel numbers (continued)

Channel	Frequency (THz)	Wavelength (nm)
67	194.40	1542.14
68	194.45	1541.75
69	194.50	1541.35
70	194.55	1540.95
71	194.60	1540.56
72	194.65	1540.16
73	194.70	1539.77
74	194.75	1539.37
75	194.80	1538.98
76	194.85	1538.58
77	194.90	1538.19
78	194.95	1537.79
79	195.00	1537.40
80	195.05	1537.00
81	195.10	1536.61
82	195.15	1536.22
83	195.20	1535.82
84	195.25	1535.43
85	195.30	1535.04
86	195.35	1534.64
87	195.40	1534.25
88	195.45	1533.86
89	195.50	1533.47
90	195.55	1533.07
91	195.60	1532.68
92	195.65	1532.29
93	195.70	1531.90
94	195.75	1531.51
95	195.80	1531.12
96	195.85	1530.72
97	195.90	1530.33
98	195.95	1529.94
99	196.00	1529.55
100	196.05	1529.16

Table 22: Supported wavelengths and channel numbers (continued)

Channel	Frequency (THz)	Wavelength (nm)
101	196.10	1528.77
102	196.15	1528.38

Examples

Typical command example.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# tunable-optics sfpp channel 5
device(conf-if-eth-0/1)# do show media optical-monitoring
N/A - Not Available.
N/S - Optical-monitoring Not Supported.
Port            Module      Supply       Channel      Frequency Wavelength Bias
Channel
                Temperature Voltage      TX Power     Error     Error      Current
RX Power
                ( C )       ( mVolts )   ( uWatts )   ( GHz )   ( nm )     ( mAmps )
( uWatts )
=============== =========== ============ ============ ========= ========== ============
============
Eth 0/1         36          3291.6       694.4        0.0       0.000      38.550
748.8

Eth 0/24                                 N/S

Eth 0/32        33          3317.1       685.1        0.0       0.000      37.132
914.5

Eth 0/48                                 N/S
```

tunneled-arp-trap enable

Enables ARP (Address Resolution Protocol) packets that come through a tunnel to be trapped to CPU.

Syntax

tunneled-arp-trap enable

no tunneled-arp-trap enable

Command Default

By default, ARP packets that come through a tunnel are trapped to CPU.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of the command to disable the trapping of ARP packets that come through a tunnel.

Examples

The following example enables the trapping of ARP packets that come through a tunnel.

```
device# configure terminal
device(config)# tunneled-arp-trap enable
```

The following example disables the trapping of ARP packets that come through a tunnel.

```
device# configure terminal
device(config)# no tunneled-arp-trap enable
```

tx-frame-count

Configures the transmission frame count.

Syntax

tx-frame-count *frame-count*

no tx-frame-count

Parameters:

frame-count

Specifies the transmission frame count. The range is from 1 to 1000.

Command Default

The default value for tx-frame-count is 10 .

Modes

Y1731 configuration mode

Usage Guidelines

Use the **no** form of the command to delete the transmission frame count configuration.

Examples

This example shows how to configure the transmission frame count.

```
device# configure terminal
device (config-cfm)# protocol cfm
device (config-cfm)# y1731
device(config-cfm-y1731)# test-profile my_test_profile
device(config-cfm-y1731-test-profile-my_test_profile)# type delay-measurement
device(config-cfm-y1731-test-profile-my_test_profile)# tx-interval 60
device(config-cfm-y1731-test-profile-my_test_profile)# measurement-interval 30
device(config-cfm-y1731-test-profile-my_test_profile)# start at 00:00:00 daily
device(config-cfm-y1731-test-profile-my_test_profile)# stop at 23:59:00
device(config-cfm-y1731-test-profile-my_test_profile)# cos 7
device(config-cfm-y1731-test-profile-my_test_profile)# threshold maximum 3294967295
device(config-cfm-y1731-test-profile-my_test_profile)# tx-frame-count 300
```

tx-interval

Configures the transmission interval.

Syntax

tx-interval *tx-interval*

no tx-interval

Parameters:

tx-interval

Specifies the transmission interval in seconds. Valid values can be 1, 10, 60, or 600 seconds.

Command Default

The default value for tx interval is 1 second.

Modes

Y1731 configuration mode

Usage Guidelines

Use the **no** form of the command to delete the transmission interval configuration.

Examples

This example shows how to configure the transmission interval.

```
configure terminal
device (config-cfm)# prtocol cfm
device (config-cfm)# y1731
device(config-cfm-y1731)# test-profile my_test_profile
device(config-cfm-y1731-test-profile-my_test_profile)# type delay-measurement
device(config-cfm-y1731-test-profile-my_test_profile)# tx-interval 60
```

tx-label-silence-timer

Sets the length of the EOL transmit label silence timer for LDP-IGP synchronization.

Syntax

tx-label-silence-timer *milliseconds*

no tx-label-silence-timer

Command Default

The default value is 1000 milliseconds.

Parameters

milliseconds

Specifies the EOL transmit label silence timer in milliseconds. Enter an integer from 100 to 60000.

Modes

MPLS LDP EOL configuration mode

Usage Guidelines

Use the **no** form of the resets the default value of 1000 milliseconds.

Examples

The following example sets the length of time for the EOL transmit label silence timer to 2000 milliseconds.

```
device(config)# router mpls
device(config-router-mpls)# ldp
device(config-router-mpls-ldp)# eol
device(config-router-mpls-ldp-eol)# tx-label-silence-timer 2000
```

type

Configure a profile type as ETH-DM or ETH-SLM.

Syntax

type [**delay-measurement** | **synthetic-loss-measurement**]

Parameters:

delay-measurement

Specifies the profile type as delay management.

synthetic-loss-measurement

Specifies the profile type as synthetic loss measurement.

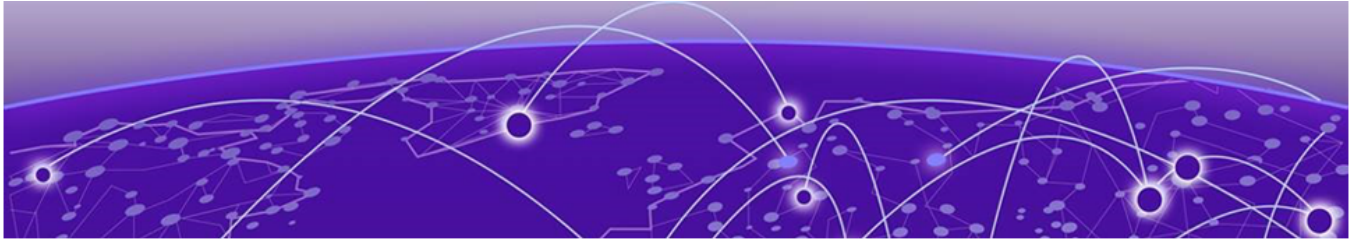
Modes

Y.1731 configuration mode

Examples

This example shows how to configure the profile type as delay measurement or as synthetic loss measurement .

```
device# configure terminal
device (config-cfm)# prtocol cfm
device (config-cfm)# y1731
device(config-cfm-y1731)# test-profile my_test_profile
device(config-cfm-y1731-test-profile-my_test_profile)# type delay-measurement

device# configure terminal
device (config-cfm)# prtocol cfm
device (config-cfm)# y1731
device(config-cfm-y1731)# test-profile my_test_profile
device(config-cfm-y1731-test-profile-my_test_profile)# type synthetic-loss-measurement
```



Commands U - Z

udld enable on page 2748
underflow-limit on page 2749
underlay-mdt-default-group on page 2751
underlay-mdt-group on page 2752
undeploy-force on page 2754
unlock username on page 2755
user-id on page 2756
update onie on page 2758
update-time on page 2759
usb on page 2761
usb dir on page 2762
usb remove on page 2763
use-v2-checksum on page 2764
user (alias configuration) on page 2765
username on page 2766
username on page 2770
vc-id on page 2771
vc-mode on page 2772
version (ERP) on page 2774
virtual-ip on page 2775
virtual-mac on page 2777
vlan on page 2778
vlan (EVPN) on page 2779
vpn-statistics on page 2781
vrf on page 2782
vrf (epvn IRB) on page 2783
vrf forwarding on page 2785
vrf-lite-capability on page 2786
vrrp-acceptmode-disable on page 2787
vrrp-extended-group on page 2788
vrrp-group on page 2789
vtep-discovery on page 2791
write erase on page 2792
wtb-time on page 2793

wtr-time on page 2794
y1731 on page 2795

udld enable

Enables the Unidirectional Link Detection (UDLD) protocol on an interface.

Syntax

udld enable

no udld enable

Command Default

Disabled on interfaces by default.

Modes

Interface configuration mode

Usage Guidelines

Use **no udld enable** to unblock the interface if it has been blocked by the UDLD protocol.

Examples

The following example enable UDLD on a specific Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# udld enable
```

underflow-limit

Sets the underflow-limit to the input value.

Syntax

underflow-limit *value*

no underflow-limit

Command Default

The default is set to zero (0), meaning there is no premature adjustment because of underflow.

Parameters

value

The selected number of consecutive samples that have to be below the threshold to trigger a premature adjustment.

Modes

MPLS sub-configuration modes

config-mpls-autobw-template-template1

config-mpls-lsp-lsp1

Usage Guidelines

The **no** function of the command sets the underflow-limit back to the default value.

MPLS is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example configures the underflow-limit in auto-bandwidth template1 to 10.

```
device>configure
device(config)# router mpls
device(config-router-mpls)# autobw-template template1
device(config-router-mpls-autobw-template-template1)# underflow-limit 10
```

The following example configures the underflow-limit for LSP1 to 10.

```
device>configure
device(config)# router mpls
device(config-router-mpls)# lsp lsp1
```

```
device(config-router-mpls-lsp-lsp1)# autobw
device(config-router-mpls-lsp-lsp1-autobw)# underflow-limit 10
```

underlay-mdt-default-group

Creates a underlay MDT default group instance.

Syntax

underlay-mdt-default-group*Group-IP*

no underlay-mdt-default-group

Command Default

Global configuration mode

Parameters

Group-IP

Specifies the IP address of the group.

Modes

Global configuration mode

Usage Guidelines

The default mdt group needs to be configured first and removed last in the optimized-replication mode.

When all vlans are removed from a group and the group config is removed. The same rule applies to BDs as well.

The **no underlay-mdt-group GROUP vlan add VLAN-RANGE** command can be used to remove a config if there is an exact match with the current config line or the remove option is used to remove vlans or BDs from a group.

Examples

The following example configures underlay mdt default group.

```
underlay-mdt-default-group 239.0.0.100
```

underlay-mdt-group

Creates a underlay MDT group instance.

Syntax

underlay-mdt-group *GROUP-IP* [**default** | [[**vlan** [**add** | **remove** *VLAN* , | *VLAN-RANGE* +] | [[**bridge-domain** [**add** | **remove**] (*BD* , | (*BD-RANGE* ,) +]

no underlay-mdt-group

Command Default

Global configuration mode

Parameters

add

Adds the VLAN or bridge-domain.

bridge-domain

Specifies the bridge-domain.

(BD, BD-RANGE) +

Specifies BD and BD range.

default

Specifies the default group.

GROUP-IP

Specifies the IP address of the Group-IP.

remove

Removes the selected VLAN or bridge-domain.

vlan

Specifies the VLAN.

(VLAN, VLAN-RANGE) +

Specifies VLAN and VLAN-RANGE.

Modes

Global configuration mode

Usage Guidelines

The default mdt group needs to be configured first and removed last in the optimized-replication mode.

When all vlans are removed from a group and the group config is removed. The same rule applies to BDs as well.

The **no underlay-mdt-group GROUP vlan add VLAN-RANGE** command can be used to remove a config if there is an exact match with the current config line or the remove option is used to remove vlans or BDs from a group.

Examples

The following example configures underlay mdt group.

```
underlay-mdt-group 239.0.0.1 vlan add 10-12,20
underlay-mdt-group 239.0.0.3 vlan add 30
underlay-mdt-group 239.0.0.4 vlan add 40
underlay-mdt-group 239.0.0.5 bridge-domain add 50,60-70
```

undeploy-force

Removes the configured TPVM and its associated disks.

Syntax

undeploy-force

Modes

TPVM Configuration mode

Usage Guidelines

The *no* format of this command is not available.

The **no deploy** command will bring down TPVM and remove the TPVM and associated disks from the running configuration. However, in some cases, the command might fail to remove the configured disks. To rectify this issue, use this command to completely remove the TPVM and its associated disks. This command will remove the associated disks from the running configuration without failing.

You can also use this command to forcibly remove any virtual disks that were retained when TPVM was uninstalled using the **no deploy** command.

Examples

This example removes the configured TPVM and its associated disks:

```
SLX (config-tpvm-TPVM)# undeploy-force
```

unlock username

Unlocks a locked user account.

Syntax

unlock username *name*

Parameters

name

Specifies the name of the user account.

Modes

Privileged EXEC mode

Usage Guidelines

Use this command to unlock a user who has been locked out because of unsuccessful login attempts. A user account is locked by the system when the configured threshold for login retries has been reached.

Examples

The following example unlocks a user account.

```
device# unlock username testUser
Result: Unlocking the user account is successful
```

user-id

Enters into the configuration mode for each BMC User ID. BMC has 10 pre-defined users with IDs in the range 1-10. Each user ID is configured independently and this command enters into each user ID's configuration mode.

Syntax

user-id *<user-id-value>*

no user-id *<user-id-value>*

Parameters

user-id-value

The BMC User ID to be configured. Each of BMC's 10 user IDs have to be configured individually.

Modes

BMC User ID mode

Usage Guidelines

The **no** format of this command resets the default configuration of the specified BMC User ID.

Examples

This example shows how to navigate into the configuration mode for the BMC User ID 1.

```
SLX # configure terminal
SLX (config)# bmc
SLX (config-bmc)# user-id 1
SLX (config-bmc-1)#
```

This example shows the configuration commands available inside the BMC User ID Configuration mode. Only the user password can be changed from within this mode.

```
SLX (config-bmc)# user-id 1
SLX (config-bmc-user-1)# ?
Possible completions:
  describe   Display transparent command information
  do         Run an operational-mode command
  exit       Exit from current mode
  help       Provide help information
  no         Negate a command or set its defaults
  password   Password for BMC user
  pwd        Display current mode path
  top        Exit to top level and optionally run command
SLX (config-bmc-user-1)#
```

This example shows the resetting of the BMC User ID configuration to its default.

```
SLX # configure terminal
SLX (config)# bmc
SLX (config-bmc)# do show running-config bmc
bmc
 user-id 1
  password $9$VaXhc9WCy+1IwRU2ZaS2vQ==
 !
 user-id 2
  password $9$VaXhc9WCy+1IwRU2ZaS2vQ==
 !
 user-id 3
 !
!

SLX (config-bmc)# no user-id 1
SLX (config-bmc)# do show running-config bmc
bmc
 user-id 2
  password $9$VaXhc9WCy+1IwRU2ZaS2vQ==
 !
 user-id 3
 !
!
```

update onie

Command to download and install the ONIE, ONIE-GRUB, and DIAG images.

Syntax

update onie { **ftp** | **sftp** | **scp** } **directory** *directory-name* **file** *image-file-name* **host** *ip-address* **user** *user-name* **password** *password* **use-vrf** *vrf-name*

Modes

Privileged EXEC Mode

Usage Guidelines

This command is only supported on the SLX 9150, SLX 9250, Extreme 8720, and Extreme 8520 devices.

This command will install ONIE, DIAG, and ONIE-GRUB at the same time. There will be a total of three device reboots during the update process as each item is installed.

Note

ONIE, DIAG, and ONIE-GRUB cannot be installed individually.

Examples

This example shows the ONIE update command usage.

```
SLX# update onie sftp host 10.10.10.1 user admin-user password password directory /media/
image-store/ filename onie-updater-x86_64-quanta_dnv-r0-14-ix8t_3abca use-vrf mgmt-vrf
```

update-time

Configures the interval at which BGP next-hop tables are modified. BGP next-hop tables should always have IGP (non-BGP) routes.

Syntax

update-time *sec*

no update-time *sec*

Command Default

This option is disabled.

Parameters

sec

Update time in seconds. Range is from 0 through 30. Default is 5 seconds.

Modes

BGP address-family IPv4 unicast configuration mode

BGP address-family IPv6 unicast configuration mode

BGP address-family IPv4 unicast VRF configuration mode

BGP address-family IPv6 unicast VRF configuration mode

Usage Guidelines

Use the **no** form of this command to restore the defaults.

The update time determines how often the device computes the routes (next-hops). Lowering the value set by the **update-time** command increases the convergence rate.

By default, the device updates the BGP4 next-hop tables and affected BGP4 routes five seconds following IGP route changes. Setting the update time value to 0 permits fast BGP4 convergence for situations such as a link failure or IGP route changes, starting the BGP4 route calculation in subsecond time.

Note
Use the **advertisement-interval** command to determine how often to advertise IGP routes to the BGP neighbor.

Examples

This example sets the BGP4+ update-time interval to 30.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family ipv6 unicast vrf red
device(config-bgp-ipv6u-vrf)# update-time 30
```

usb

Enables or disables an attached USB device. The device is inaccessible until it is enabled.

Syntax

usb { **on** | **off** }

Parameters

on

Turns the USB device on.

off

Turns the USB device off.

Modes

Privileged EXEC mode

Usage Guidelines

This command is executed on the local device. A device reload automatically turns the USB device off.

This command is supported only on the local device.

Examples

To enable a USB device attached to the local device:

```
device# usb on

USB storage enabled
```

To disable a USB device attached to the local device:

```
device# usb off

USB storage disabled
```

usb dir

Lists the contents of an attached USB device.

Syntax

usb dir

Modes

Privileged EXEC mode

Usage Guidelines

This command is executed on the local device. The USB device must be enabled before this function is available.

This command is supported only on the local device.

Examples

To list the contents of the USB device attached to the local device:

```
device# usb dir
firmwarekey\ 0B 2016 Aug 15 15:13
support\ 106MB 2016 Aug 24 05:36
support1034\ 105MB 2016 Aug 23 06:11
config\ 0B 2016 Aug 15 15:13
firmware\ 380MB 2016 Aug 15 15:13
Available space on usbstorage 74%
```

usb remove

Removes a file from an attached USB device.

Syntax

usb remove directory *directory* **file** *file*

Parameters

directory *directory*

Specifies one the name of the directory where the file you want to remove is located. Valid USBstorage directories are /firmware, /firmwarekey, /support, and /config.

file *file*

Specifies the name of the file to be removed.

Modes

Privileged EXEC mode

Usage Guidelines

This command is executed on the local device. The USB device must be enabled before this function is available.

This command is supported only on the local device.

Examples

To remove a configuration file from a USB device attached to the local device:

```
device# usb remove directory config file startup-config.backup
```

use-v2-checksum

Enables the v2 checksum computation method for a VRRPv3 IPv4 session.

Syntax

use-v2-checksum

no use-v2-checksum

Command Default

VRRPv3 uses the v3 checksum computation method.

Modes

Virtual-router-group configuration mode

Usage Guidelines

Some non-Extreme Networks devices only use the v2 checksum computation method in VRRPv3. This command enables v2 checksum computation method in VRRPv3 and provides interoperability with these non-Extreme Networks devices.

The **no** form of this command enables the default v3 checksum computation method in VRRPv3 sessions.

Examples

The following example shows the v2 checksum computation method enabled for an VRRPv3 IPv4 session on an Extreme Networks device.

```
device(config)# protocol vrrp
device(config)# interface ve 100
device(config-Ve-100)# vrrp-group 10 version 3
device(config-vrrp-group-10)# use-v2-checksum
```

user (alias configuration)

Launches the user-level alias configuration mode, in which you can manage user aliases.

Syntax

user *username*

no user *username*

Parameters

username

Specifies the account login name.

Modes

Alias configuration mode

Usage Guidelines

To delete all aliases defined for a specified user, enter the **no** form of this command.

Examples

The following example accesses user-alias configuration mode for the user jdoe, and defines a user-level alias named "sv" for the **show version** command.

```
device# configure terminal
device(config)# alias-config
device(config-alias-config)# user jdoe
device(config-user-jdoe)# alias sv "show version"
```

username

Creates and configures a user account.

Syntax

username *username* **password** *password* **role** *role_name* [**access-time** *HHMM* **to** *HHMM*] [**desc** *description*] [**enable** { **true** | **false** }] [**encryption-level** { **0** | **7** | **10** }] [**expire** { **never** | *YYYY-MM-DD* }] [**role** *role_name*] [**acct-inactivity-expiry-period** *1-180*] [**acct-inactivity-warning-period** *1-120*]

no username *name*

Parameters

username

Specifies the account login name. This includes the system default accounts, *root*, *admin* , and *user*. You can also use this command to create *user defined* accounts.

access-time *HHMM* **to** *HHMM*

Restricts the hours that the user may be logged in. Valid values range from 0000 through 2400 in 24-hour format. By default, users are granted 24 hour access.

For example, to restrict access to the daily work schedule, use **access-time 0800 to 1800** . By default, there is no access-time limitation. To change access time, include both the new "from" time and "to" time. To restore default access time, specify **access-time** *0000* **to** *2400* .

desc *description*

This is an optional parameter. Specifies a description of the account (optional). The description can be up to 64 characters long, and can include any printable ASCII character, except for the following characters: single quotation marks (‘), double quotation marks ("), exclamation point (!), colon (:), and semi-colon (;). If the description contains spaces, enclose the complete description text in double quotation marks.

enable

Enables or disables the account.

true

(Default) Enables the account.

false

Disables the account. A user whose account is disabled cannot log in.

expire

Specifies the date on which the user account expires.

never

(Default) Does not specify a user account expiration date.

YYYY-MM-DD

Specifies the date on which the user account expires.

password *password*

Specifies the account password. To use the exclamation mark (!) character, either precede it with the escape character (\)—. **secret\!password** —or enclose the password within double quotes—"secret!password".

role *role_name*

Specifies the role assigned to the account.

encryption-level { **0** | **7** | **10** }

Specifies the password encryption level. The values are 0 (clear text), 7 (encrypted), and 10 (SHA512 hash). *SHA512 hash* is the default. If service password-encryption is enabled, it overrides a user-level setting.

acct-inactivity-expiry-period *1-180*

Specifies the number of days an account is allowed to be inactive before it is disabled.

acct-inactivity-warning-period *1-120*

The time duration (in days) after which warning will be generated prior to account getting disabled.

Modes

Global configuration mode

Usage Guidelines

This command can also be used to reset the default password for the system accounts, *root*, *admin*, and *user*.

The *username* must be of 1-40 characters. It must begin with a letter or underscore and contain only letters, numbers, underscore (_) and period(.) symbols. Username is case sensitive and cannot be the same as that of an existing role.

When creating a username, you must specify a password and a role. When modifying a username, it is sufficient to enter the **username** *username* command, followed by the new values.

The maximum number of user accounts on a device is 64.

Note
When configuring the expiry date for a user account, do not configure beyond 19th of January 2038 (2038-01-19). When you configure a date that is beyond this cut off date, the user account will not expire and the account will not get locked.

If a user's password, access time, or role is changed, any existing login sessions for that user are terminated.

To specify **access-time**, use the system time defined for the Extreme Networks operating system. For the current system time, use the **show clock** command.

To delete a user account, enter the **no username** with the name of the account to be deleted.

The system default accounts cannot be deleted. However, passwords for these accounts can expire. Password expiry will depend on the configuration of the `password-attributes max-password-age` configuration.

Note

This NOTE is applicable when upgrading from SLX-OS v 20.6.2 and below to the current SLX-OS version.

For the *root* account, to apply password expiry, you must use the `no password-attributes max-password-age` to remove the existing configuration. Then, use the `password-attribute max-password-age` command to set the desired password expiry configuration.

Examples

The following example configures a user account.

```
device# configure terminal
device(config) # username testUser password ******** role user desc testUser
```

The following example modifies an existing user account.

```
device# configure terminal
device(config) # username testUser desc "add op test user"
```

The following example modifies an existing user account, restricting the hours that an existing user may be logged in from 08:00 AM through 06:00 PM.

```
device# configure terminal
device(config) # username testUser access-time 0800 to 1800
```

The following example sets the expiry period for the account *testUser* to 120 days. It also configures warning period to 90 days. A warning log entry is generated after the account's inactivity (in number of days) crosses the configured warning period. The user account gets locked after the expiry period.

Ensure that the **acct-inactivity-warning-period** value is lesser than or equal to the period specified in the **acct-inactivity-expiry-period** setting.

```
device # configure terminal
device(config) # username testUser acct-inactivity-expiry-period 120 acct-inactivity-
warning-period 90
```

The following example shows how to set the password and password expiry parameters for the system default account, the *admin* account.

```
device # configure terminal
device(config) # username admin password falsepassword desc admin-account expire
```

```
2025-12-31 role admin acct-inactivity-warning-period 20
device(config) # password-attributes max-password-age 200
```

username

Creates and configures a user account.

Syntax

username *username* **password** *password*

Parameters

username

Specifies the account login name.

password *password*

Specifies the account password. To use the exclamation mark (!) character, either precede it with the escape character (\)—. **secret\!password** —or enclose the password within double quotes—"secret!password".

Modes

GRUB configuration mode

Usage Guidelines

The *username* must be of 1-40 characters. It must begin with a letter or underscore and contain only letters, numbers, underscore (_) and period(.) symbols. Username is case sensitive and cannot be the same as that of an existing role. When creating a username, you must specify a password.

Examples

The following example configures a user account for securing GRUB.

```
SLX # configure terminal
SLX (config)# grub
SLX (config-grub)# username testUser password ********
SLX (config-grub)#
```

vc-id

Configures a virtual connection identifier (VC ID) for a bridge domain.

Syntax

vc-id *id*

no vc-id

Command Default

A virtual connection identifier is not configured.

Parameters

id

Specifies a virtual connection identifier. The range is from 1 through 4294967295.

Modes

Bridge-domain configuration mode.

Usage Guidelines

This feature is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

For VLL, the VC ID is the VLL cross-connection instance ID.

For VPLS, the VC ID is the virtual switch instance ID.

When a VC ID is configured for a VPLS bridge domain, it is used for all configured pseudowires (circuit emulation services).

The **no** form of the command removes the VC ID configuration.

Examples

The following example shows how to configure a VC ID (5) for bridge domain 4.

```
device# configure terminal
device(config)# bridge-domain 4
device(config-bridge-domain-4)# vc-id 5
```

vc-mode

Configures the virtual connection (VC) mode for a pseudowire (PW) profile.

Syntax

vc-mode { **raw** | **raw-passthrough** | **tag** }

no vc-mode

Command Default

The default VC mode is **raw** .

Parameters

raw

Specifies using raw mode. At VC label imposition, when a tagged packet is received on a tagged AC endpoint, the VLAN tag is removed before it is sent out on the wire. Untagged packets that are received on an untagged AC endpoint are encapsulated as is and sent out on the wire.

raw-passthrough

(is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.) Specifies using raw-passthrough mode, which enables interoperation with third-party devices. When all endpoints are configured as tagged endpoints, raw passthrough mode behaves the same way as tagged mode. When all endpoints are configured as untagged endpoints, raw-passthrough mode behaves the same way as raw mode. Select the **raw-passthrough** option, when all endpoints are configured as untagged endpoints (even when peer devices signal the PW VC mode as raw).

tag

Note
The **tag** option is not supported on the SLX 9640 platform.

Specifies using tag mode. At VC label imposition, when a tagged packet is received on a tagged AC endpoint, the packet is encapsulated as is and sent out on the wire. When an untagged packet is received on an untagged AC endpoint, a dummy tag is added and it is sent out on the wire.

Modes

Pseudowire-profile configuration mode.

Usage Guidelines

The **no** form of the command restores the default value.

The **raw-passthrough** parameter is supported on the Extreme 8820, SLX 9740, SLX 9640, and SLX 9540 devices only.

Examples

The following example shows how to set the VC mode to **raw-passthrough** for a PW profile named test.

```
device# configure terminal
device(config)# pw-profile test
device(config-pw-profile-test)# vc-mode raw-passthrough
```

The following example shows how to set the VC mode to **tag** for a PW profile named test.

```
device# configure terminal
device(config)# pw-profile test
device(config-pw-profile-test)# vc-mode tag
```

version (ERP)

Configures an ITU-T G.8032 Version number for Ethernet Ring Protection (ERP).

Syntax

version *number*

no version

Command Default

The default Version number is 2.

Parameters

number

Specifies an ITU-T G.8032 Version number.

Modes

ERP configuration mode

Usage Guidelines

Use the **no** form of this command to restore the default.

Examples

The following example configures Version 1.

```
device# configure terminal
device(config)# erp 1
device(config-erp-1)# version 1
```

virtual-ip

Configures a virtual IPv4 address or IPv6 address for the virtual router.

Syntax

virtual-ip { *ipv4-address* | *ipv6-address* }

no virtual-ip { *ipv4-address* | *ipv6-address* }

Parameters

ipv4-address

Virtual IPv4 address of the virtual router.

ipv6-address

Virtual IPv6 address of the virtual router.

Modes

Virtual-router-group configuration mode

Usage Guidelines

The virtual IPv4 address or IPv6 address is the IP address that an end-host sets as its default gateway. The virtual IP address must belong to the same subnet as the underlying interface. A maximum of 16 virtual IP addresses can be configured for VRRP; only one virtual IP address can be configured for VRRP-E. The session is enabled as soon as the first virtual IP address is configured.

You can perform this command for VRRP or VRRP-E. VRRPv3 introduced the ability to use an IPv6 address when an IPv6 VRRPv3 group is configured.

This command accepts both fe80/10 link local addresses or fe80/64 addresses as virtual-IP.

Enter the **no virtual-ip** command with a specified virtual IP address to delete the specified virtual IP address

Examples

To assign a virtual IP address of 192.53.5.1 to the VRRP virtual group 1:

```
device(config)# protocol vrrp
device(config)# interface ethernet 1/6
device(conf-if-eth-1/6)# vrrp-group 1
device(config-vrrp-group-1)# virtual-ip 192.53.5.1
```

To assign a virtual IP address of 192.53.5.1 to the VRRP-E virtual group 1:

```
device(config)# protocol vrrp
device(config)# interface ve 20
device(config-ve-20)# vrrp-group-extended 1
device(config-vrrp-extended-group-1)# virtual-ip 192.53.5.1
```

To assign a virtual IPv6 address of 2001:2019:8192::1 to the VRRP-Ev3 virtual group 19:

```
device(config)# ipv6 protocol vrrp-extended
device(config)# interface ve 2019
device(config-ve-2019)# ipv6 address 2001:2019:8192::122/64
device(config-ve-2019)# ipv6 vrrp-extended-group 19
device(config-vrrp-extended-group-19)# virtual-ip 2001:2019:8192::1
```

virtual-mac

Enables generation of a virtual MAC with 0 IP hash.

Syntax

virtual-mac *virtual_mac_address*

Parameters

virtual_mac_address

Specifies a virtual MAC address.

Modes

VRRP-Extended group configuration mode

Usage Guidelines

The distributed VXLAN gateway functionality depends on VRRP-E for multi-homing. By default, the VRRP-E virtual MAC is derived as 02:e0:52:*<2-byte-ip-hash>*:*<1-byte-vrid>*. The VXLAN gateway requires that the virtual MAC be a function of only VRID. The two-byte hash of the virtual IP should be set to zeros, for example, 02e0.5200.00xx:100.

Examples

To enable the generation of a virtual MAC:

```
device# configure terminal
device(config)# interface ve 10
device(config-Ve-10)# vrrp-extended-group 100
device(config-vrrp-extended-group-100)# virtual-mac 02e0.5200.00xx:100
```

vlan

Specifies a VLAN and enters VLAN configuration mode.

Syntax

vlan *vlan_id*

no vlan *vlan_id*

Command Default

No VLAN is configured.

Parameters

vlan_id

Specifies a VLAN ID. Range is from 1 through 4090.

Modes

Global configuration mode

Usage Guidelines

Use the **no** form of this command to delete a VLAN.

Examples

To configure VLAN 10:

```
device# configure terminal
device(config)# vlan 10
device(config-vlan-10)#
```

vlan (EVPN)

Specifies a VLAN, or adds or removes a range of VLANs, for an Ethernet Virtual Private Network (EVPN) instance.

Syntax

vlan *VLAN-ID*

no vlan *VLAN-ID*

vlan { **add** | **remove** } {*VLAN-range* }

Command Default

Disabled

Parameters

VLAN-ID

Specifies a VLAN.

add

Adds a range of VLANs to the default EVPN instance.

remove

Removes a range of VLANs from the default EVPN instance.

VLAN-range

Specifies a hyphen-delimited VLAN range.

Modes

EVPN configuration mode

Usage Guidelines

Each VLAN/BD added to an EVPN configuration is considered as an EVPN instance and is assigned a unique EVPN instance ID (EVI) internally. The EVI is calculated as shown in the following table.

Table 23: Calculating EVI values from VLAN/BD values

VLAN/BD	EVI value
VLAN: 1–4096	VLAN ID
BD: 1–4096	BD ID + 4096

Important
To interoperate with third-party vendors, the RTs across the interoperating devices must be the same. If third-party devices do not support automatic RT assigment, or the EVIs are not calculated as shown in the above table, the VLAN/BD instances must be configured manually to ensure that RTs across the devices are compatible.

Examples

The following example specifies a VLAN and enter VLAN configuration mode.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# vlan 100
device(evpn-vlan-100)#
```

The following example adds VLANs 100 through 200 to the default EVPN instance.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# vlan add 100-200
```

The following example removes VLANs 150 through 180 from the default EVPN instance.

```
device# configure terminal
device(config)# evpn
device(config-evpn-default)# vlan remove 150-180
```

vpn-statistics

Enables VPN statistics for a VRF.

Syntax

vpn-statistics

no vpn-statistics

Command Default

No RD is assigned to the VRF.

Parameters

as-num

Composed of the local ASN number followed by a colon ":" and a unique arbitrary number. For example 3:6.

ip-num:id

Composed of the local IP address followed by a colon ":" and a unique arbitrary number.

Modes

VRF configuration mode

Usage Guidelines

The **no** form of the command returns to the default setting.

Examples

The following example shows how to enable VPN statistics for a VRF.

```
device# configure terminal
device(config)# vrf vpn1
device#(config-vrf-vpn1)# rd 1:2
device#(config-vrf-vpn1)# vpn-statistics
```

vrf

Creates a Virtual Routing and Forwarding (VRF) instance and enters VRF configuration mode.

Syntax

vrf { **mgmt-vrf** | **default-vrf** | *vrf-name* }

Parameters

mgmt-vrf

Specifies the management VRF.

default-vrf

Specifies the default-vrf.

vrf-name

Specifies the user-defined name of the VRF. The string can be up 64 characters long and should not contain punctuation or special characters.

Modes

Global configuration mode

Port-channel configuration mode

Examples

This example creates the VRF instance "myvrf" and enters VRF configuration mode.

```
device# configure terminal
device(config)# vrf myvrf
device(config-vrf-myvrf)#
```

vrf (epvn IRB)

Specifies a Ve interface, and optionally sets the cluster gateway for the Ve interface in Ethernet Virtual Private Network (EVPN) IRB for the VRF instance.

Syntax

evpn irb ve VE-ID [cluster-gateway]

no evpn irb

CLI_section_ command default

Disabled

Parameters

VE-ID

Specifies a VE interface number.

cluster-gateway

Set the cluster-gateway for the VE interface.

Usage Guidelines

The **no** form of this command returns to the default setting.

Modes

VRF Configuration mode.

Examples

The following example specifies a VE interface 100 in EVPN IRB to the vrf1 instance.

```
device# configure terminal
device(config)# vrf vrf1
device(config-vrf-vrf1)# evpn irb ve 100
device(config-vrf-vrf1)#
```

Examples

The following example specifies a VE interface 100 and sets cluster gateway for Ve 100 in EVPN IRB to the vrf1 instance.

```
device# configure terminal
device(config)# vrf vrf1
device(config-vrf-vrf1)# evpn irb ve 100 cluster-gateway
```

Examples

The following example removes Ve 100 cluster gateway association from the vrf1 instance.

```
device# configure terminal
device(config)# vrf vrf1
device(config-vrf-vrf1)# no evpn irb
```

vrf forwarding

Configures any port as a VRF port.

Syntax

vrf forwarding{ **mgmt-vrf** | **default-vrf** |*vrf-name* }

no vrf forwarding { **mgmt-vrf** | **default-vrf** |*vrf-name* }

Parameters

mgmt-vrf

Specifies the management VRF.

default-vrf

Specifies the default-vrf.

vrf_name

Specifies the user-defined name of the VRF.

Command Default

By default, the out-of-band (OOB) management port (the eth0 interface) is part of the predefined VRF named mgmt-vrf.

Modes

Interface subtype configuration mode

Usage Guidelines

Use the **no** form of the command to disable the specified VRF.

Examples

This example enables enable the management VRF on an Ethernet interface and assigns the interface to a subnet.

```
switch(config)# int te 3/0/2
switch(conf-if-te-3/0/2)# vrf forwarding mgmt-vrf
switch(conf-if-te-3/0/2)# ip addr 10.1.1.1/24
```

This example disables a management VRF that is configured on a VE interface.

```
switch(config)# int ve 100
switch(conf-Ve-100)# no vrf forwarding mgmt-vrf
```

vrf-lite-capability

Sets the download bit (DN bit) check *off* during MP-BGP redistribution into OSPF.

Syntax

vrf-lite-capability

Parameters

There are no parameters for this command.

Modes

Router OSPF mode

Usage Guidelines

no format of this command is not available.

Examples

The following example show the usage of the *vrf-lite-capability* command.

```
SLX (config-router-OSPF-vrf-T1)# vrf-lite-capability
SLX (config-router-OSPF-vrf-T1)#
```

vrrp-acceptmode-disable

Disables accept mode for the backup Virtual Router Redundancy Protocol (VRRP) virtual IP (VIP).

Syntax

vrrp-acceptmode-disable

no vrrp-acceptmode-disable

Command Default

When configured, accept mode is enabled by default.

Modes

Global configuration mode

Usage Guidelines

The **no** form of the command enables accept mode for the backup VRRP VIP.

When enabled, accept mode allows a backup VRRP master device to respond to ping, traceroute, and Telnet packets if it becomes the master VRRP device.

Examples

The following example shows how to disable accept mode for the backup VRRP VIP.

```
device# configure terminal
device(config)# vrrp-acceptmode-disable
```

vrrp-extended-group

Configures a virtual-router-extended group and enters into the virtual router configuration mode..

Syntax

vrrp-extended-group *group-ID*

no vrrp-extended-group *group-ID*

Parameters

group-ID

A user-assigned number from 1 through 255 that you assign to the virtual router group.

Modes

Port-channel interface configuration mode

Virtual Ethernet (ve) interface configuration mode

Usage Guidelines

This configuration is for virtual Ethernet (VE) interfaces only.

Enter **no vrrp-extended-group** *group-ID* to remove the specific VRRP Extended group.

If you remove a group, you cannot retrieve it. You would have to redo the configuration procedure.

Examples

The following example shows how to assign the VE interface with a VLAN number of 20 to the virtual router extended group with the ID of 1. (First you must enable VRRP-E on the switch.)

```
device(config)# protocol vrrp-extended
device(config)# interface ve 20
device(config-ve-20)# vrrp-extended-group 1
```

vrrp-group

Configures a virtual router group (VRRP) and enters into the virtual router configuration mode.

Syntax

vrrp-group *group-ID* [**version** { **2** | **3** }]

no vrrp-group *group-ID* [**version** { **2** | **3** }]

Command Default

VRRP version 2 is the default.

Parameters

group-ID

A value from 1 through 255 that you assign to the virtual router group.

version

Specifies in which version of VRRP the IPv4 VRRP group is to be configured.

2 | **3**

Version 2 or version 3 of VRRP.

Modes

Interface subtype configuration mode

Usage Guidelines

Enter **no vrrp-group** *group-ID* to remove a specific VRRP group. If you remove a group, you cannot retrieve it. You would have to redo the configuration procedure.

You can specify in which version of VRRP the VRRP group is configured using the **version** keyword and either 2 or 3 as the version number. VRRPv3 supports both IPv4 and IPv6 addresses.

Examples

The following example shows how to assign an Ethernet interface to the virtual router group with the ID of 1. (First you must enable VRRP on the switch.)

```
device(config)# protocol vrrp
device(config)# interface ethernet 1/6
device(config-if-eth-1/6)# vrrp-group 1
```

The following example shows how to assign an Ethernet interface to the virtual router group with the ID of 1 for VRRPv3. (First you must enable VRRP on the switch.)

```
device(config)# protocol vrrp
device(config)# interface ethernet 1/6
device(conf-if-eth-1/6)# vrrp-group 1 version 3
```

vtep-discovery

Enables automatic VXLAN tunnel endpoint (VTEP) discovery by BGP.

Syntax

vtep-discovery

no vtep-discovery

Command Default

Enabled.

Modes

BGP address-family L2VPN EVPN configuration mode

Usage Guidelines

The **no** form of this command disables automatic VTEP discovery and creation of VXLAN tunnels.

Examples

The following example disables automatic VTEP discovery by BGP.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# no vtep-discovery
```

The following example re-enables automatic VTEP discovery and creation of VXLAN tunnels by BGP.

```
device# configure terminal
device(config)# router bgp
device(config-bgp-router)# address-family l2vpn evpn
device(config-bgp-evpn)# vtep-discovery
```

write erase

Returns the switch to factory default state.

Syntax

write erase

Modes

Privileged EXEC mode

Usage Guidelines

This command can be used for device recovery or device configuration reset to the factory default state. Due to its disruptive nature, this command prompts the user about the consequence of losing all current user configuration and resetting the switch to the factory default state. It waits for the user's confirmation before proceeding.

Examples

The following command shows executing the **write erase** command.

```
device# write erase
This command will erase all the configuration on the Compact Flash.
The specified VCS parameters will be set appropriately while
preserving the licenses and management ip-address.

System will go through disruptive reboots during the process.
Please upload all configurations if they need to be saved before
continuing with this command.

Do you want to continue? [y/n]:
```

wtb-time

Specifies the Wait to Block (WTB) time for Ethernet Ring Protection (ERP).

Syntax

wtb-time *time*

no wtb-time

Command Default

The default WTB value is 5500 milliseconds (ms).

Parameters

time

Time in ms. Range is from 5100 through 7000, in multiples of 100.

Modes

ERP configuration mode

Usage Guidelines

The WTB time ensures that the clearing of a single Forced Switch (FS) command does not trigger the reblocking of the Ring Protection Link (RPL) when multiple FS situations exist in an Ethernet ring.

Use the **no** form of this command to restore the default value.

Examples

The following example configures a WTB time of 5100 ms.

```
device# configure terminal
device(config)# erp 1
device(config-erp-1)# wtb-time 5100
```

wtr-time

Specifies the Wait to Restore (WTR) time for Ethernet Ring Protection (ERP).

Syntax

wtr-time *time*

no wtr-time

Command Default

The default WTR value is 5 minutes.

Parameters

time

Time in minutes. Range is from 1 through 12.

Modes

ERP configuration mode

Usage Guidelines

The WTR time is configured on the Ring Protection Link (RPL) owner to prevent the frequent operation of the protection switching, which can result from detection of intermittent signal failures.

Use the **no** form of this command to restore the default value.

Examples

The following example configures a WTR time of one minute.

```
device# configure terminal
device(config)# erp 1
device(config-erp-1)# wtr-time 1
```

y1731

Enters the Y.1731 configuration mode.

Syntax

y1731

no y1731

Command Default

This feature is disabled.

Modes

Protocol CFM configuration mode

Usage Guidelines

Use the **no** form of the command to delete all test and action profiles configured under Y.1731 mode and the corresponding associations with source and target MEP pair.

Examples

This example shows how to enters the Y1731 configuration mode.

```
device# configure terminal
device(config)# protocol cfm
device((protocol-cfm)# y1731
```